Department
for Business
Innovation & Skills

UK CYBER SECURITY STANDARDS

Research Report
November 2013

Survey conducted by

pwc

Commissioned by:

The Department for Business, Innovation and Skills (BIS) is building a dynamic and competitive UK economy by creating the conditions for business success; promoting innovation, enterprise and science; and giving everyone the skills and opportunities to succeed. To achieve this it will foster world-class universities and promote an open global economy. BIS - Investing in our future. For further information, see www.gov.uk/bis.

Conducted by:

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.co.uk.

Our security practice, spanning across our global network, has more than 30 years' experience, with over 200 cyber security professionals in the UK and 3,500 globally. Our integrated approach recognises the multi-faceted nature of cyber security and draws on specialists in process improvement, value management, change management, human resources, forensics, risk, and our own legal firm. The PwC team was led by Andrew Miller and Ben Emslie. We'd like to thank all those involved for their contribution to this research.

Foreword

The Department for Business, Innovation and Skills (BIS) recognises the importance of cyber security to the UK economy. Without effective cyber security, we place our ability to do business and to protect valuable assets such as our intellectual property at unacceptable risk.

A vital prerequisite for driving forward our collective maturity and confidence in this area is the timely availability of relevant and appropriate cyber security standards with which organisations can develop and demonstrate their cyber security abilities and credentials. BIS is therefore committed to collating information about cyber security standards and making it available publicly.

As part of this initiative, BIS commissioned a research project into the availability and adoption of cyber security standards across the UK private sector. This report combines the responses to an extensive and wide-ranging online survey, the findings of a series of in-depth one-to-one interviews with a broad range of UK business leaders, and an analysis of the current cyber security standards landscape in order to provide an insight into the current levels of both supply and demand in this area. It also, and perhaps more importantly, aims to identify the prevailing motivators and constraining factors for organisation's adoption of cyber security standards in order to inform the Government's efforts in coordinating and ensuring the nation's collective cyber security.

David Willetts

David Willetts
Minister for Universities and Science

Executive Summary

The number of standards relating to cyber security in some form exceeds 1,000 publications globally. This makes for a complex standards landscape. Despite the quality and general applicability of most individual standards, there was no comprehensive standard identified that provided a 'one size fits all' approach. Conversely the complex landscape made it difficult for organisations to identify the standards relevant to their organisation and business activities.

67%	of publications focus on organisational cyber security standards, adding complexity to this over-represented section of the landscape
3%	of publications focus on people cyber security standards, showing a clear lack of representation and focus in this area
56%	of cyber security publications covered in this report were able to be defined as a 'standard' e.g. rather than a framework or certification
89%	of these publications were sector agnostic and therefore targeting the general market

The awareness of cyber security threats and the importance placed on them was generally high; but organisations mitigate cyber security risk differently depending on the size of the organisation and its sector. This affects the importance placed on the use of standards and certification as an approach.

8th	business priority for organisations is the safeguarding of information assets
7/10	was the average level of importance placed on cyber security certification with 10/10 representing the highest importance
35%	of organisations plan an increase in cyber security spending

Some organisations questioned the relevance of cyber security standards to directly mitigate their organisation's cyber security risk. As a result they often focussed on establishing internal controls and the procurement of new products and services. Standards sometimes supported these approaches but generally only indirectly.

48%	of organisations implemented new policies to mitigate cyber security risks
43%	conducted cyber security risk assessments and impact analysis to quantify these risks
10%	of organisations investing in BYOD implemented a related standard (covering security) to some level. This also showed a particular interest in this technology over others
34%	of organisations who purchased certified products or services did so purely to achieve compliance as an outcome

An increase in products and services standards since 2005 suggests a trend in organisations seeking externally provided security services and off the shelf products. Despite this increase, the supply of standards fails to match the levels of investment across the categories.

Products		*Organisational*	
16%	*V* *s*	*67%*	% of standards relating to this category
69%		*42%*	% of organisations investing over £1k p.a. in this category
25%	of organisations believe people standards to be 'not important at all'		

While many organisations implement cyber security standards to some degree, the majority partially implement the controls deemed relevant and self-certify this compliance. Only a small proportion invests in gaining external certification.

52%	of organisations implement a standard to some level
25%	of organisations invest in full implementation of at least one standard

1in4	of the 25% of organisations above that fully implement a standard invested in external certification

Organisations stated predominantly commercial and business reasons for their lack of adoption of cyber security standards and the investment in external certification. This suggests a perceived lack of clarity surrounding the business case for cyber security standards. No standard reviewed as part of this research incorporated a business case element.

1st	main barrier to cyber security standards is that they are too expensive
2nd	most commonly stated barrier is the difficulty in calculating a return on investment

3rd	barrier is that there appears to be no discernible financial incentive to invest

The average current investment in cyber security and cyber security standards was generally low but many had plans for the future, showing a potential rise in future adoption.

54%	of organisations invest less than *5%* of their cyber security budget on cyber security standards compliance
34%	of organisations plan to develop an Information Security Management System in the future
39%	plan to achieve certification to a cyber-security standard in the future

Table of Contents

Background and purpose

The standards landscape for cyber security is highly complex, with various Government and industry-led standards and schemes in existence and in development, domestically and internationally. Without a clear understanding of this landscape, and the current and potential uptake of standards, Government is unable to identify and develop evidence-based policies to close the gaps in the landscape or support the uptake of good standards for cyber security products and services.

The purpose of this report is to inform the understanding of the cyber security standards landscape, and the current and potential uptake of standards in the UK. This has been achieved via research to identify what standards organisations have adopted, why they have chosen such an approach and how they have used these standards to support their organisation.

Research approach

In order to produce this report a number of research methods were applied. These included:

1. The identification of the prevalent cyber security standards in the UK, determined by the respondents and contributors to this research.

2. Gathering information on existing standards, and documenting their coverage and content. This was corroborated and enhanced by subsequent cross referencing with the information gathered in the steps below.

3. Engagement with a broad range of UK organisations via an online survey and a series of one-to-one interviews to identify current trends in UK cyber security standard adoption; the motivators for organisations to do so; and the barriers or constraints that inhibits investment in this area.

    a. The online survey reached an audience of approximately 30,000 organisations, yielding over 500[1] responses. It should be noted that extrapolation of survey data across the whole of the UK should always be treated with caution, especially given the self-selecting nature of the survey and the response levels for some of the questions. The relatively low response rate, despite the broad distribution, may in itself represent a significant finding; that private sector awareness of and/or interest in the area of cyber security standards may be generally low. A common view expressed during the research was that cyber security standards were not high on the agenda of respondents' organisations; perhaps supporting this hypothesis and indicating why the footfall was relatively low and the abandonment rate relatively high.

    b. The survey was supplemented by 20 one-to-one interviews with senior individuals responsible for cyber security standards in organisations of all sizes and ages

[1] Note that not all 500+ potential respondents who viewed the survey went on to complete it. Responses were captured on a question-by-question basis, revealing an approximately linear rate of respondent abandonment through the survey. The actual sample size from which each statistic is drawn is shown directly beneath the relevant figure.

across a broad range of market sectors, from all regions of the UK as well as global organisations with a UK presence.

Figures 1 to 4 in the section below illustrate the wide range of organisations represented by this study's survey respondents and interview participants. Further information regarding the approaches adopted for the survey and interview elements of this study, along with further detail regarding the demographics of the respondents/interviewees, can be found at Annex A. In particular the strength of the statistical conclusions around the survey data collected and presented in this report should also be considered. These are outlined in more detail in Annex A.

Overview of survey respondents

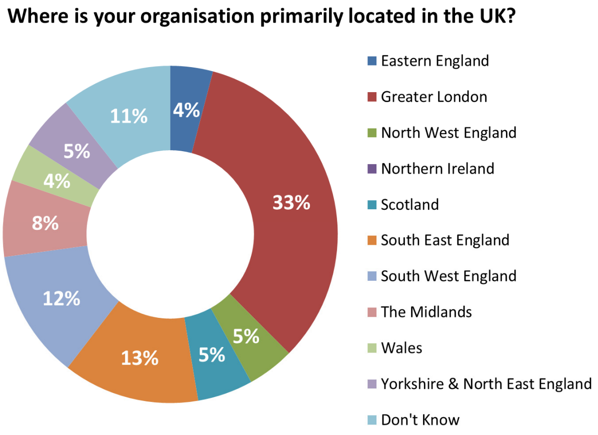


Figure 1 (based on 243 responses)

Figure 2 (based on 223 responses)

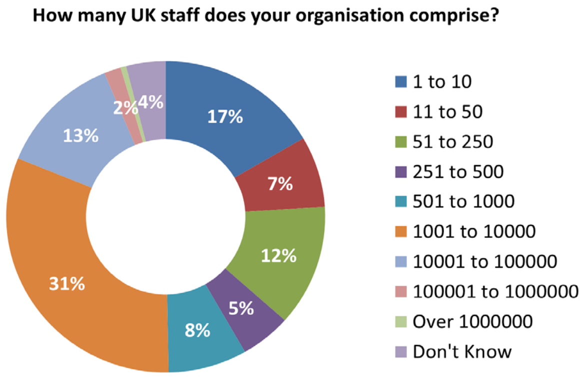


Figure 3 (based on 175 responses)

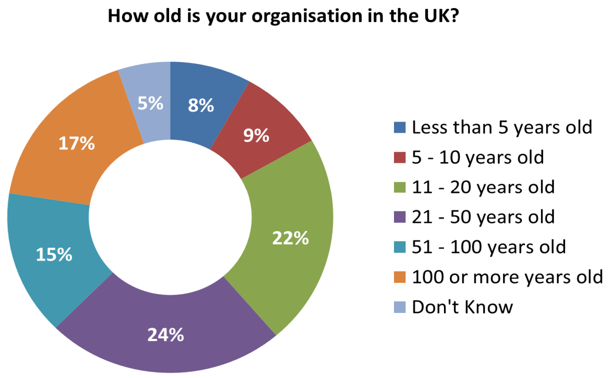


Figure 4 (based on 173 responses)

The cyber security standards landscape

This section aims to identify the standards that lie within the current UK cyber security standards landscape, and then draw evidence-based observations regarding those standards against a number of pre-defined dimensions of interest. The standards identification approach, dimensions of interest and terminology used in this section are all defined at Annex B.

This section also presents a detailed analysis of a sub-set of these standards against the PwC cyber security framework in order to map their coverage and content. This framework is explained in detail at Annex D.

The section is structured using a number of sub-sections, as follows:

- **The current UK cyber security standards landscape.** This sub-section introduces how standards were identified for this study, defines some of the terminology used, and identifies the dimensions against which the standards have been mapped. It presents a factual, high-level mapping of the cyber security standards landscape and uses metadata about these standards to draw evidence-based observations regarding the landscape's coverage.
- **Products and services coverage analysis.** Focuses specifically on the coverage achieved by standards relating to products and services within the cyber security standards landscape, based on the definition in Annex B and identified as described in Figure 10.
- **Interdependencies between standards.** Comments on the relationships and interdependencies between individual standards (or families of standards) where applicable.
- **Detailed mapping of content.** A subset of standards was selected, and each standard within the subset was tested for coverage against a defined framework. This sub-section describes the approach taken to achieve this detailed mapping, and its outcome.

Figure 7 below allows the many-to-many relationship between each publication and the content category/categories it covers to be seen clearly. Publication reference numbers have been placed on the diagram, rather than publication titles, due to the prohibitive density of text that would arise through taking the latter approach. The translation between publication reference numbers and publication titles can be made using the two left-most columns of the tables in Annex C.

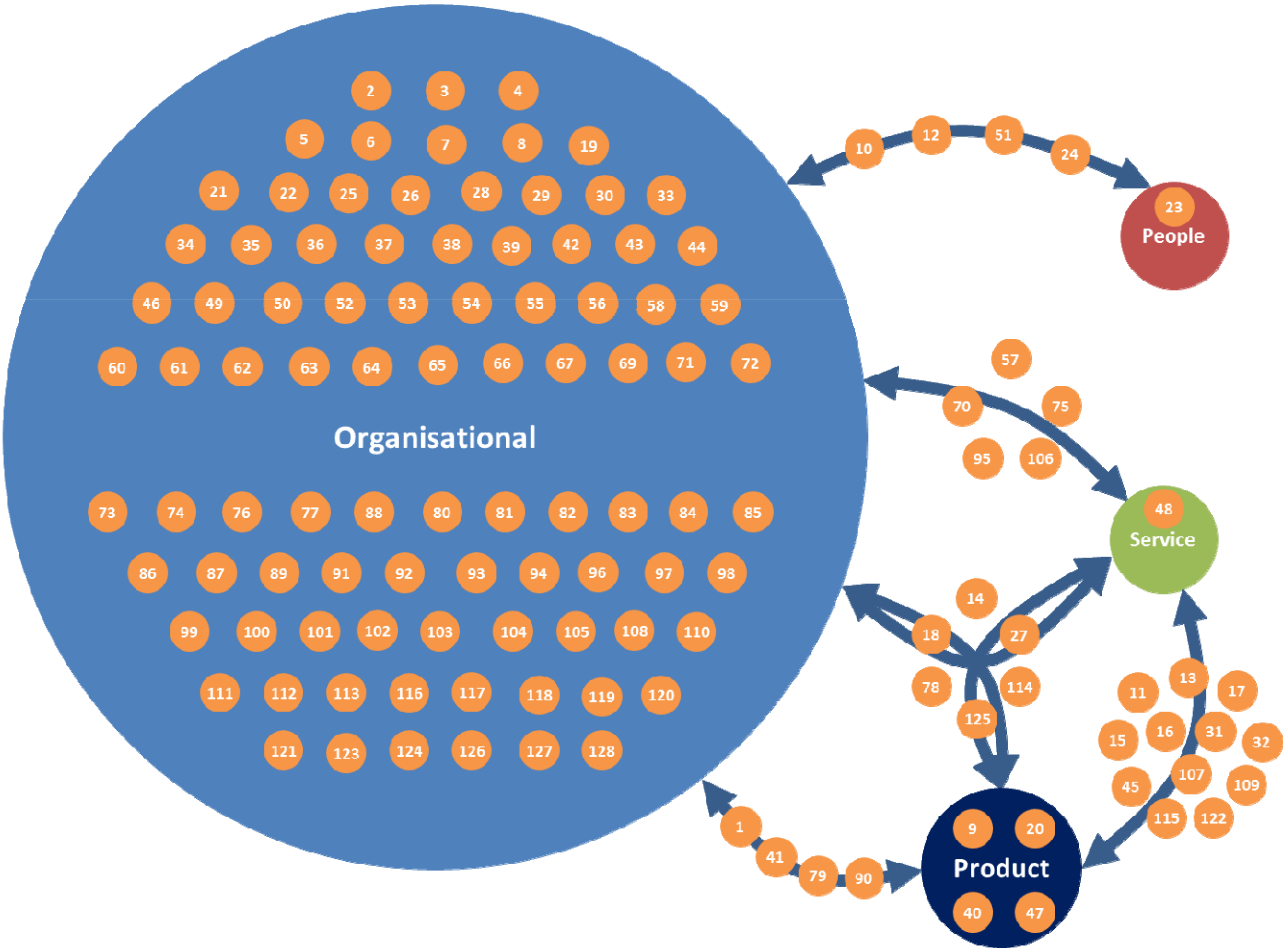


Figure 7: *distribution of publications within the landscape by content category*

It is apparent from Figure 7 above that the availability of existing cyber security publications is heavily skewed towards the Organisational aspects of cyber security. Other notable observations include:

- There is no single publication that covers all 4 of the Organisation, People, Product and Service categories.
- While 5 publications (3%) are related to the People aspects of cyber security at least in part, only one is solely People-focused. This may suggest that there is currently a dearth of information within publications available to organisations regarding how they should/could address the People aspect of cyber security.
- While there is reasonable coverage of the Product and Service aspects of cyber security (32 publications in total, or 25% of the landscape), coverage is relatively light in specific areas. For example, there is only one publication that is solely Service-focused. This is ISO/IEC 17021 ("Conformity Assessment - Requirements for Bodies Providing Audit and Certification of Management Systems"), which is aimed solely at certification bodies rather

The current UK cyber security standards landscape

The approach, definitions and dimensions of interest outlined in Annex B were used to produce a 'high-level' cyber security standards landscape map in tabular form, which can be found at Annex C. From what is necessarily a snapshot view, obtained through a combination of survey/interview responses and this research, a total of 128 standards were identified for inclusion within the landscape. The metadata within the high-level mapping was used to produce the statistics that follow, from which the evidence-based observations found in this report have been drawn against the dimensions of interest defined at Annex B.

Publication nature

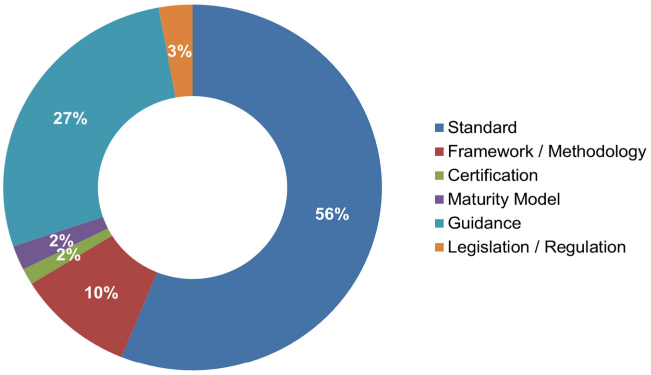


Figure 5: *distribution of publication natures within the landscape*

Figure 5 shows the distribution of publication natures within the landscape.

More publications are standards than all of the other 5 publication natures combined, representing 56% of publications within the landscape. Notably, this means that the majority of publications in the cyber security arena should enable their adopters to be audited against and thus certified as meeting their contents (providing certification bodies choose to offer certifications against a given standard). Guidance is the second most prevalent publication nature at 27% of the landscape; and legislation/regulation the least prevalent at 3% of the landscape. Several of the guidance publications identified within the landscape are supplements to, or elaborations upon, more formal, directive standards.

Content category

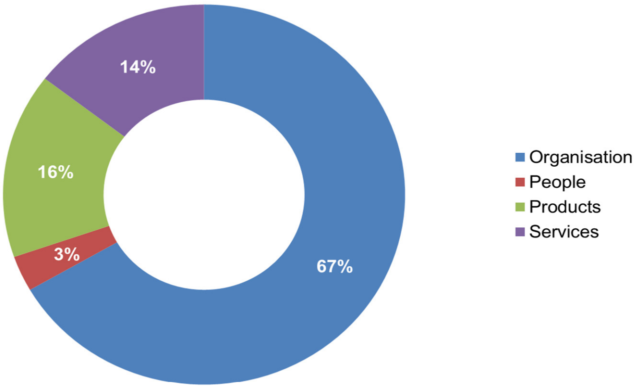


Figure 6: content (by category) of the publications within the landscape

Figure 6 shows the coverage of each content category by the publications within the landscape.

Publications which focus on the organisational aspects of cyber security are in the majority, representing 67% of publications within the landscape and more than the other 3 categories combined.

Products and Services receive approximately equal levels of coverage at 16% and 14% respectively.

The People aspect of cyber security receives very little coverage, constituting just 3% of publications within the landscape, suggesting that this aspect may be under-represented.

It should be noted that a given publication or family of publications may legitimately achieve coverage against multiple content categories (the categories are not mutually exclusive, as per the detailed category definitions in Annex B). Figure 6 above does not fully reflect these many-to-many relationships but gives an indication of coverage distribution on the basis of predominant density. The proportion of publications which map to multiple categories is sufficiently small that any inaccuracies introduced through this simplification are likely to be insignificant.

than adopters. There is therefore no solely Service-specific publication available to organisations wishing to utilise such documentation. This may suggest that there is currently a lack of information available to organisations regarding how they should address the Service aspect of cyber security.

Industry sector

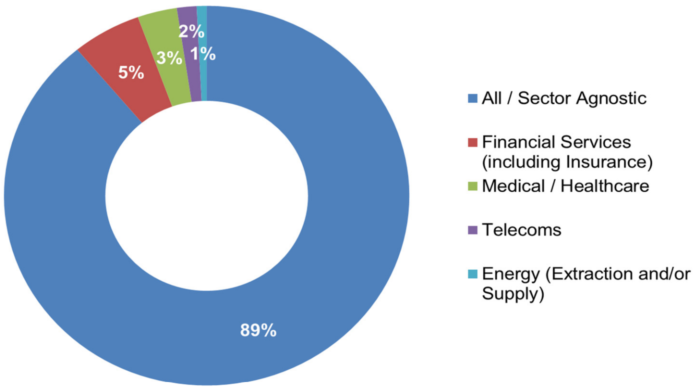


Figure 8: *industry sector applicability of the publications within the landscape*

Figure 8 shows industry sector applicability of the publications within the landscape.

The vast majority (89%) of publications are sector-agnostic. The only industry sectors with sector-specific publications are:

- Financial services, including insurance (5%).
- Medical/healthcare (3%).
- Telecommunications (2%).
- Energy, including extraction and supply (1%).

Notably the sectors above are those with some of the heaviest regulatory requirements in other risk areas; perhaps because incidents affecting these sectors are viewed as likely to have a severe impact.

Relevance

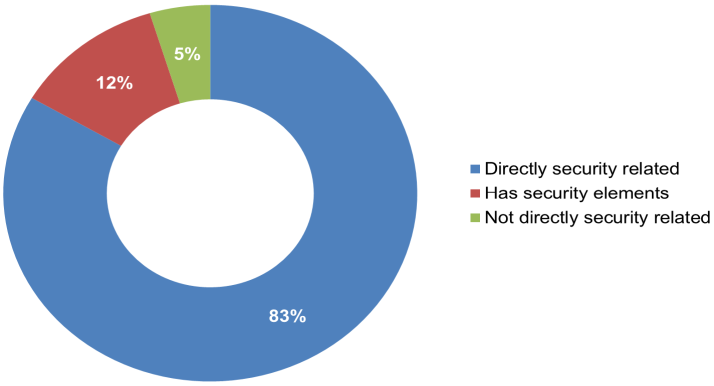


Figure 9: *degree of cyber security relevance of the publications within the landscape*

Figure 9 shows the degree of cyber security relevance of the publications within the landscape.

The vast majority (83%) of publications are directly security-related.

A small number (12%) of publications are not solely security-focused, but have discrete security elements within them. For example, TOGAF is a Technical Architecture framework; but contains a discrete chapter on Security Architecture.

An even smaller number (5%) of publications are not security-focused and have no discrete security section; but address security subjects immediately alongside other subject matter.

Prevalence

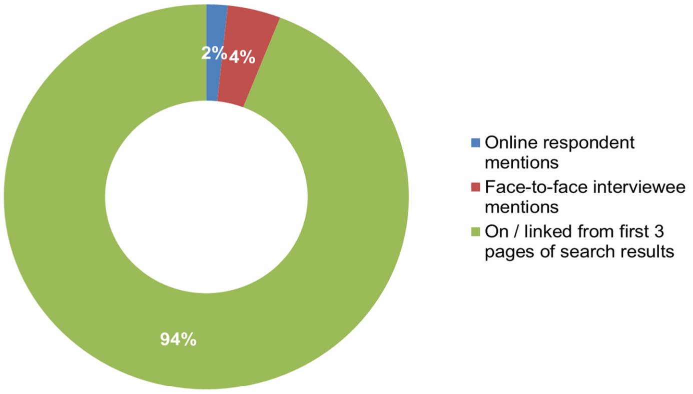


Figure 10: *the means through which publications within the landscape were identified*

Figure 10 shows the means through which the publications within the landscape were identified.

The vast majority (94%) of publications were identified through being one of the first 30 results for the search strings "cyber security standards" or "information security standards" on a popular Internet search engine; or linked/referenced directly from such a result.

The publications mentioned by face-to-face interviewees correlated heavily with the results of the Internet search, although there were some additions to the landscape (4%) as a result of the interviews. Online survey respondents mentioned a very small number of publications (2%) that had not already been captured within the landscape.

Language

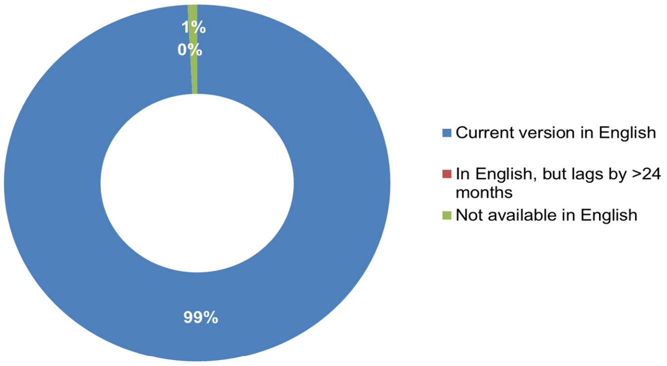


Figure 11: *the proportion of the publications within the landscape which are available in English*

Figure 11 shows the proportion of the publications within the landscape which are available in English.

All bar one of the publications identified have a current version (99%) available in English.

The one non-English publication is ISME, which is an adaptation of the German Bundesamt fur Sicherheit in der Informationstechnik (BSI) '100 Series' of publications for the Estonian public sector, published in Estonian.

It was anticipated that some publications might be written in languages other than English and then translated into English some time later. This proved unfounded: the current versions of all foreign publications are available in English.

Classification

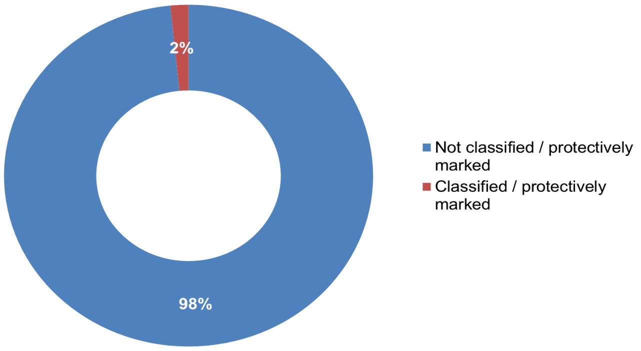


Figure 12: *the proportion of the publications within the landscape which are classified*

Figure 12 shows the proportion of the publications within the landscape which are classified by a government entity.

All bar two of the publications identified are unclassified / not protectively marked. The 2 classified publications are:

- The UK MOD's Joint Service Publication (JSP) 440 (Defence Manual of Security).
- The South African Government's Minimum Information Security Standards.

There is likely to be classified cyber security documentation within the government, military and/or intelligence spheres which are not known (regardless of whether they are available) to the private sector.

Status

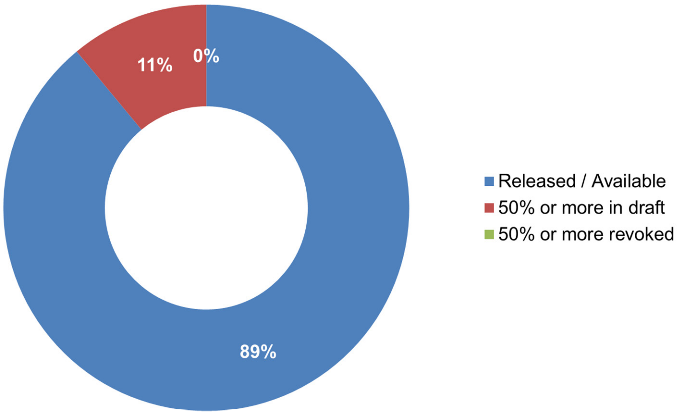


Figure 13: *the proportion of the publications within the landscape which are released/available*

Figure 13 shows the proportion of the publications within the landscape which are released / available (i.e. the publication is not currently in drafted or awaiting approval for release).

The vast majority (89%) of publications are released and available. A small number (11%) are in draft, such as:

- ISO27014 & ISO27015 (cloud computing).
- ISO27033 (network security) & ISO27034 (application security).
- ISO27038 to 27040 (operational security).
- ISO27041 to 27044 (incident management, investigations and digital forensics).

Intended audience

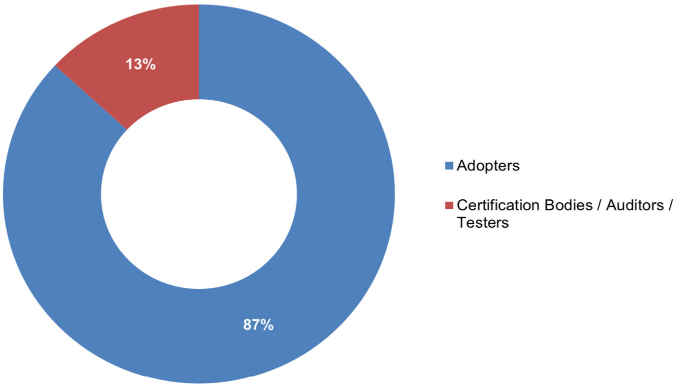


Figure 14: *the intended audiences of the publications within the landscape*

Figure 14 shows the intended audiences of the publications within the landscape.

Of the 128 publications within the landscape:

- 110 are aimed solely at adopters (i.e. the subjects of potential certification).
- 8 are aimed solely at certification bodies, auditors and/or testers.
- 10 are aimed at both adopters and certification bodies (to some extent).

This distribution does not seem particularly remarkable: it is plausible that some publications could contain sufficient information for both adopter and auditor, while in some situations it may be preferable to meet the needs of two communities separately.

Origin

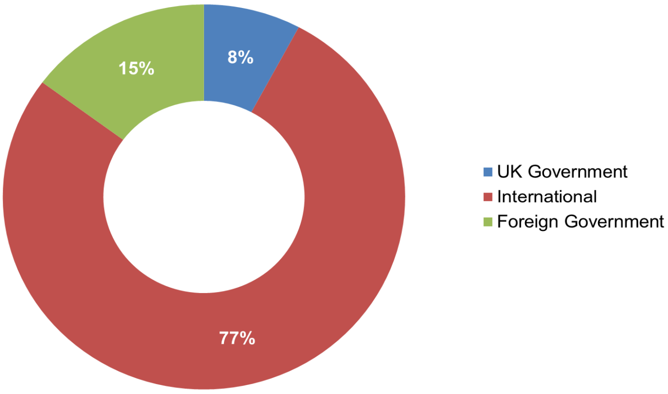


Figure 15: *the origins of the publications within the landscape*

Figure 15 shows the origins of the publications within the landscape.

The majority (77%) of publications have either originated as an international publication through open, cross-border collaboration from the outset; or have been 'internationalised' by organisations such as ISO selecting the 'best in class' publications produced by a single country or group of countries and re-branding them as their own.

Governments, which have traditionally led research in cyber security due to its evolution from the cryptography and code-breaking arena, seem to have become less active than the private / not-for-profit sector in recent years.

Agedness

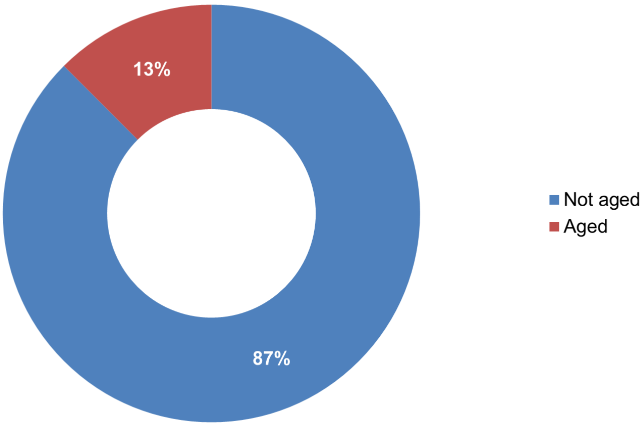


Figure 16: *the proportion of the publications within the landscape which are aged*

Figure 16 shows the proportions of the publications within the landscape which are aged (for the purposes of this report, any publication last revised more than 10 full calendar years ago, i.e. prior to 1st January 2003, is considered aged).

The vast majority (87%) of publications have been revised in the last 10 full calendar years. Perhaps surprisingly, given the prevailing rate of technological change and the recent emergence of cyber security in the public consciousness, 16 publications (13%) had not been revised since 1st January 2003.

Four mainstream publications were last revised in the mid-1990s (ISO/IEC10181-1:1996, ISO/IEC 7498-1:1994, NIST Special Publications 800-12 & 800-14); while one was last revised in the 1986 (TCSEC / 'The Orange Book').

Figure 17 below shows the distribution of publication agedness in more detail, by the year of the publication's most recent revision. The colour coding reflects the nature of the publications last revised in each year.

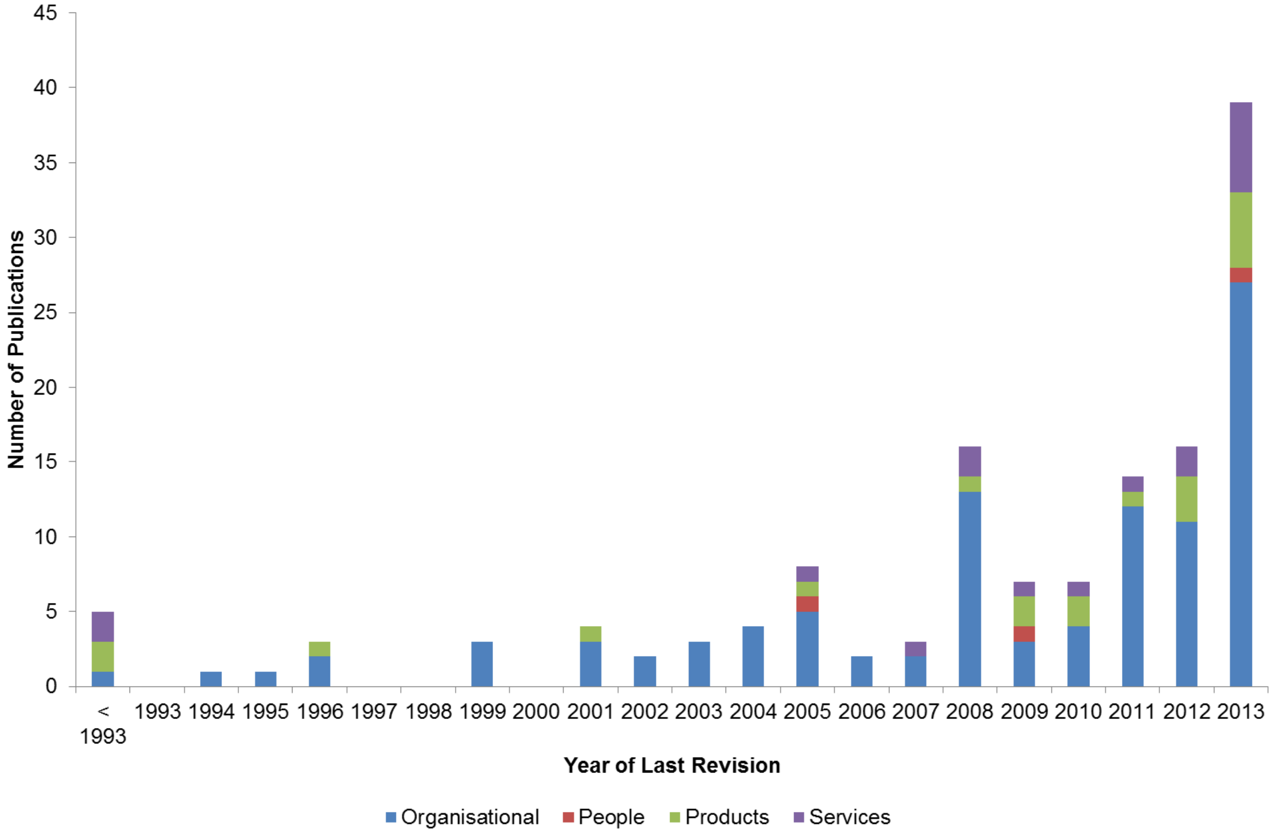


Figure 17: *publication agedness by year of last revision*

Notably, non-organisational publications (i.e. those that relate to the People, Product or Service aspects of cyber security) appear much more frequently from 2005. This may indicate that the emergence of business practices such as outsourcing, off-shoring and mobile working, and the emergence of 'X'-as-a-service (XaaS) capability delivery models such as cloud computing, may be re-focusing the emphasis of cyber security risk and thus the publications designed to mitigate/manage it away from internal, organisation-centric systems of control towards those related to externally-provisioned services and commercial-off-the-shelf products.

Additionally, the ready availability of publications relevant to the Organisation category and the length of time for which they have been available may have enabled organisations to become more confident in their ability to manage the organisational aspects of cyber security than the People, Product or Service aspects. The recent emergence of publications that address these aspects may reflect such a change in focus.

Product and Service coverage

This section aims to provide a more detailed analysis of the coverage of individual Product and Service types by the publications within the identified cyber security standards landscape.

Note that the charts in this section do not show the proportion of *publications* that are attributable to a given Product or Service type. Instead, they show the proportion of *publication to product/service type mappings* that are attributable to a given Product or Service type. The rationale for presenting the statistics in this form is that it shows the overall density of coverage against each Product or Service type using a two-dimensional representation, rather than attempting to model what is in actuality a many-to-many relationship between publications and the Products and/or Services that they cover using multi-dimensional graphs. It also prevents the sum of the percentages provided exceeding 100%, which can be counterintuitive.

Product type coverage

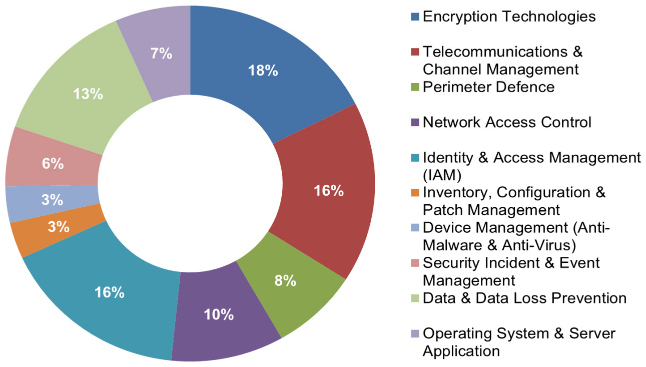


Figure 18*: product type coverage by publications within the landscape*

Figure 18 shows the product type coverage by publications within the landscape. (The definitions for each of the product types can be found at Annex B)

Each of the 10 product types is covered by at least one of the publications within the landscape.

There is a degree of variation in the extent to which each product is covered however. Encryption products (18%), telecommunications & channel management (16%) and identity & access management (16%) were the best represented product types, with almost 3 times the level of coverage as the least represented types. Device management (anti-malware/anti-virus) and inventory, configuration and patch management were the least represented types, each having 3% of total coverage.

Service type coverage

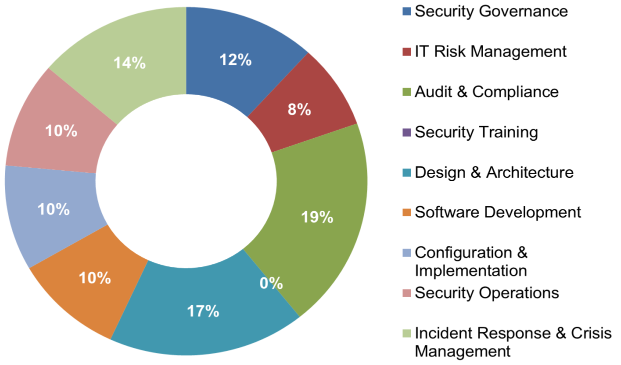


Figure 19: *service type coverage by publications within the landscape*

Figure 19 shows the service type coverage by publications within the landscape. (The definitions for each of the service types can be found at Annex B)

Notably, one of the 10 service types is not covered by any of the publications within the landscape. This is Security Training, which mirrors previous observations in this report regarding the People aspect of cyber security having the least coverage of the 4 categories used in this study.

There is a similar degree of variation in the extent to which each service is covered as was previously noted for the variation in product type coverage. Audit & compliance (19%) and design & architecture (17%) were the best represented services types. Security training (0%) was the least represented service type, with IT risk management (8%) as second least represented.

Interdependencies between standards

Not all of the publications identified within the landscape are separate, independent publications. Some:

- Are independent in terms of subject matter, but are published by the same publisher such that they have a common ‘look and feel’. This may incline a potential adopter who is looking for a standard that covers a given subject to refer to that publisher’s publication portfolio.
- Are grouped into series by subject matter, but may not be interlinked. For example, European Telecommunications Standards Institute (ETSI) publications tagged with the security ‘keyword’ but which cover diverse technologies; or International Telecommunications Union (ITU) publications which carry the publication code prefix ‘X’ to indicate that their content relates to security, but which only collectively exist as the ‘X series’ in a complementary rather than sequential or interdependent manner. (Note that ‘grouping’ in this sense is a matter of landscape scope; rather than the granularity with which the landscape is mapped.)
- Form hierarchical families where one publication references or encapsulates another. For example, ISO27002 elaborating upon ISO27001.
- Attempt to identify and/or draw together ‘best in class’ material by signposting specific sections, clauses or controls within other publications. For example, Publically Available Standard (PAS) 555 signposts material from ISO standards 9000, 20000, 27001, 22301 and 31000, aligned against its own framework.

The process for determining whether a family of publications should be mapped as a single line item, or as multiple individual publications or sub-families, is described in the ‘granularity at which publications are mapped’ section within Annex B.

Detailed mapping of standard content

The high-level cyber security standards landscape at Annex C provides a view of how existing publications map to the landscape against a series of pre-defined dimensions of interest at a metadata and content synopsis level. The high-level mapping does not in itself provide a view of the extent to which publication content may vary in focus *within a given publication*. For example, the high-level mapping does not attempt to assess any given publication’s comprehensiveness against all the sub-elements of the subject it claims to cover.

As a detailed review of all 127 publications within the identified landscape is beyond the scope of this study, this section will map a sub-set of the publications within the landscape at a lower level. It will examine these publications in terms of their low-level coverage relative to their specified subjects in order to draw observations as to their purpose, intended audience, focus and comprehensiveness and thus provide a view of their breadth and depth.

A shortlist of 9 publications to undergo the detailed mapping process was produced by applying a set of pre-defined criteria. These criteria, which can be found in full at Annex D, attempt to identify the standards to which a potential first-time adopter of cyber security standards within the UK private sector might turn on; using factors such as the publications’ last revision date (not too old), its language (in English), its accessibility (not classified or otherwise constrained to the government), etc.

As there is no single, globally-recognised framework to describe the domains that comprise the totality of ‘cyber security’ in the round, this report has used the 6 domains within the PwC cyber security framework for the detailed mapping process. The detail behind the cyber security framework and the coverage level numbering system used are at Annex D.

The detailed mapping process was used to produce the tables at Annex E, which show the comprehensiveness of each shortlisted publication against the assessment framework’s domains.

The key findings of the detailed mapping process were:

- There is no single identified standard that comprehensively covers the totality of cyber security as defined by the framework.
- All of the 9 shortlisted standards are predominantly Organisational in focus, with the exception of PCI-DSS (which covers products and services) and HMG SPF which covers people standards.
- Both the Australian ISM and the German BSI 100 Series standards demonstrate good coverage against their stated subject matter; although it is not known as to whether a given standard being authored by a foreign government may be off-putting to prospective UK private sector adopters.
- 6 of the 9 are categorised as standards; with HMG SPF categorised as a framework; and the ISM and BSI 100 Series categorised as guidance.
- 4 of the 9 publications require the reader to purchase it or to join a membership body.

A summary overview of the detailed mapping output at Annex E is at Figure 20 overleaf.

Publication Name	Accessibility	Type						Category				Domain Mapping					
		Standard	Framework	Certification	Maturity Model	Guidance	Legislation	Organisation	People	Product	Services	Governance	People	Prepare	Operations	Intelligence	Respond
Australian Defence Signals Directorate (DSD) Information Security Manual (ISM); formerly known as "ACSI33"	Freely available					x		x				3	2	3	3	2	2
Bundesamt fur Sicherheit in der Informationstechnik (BSI) '100 Series'	Freely available					x		x				2	1	2	1	2	3
HMG SPF (Security Policy Framework)	Freely available		x					x	x			2	2	2	2	2	2
IASME (Information Assurance for Small & Medium-sized Enterprises)	Freely available	x						x				2	1	1	1	1	1
ISF (Information Security Forum) Standard for Good Practice for Cyber Security (SGP)	Freely available to ISF members	x						x				3	3	3	2	3	3
ISO27001:2005	Available at cost	x						x				2	1	2	3	1	2
ISO27002:2005	Available at cost	x						x				3	2	3	3	2	3
Payment Card Industry Data Security Standard (PCI-DSS)	Freely available	x						x		x	x	2	1	3	2	2	1
Publicly Available Specification (PAS) 555:2013 (including Annexes)	Available at cost	x	x					x				2	2	1	1	1	2

Figure 20: *Detailed mapping snapshot (see Annex E for full version)*

Note: ISO27032 has been omitted from this analysis, despite being the only ISO publication to have 'cyber' in its title, due to awareness of this standard across the marketplace being much lower than that for ISO27001/27002. This is likely to be a factor of its relatively recent publication (the first finalised edition of ISO27032 was published in 2012).

Adoption of cyber security standards by UK industry

Whereas the previous section looked at the publications comprising the cyber security standards landscape, this section focuses on the current extent of cyber security standard adoption within the UK private sector.

The evidence gathered through the online survey and one-to-one interview responses is analysed within this section to provide a statistical insight into which standards are the most frequently adopted by UK organisations; the extent to which they are adopted; organisations' motivations for adopting various standards; and the business benefit that the adopting organisation believes that they subsequently realise as a result of such adoption. This section also analyses respondents' motivations for and barriers to their investment in implementing and/or certifying to particular standards.

Organisations' prioritisation of cyber security

Before identifying the extent to which various cyber security standards are adopted by UK industry, it is important to first identify the context within which UK industry's decisions surrounding cyber security standards adoptions are made. Accordingly, the first substantive questions within the online survey were related to understanding each respondent's organisation's current prioritisation of cyber security as an issue in the round. This included asking each respondent to gauge the importance of cyber security as business objective and to comment on the level of financial investment that their organisation was making in this area.

Organisations' prioritisation of cyber security relative to other business objectives

Figure 21 below illustrates respondents' responses regarding their organisations' business priorities. Cyber security was deliberately not called out by this name; rather, it was abstracted as the business objective of 'safeguarding of information assets'.

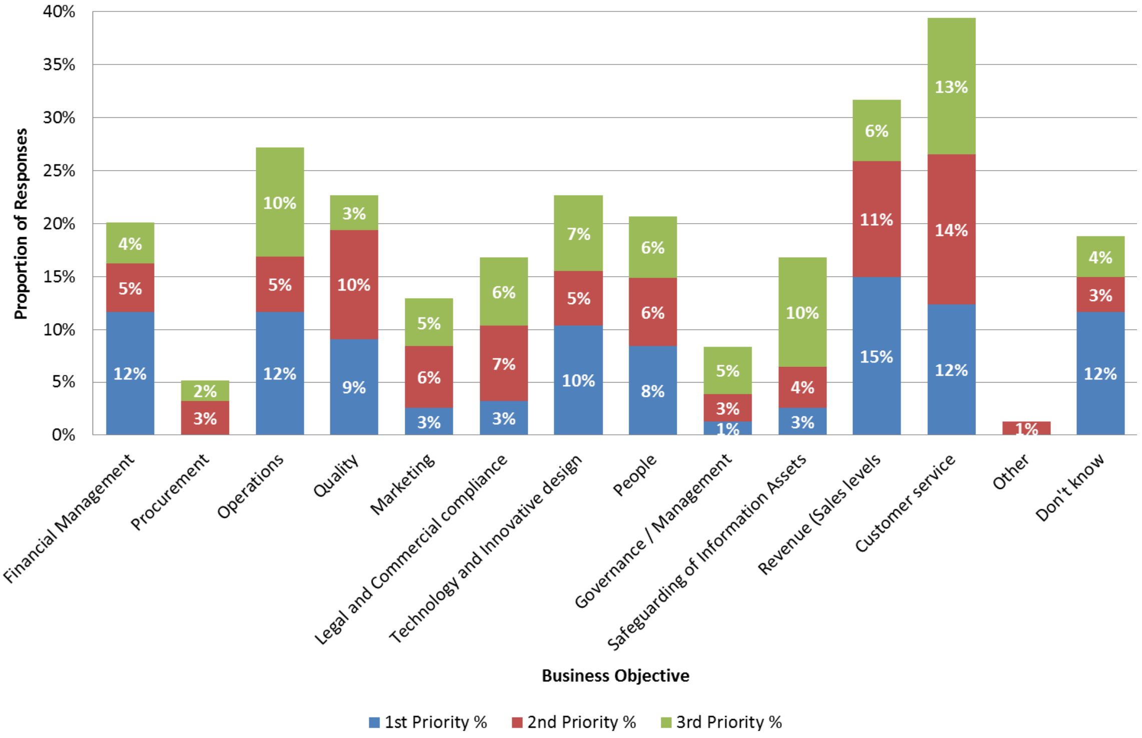


Figure 21: *the priorities each respondent's organisation places on its business objectives (based on 155 responses)*

Figure 21 demonstrates that the protection of information assets, including (by inference) cyber security, does not represent a particularly high priority for respondents' organisations. The most highly prioritised business objectives, according to survey respondents, were 'customer service' and 'revenue'; showing a highly business-focused respondent pool. The protection of information assets was the tenth most frequent response out of the 14 options (including "other") presented overall. Even "don't know" scored more highly. Notably, and more positively, the protection of information assets was the second most frequent response when respondents were asked to identify their organisation's third most important business priority, with 10% of third priority responses assigned to the protection of information assets.

A common response from the one-to-one interviews was that cyber security was of growing importance and the focus, attracting increasing investment from respondents' organisations. However the majority of interviewees deemed the adoption of or certification to cyber security standards as being of no more than moderate importance in support of their broader cyber security programmes, and more 'desirable' than 'essential'. This is explored further in the 'prioritisation of cyber security standards adoption' section that follows.

Organisations' levels of investment in cyber security

Figure 22 below shows how much financial investment each respondent's organisation had made in the last 12 months in relation to each of the 4 categories of cyber security defined in Annex B.

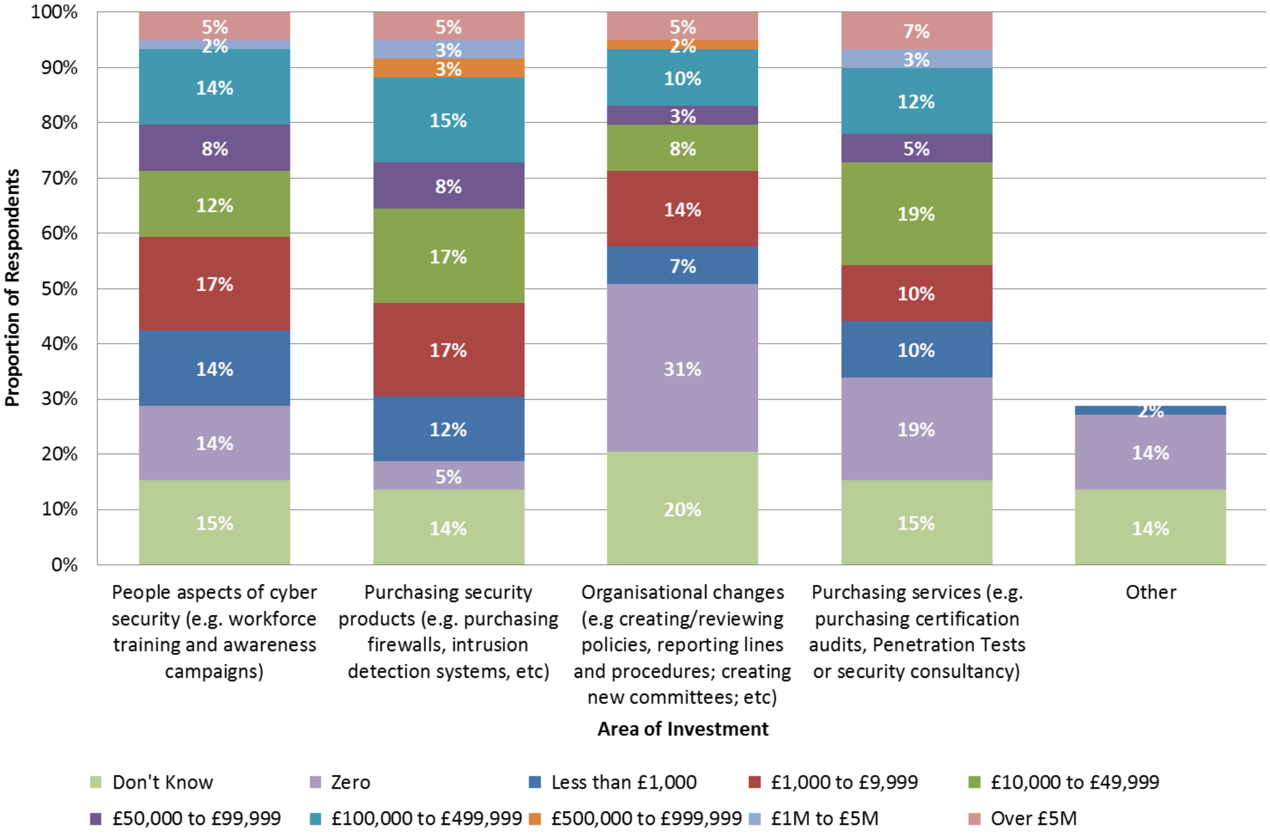


Figure 22: *organisations' investment in various areas of cyber security within the last 12 months (based on 59 responses)*

Figure 22 shows that investment was heaviest in the Products space, with over half (53%) of respondents' organisations investing more than £10,000 in this area over the last 12 months and more than a quarter (27%) investing over £100K. Investment was lightest in the Organisational standards space, with 37% of respondents' organisations investing less than £1,000.

Notably, the relative levels of availability of standard that cover each of the 4 categories (Organisation, People, Product and Service) do not seem to correlate with the levels of investment that organisations are currently making. In fact, the overwhelming prevalence of Organisational standards runs contrary to the fact that organisations are currently investing less heavily in Organisational changes that in changes related to People, Products or Services.

Organisations' prioritisation of cyber security standards adoption specifically

The online survey next sought to identify the importance that respondents' organisations placed on obtaining certification against one or more cyber security standards specifically. The results of the responses to this element of the survey can be seen in **Figure 23** below.

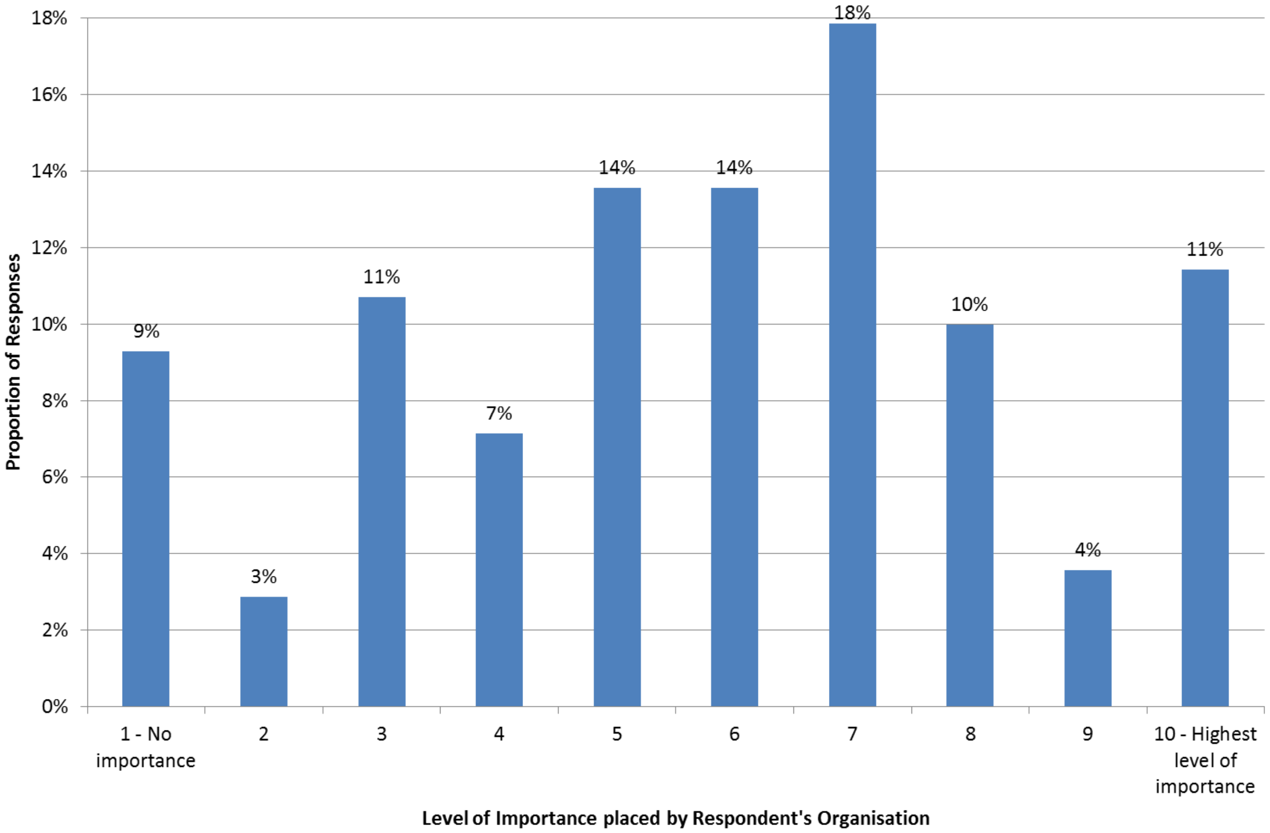
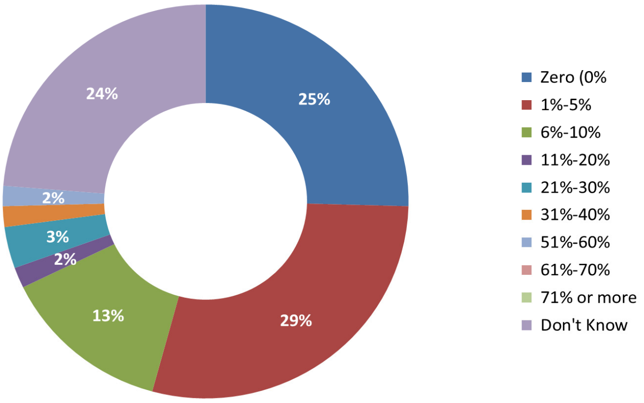


Figure 23: *The level of importance an organisation places on cyber security certification (based on 140 responses)*

Notable features of Figure 23 include that:

- 43% of respondents viewed cyber security certification as having an importance level of 7 or higher, indicating that respondents saw value in cyber security standards certification.
- 11% viewed cyber security certification as being of the highest importance (10 out of 10).
- 44% viewed cyber security certification as being of middling importance (5 out of 10) or lower.



Anticipating that perceptions as to the importance of cyber security standard certification may differ from levels of actual investment in such certification, respondents were then asked to identify the proportion of their organisation's overall cyber security budget that was invested in standards compliance or certification specifically. Figure 24 shows the responses to this question.

Figure 24 shows that less than half (46%) of organisations invested 5% or more of their cyber security budget in standards compliance and/or certification in the last 12 months.

Figure 24: *cyber security budget spent on cyber security standards compliance in the last 12 months (based on 59 responses)*

Present levels of cyber security standard adoption within the UK private sector

Figure 25 is a key output from the online survey: it shows which standards are adopted within the UK private sector, and the extent to which they are adopted.

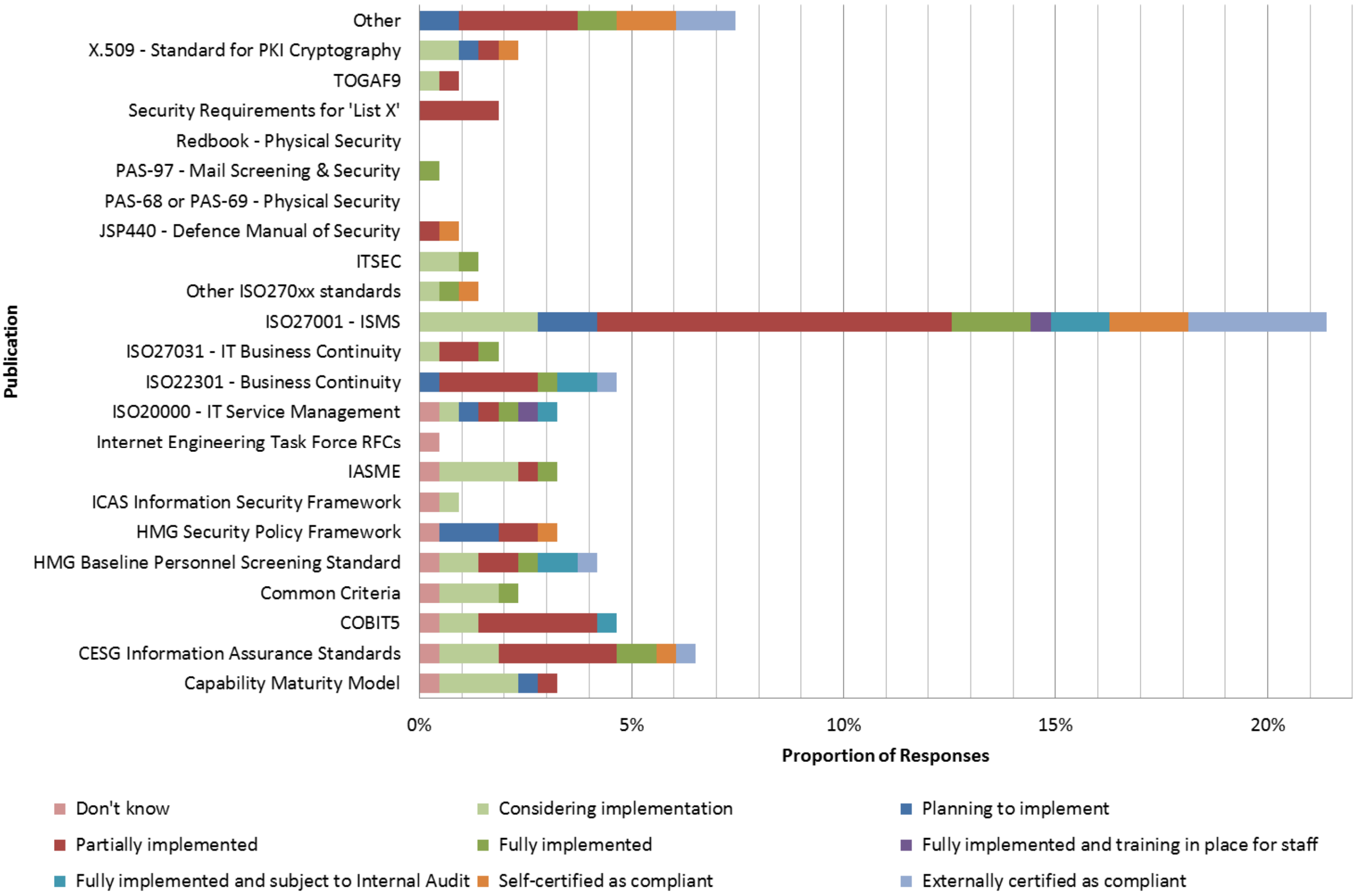


Figure 25: the standards that are adopted within the UK private sector, and the extent to which they are adopted (based on 110 responses)

ISO27001 is the most frequently adopted standard by a significant margin; with over 21% of respondents stating that their organisation had adopted it to some extent (or are planning/considering to do so). Figure 25 also shows considerable variation in the extent to which organisations adopt standards:

- Only 7 out of the 19 organisations (37%) that believe they have fully implemented ISO27001 have gone on to obtain formal external certification of such compliance.

- Only 13 out of the 53 organisations (25%) that believe they have fully implemented any of the standards shown in Figure 25 have gone on to obtain formal external certification of such compliance.

- ‘Partial implementation’ was the most frequent level of implementation across all of the standards that had been adopted to some extent, at 27%.

Note that where the ‘other’ response was given, respondents were provided the opportunity to enter a free text response. The most popular publications referenced via the ‘other’ free text field were PAS 555 (1%) and PCI-DSS (1%).

Variation in standards adoption by category

This section aims to identify any variations that may exist in the levels of standards adoption or investment between the 4 categories of Organisation, People, Products and Services defined previously in this report. **Figure 26** below illustrates respondents’ focus of investment when mitigating cyber security risks, by category.

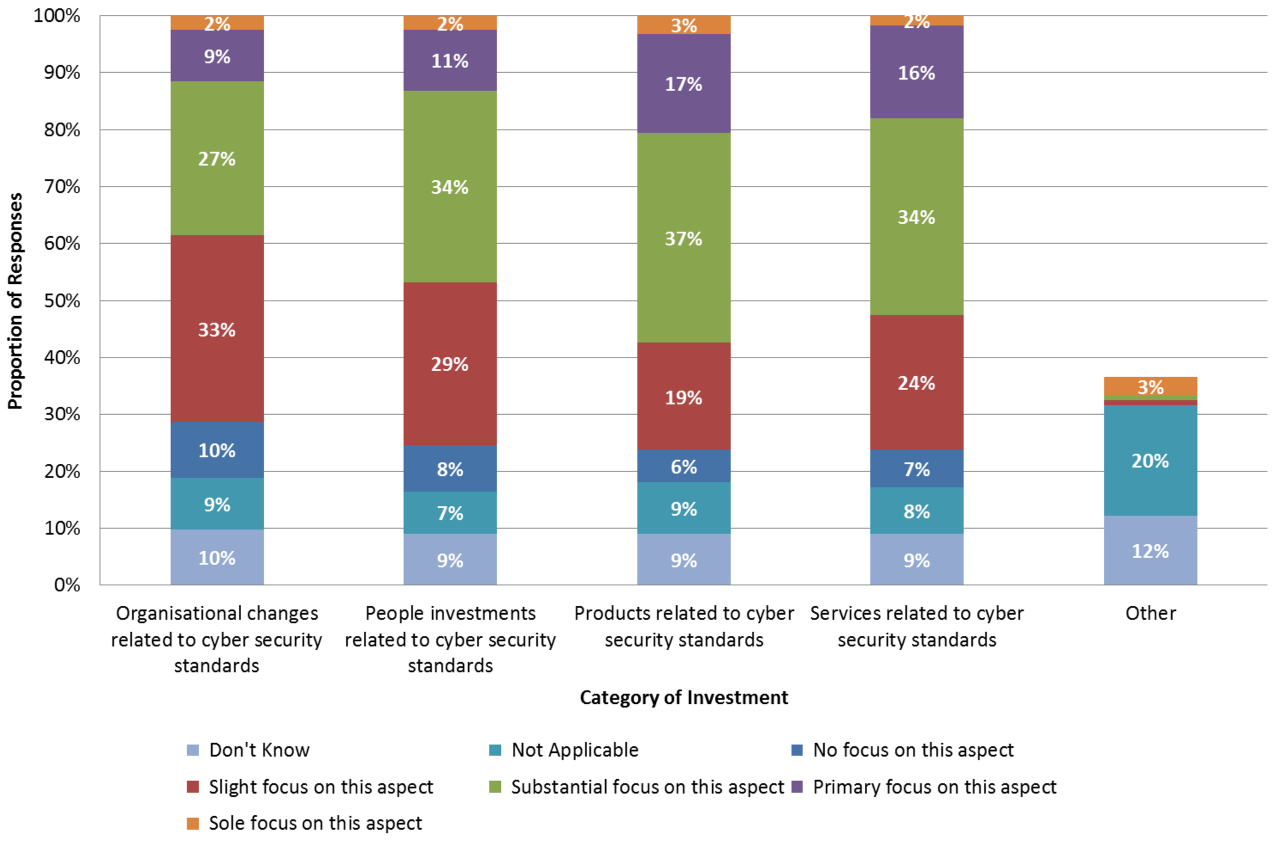


Figure 26: *organisations’ focus in mitigating cyber security risks (based on 122 responses)*

Organisational standards make up for 67% of the standards landscape and yet organisational changes account for the least focus when organisations mitigate cyber risk. This is consistent with Figure 22 and its associated analysis, which is in financial terms. Respondents' organisations have the greatest focus on Products and Services when mitigating cyber security risk.

People standards

Figure 27 shows responses to an online survey question regarding the certifications that respondents' organisations look for when recruiting people into cyber security roles.

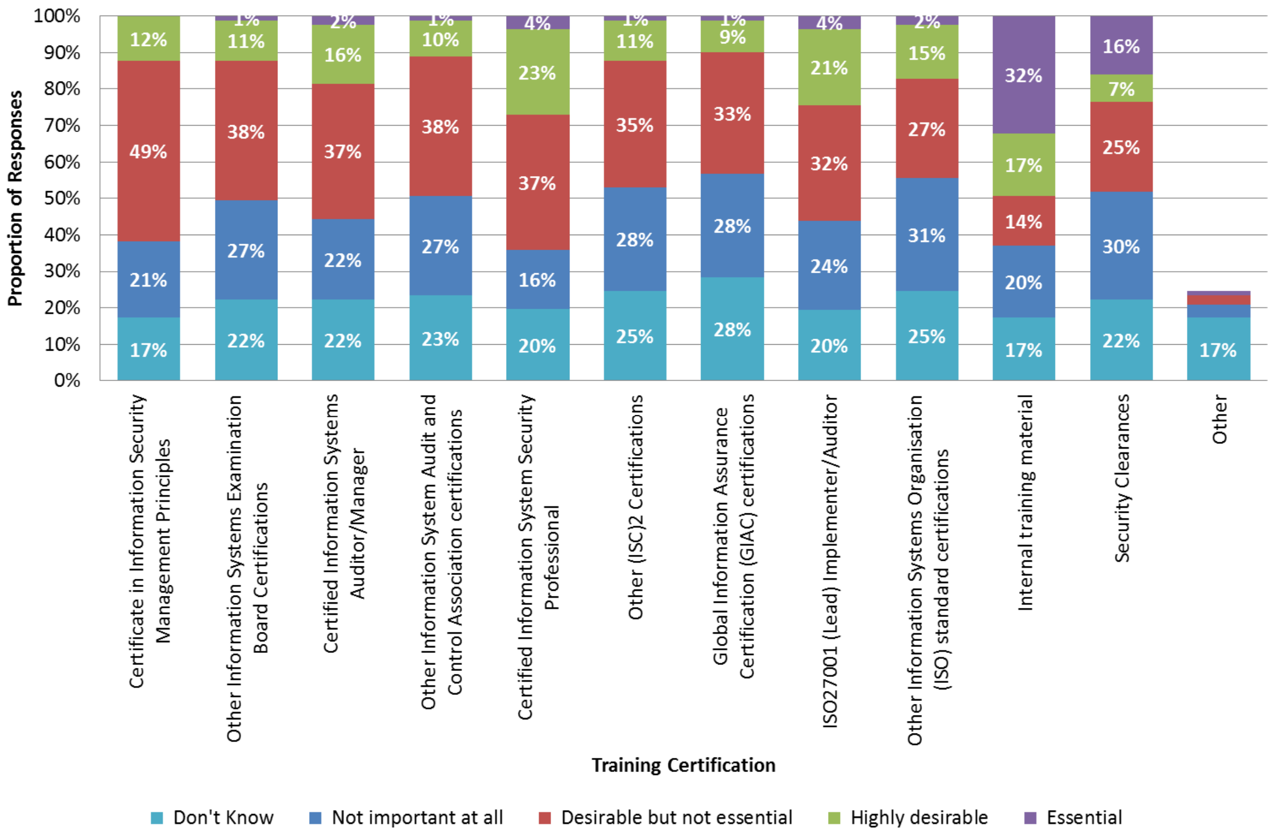


Figure 27: *preferred cyber security certifications when recruiting staff for cyber security related roles (based on 81 responses)*

Nearly half of organisations broadly believe that certifications are not important at all or do not know whether they are desirable or essential for cyber security related roles. When those that do view certifications as important recruit staff into cyber security roles:

- CISSP is the most desirable certification for cyber security staff, with 27% of respondents stating that they viewed CISSP as 'essential' or 'highly desirable'
- ISO27001 qualifications were a close second with 25% stating that they viewed such qualifications as 'essential' or 'highly desirable'.
- 30% stated that security clearances are not important at all; however sector focus is likely to be a factor, with security clearances commonly viewed as important or essential when working for or alongside Government departments.

- 32% see completion of their own organisation's internal training programme as essential, potentially suggesting either greater confidence in the ability of their internal syllabus to meet their needs than those of external certifications; or alternatively, completion of such courses as an exercise in transferring the organisation's vicarious liability to its individual employees.

Figure 28 explores this in more detail, showing the modes of internal training which are deemed most desirable for staff in non cyber security related roles.

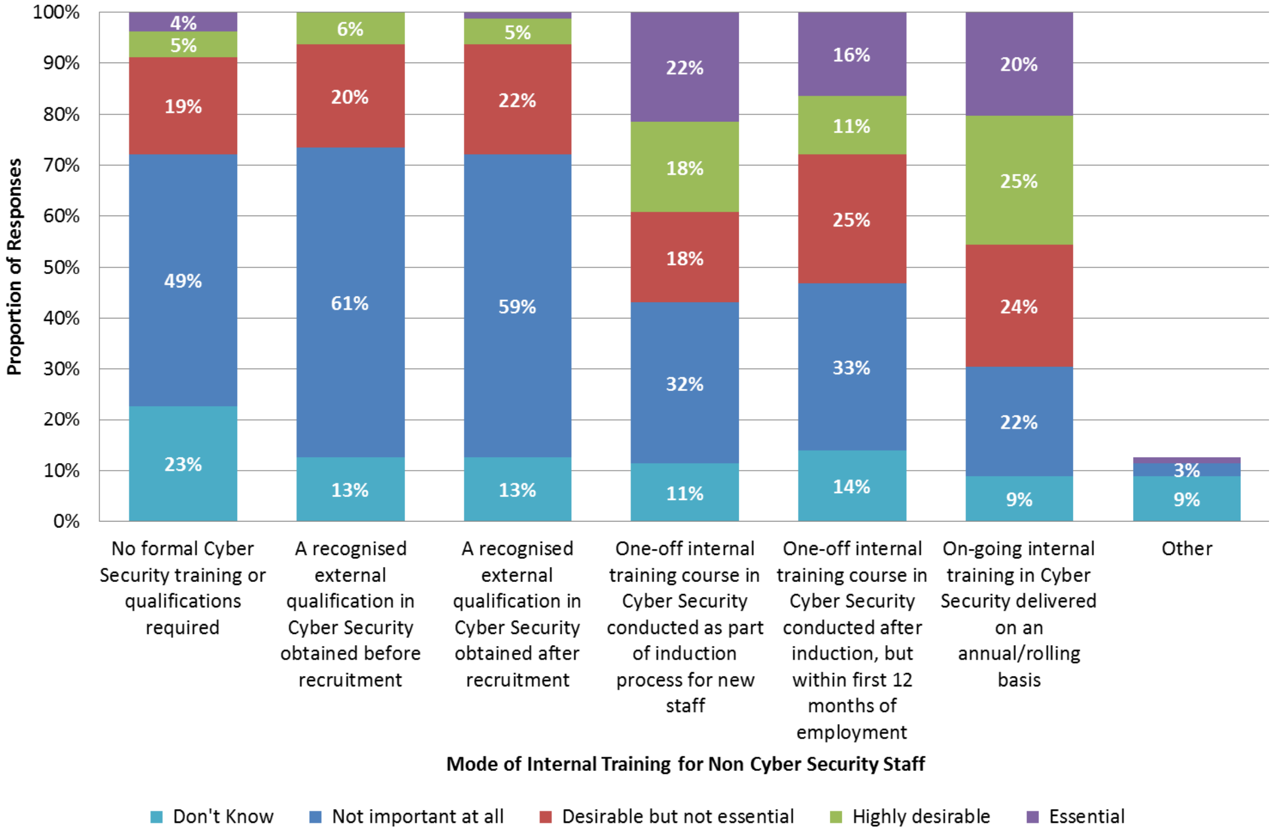


Figure 28: mode and *importance of cyber security training when recruiting staff for non- cyber security related roles (based on 79 responses)*

Notably:

- Only 6% of respondents stated that an external cyber security qualification would be 'essential' or 'highly desirable' for staff in non cyber security roles, either prior to or after recruitment.
- 40% of respondents stated that an internal cyber security training course would be 'essential' or 'highly desirable' for staff in non cyber security roles as part of their induction into the organisation.
- A similar number, 45%, stated that such training would be 'essential' or 'highly desirable' on an annual/rolling basis.

Adoption of standards related to products and services

Interest and investment in cyber security is growing in the UK and as the previous section outlines, organisations are focussed on investment in products and services when mitigating cyber security risk. However, the availability of standards for products and services is relatively low (pages 10 & 11) as is the current adoption of those that are available. As a result this section aims to identify why products and services related standards are adopted as well as why they may not. It will additionally identify what types of products and services receive investment.

Reasons for investment

Figure 29 shows that compliance was the primary outcome for organisations investing in certified products and services.

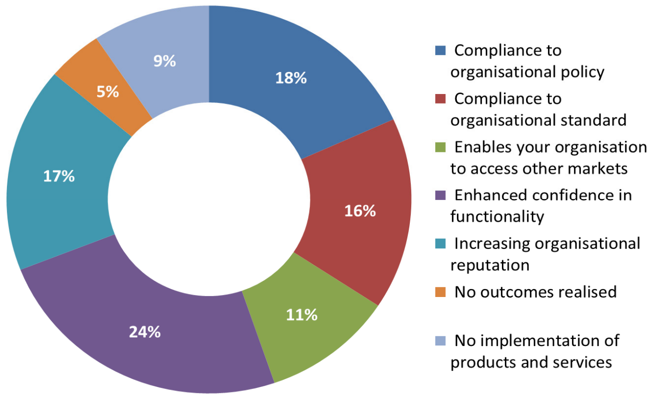


Figure 29: *realised outcomes having purchased or implemented security certified products or services (based on 86 responses)*

34% stated compliance as the main motivator; perhaps suggesting that investment is the result of obligation rather than desire. This was closely followed by 24% claiming confidence in functionality was their main reason to invest. In contrast 5% state they have realised no outcomes at all following expenditure. Whilst this number is small it is important to note as this set of organisations are witnessing no benefit from investment which could reduce level of investments in the future and perhaps explain a part lack in current adoption.

When asked ‘what are your organisation's main criteria when considering investment in products and services’ (based on 66 responses), maintaining data integrity was the main functional criteria for organisations to adopt product and service related cyber standards with 35% (products) and 29% (services) respectively stating this as their main reason to invest. 26% of organisations confirmed protecting customer information as the most important reason to invest in product related standards and 24% agreed this as the case for investing in service related standards. Protecting organisational reputation was the next highly rated motivator to invest in product and service related standards; 25% and 23% of organisations rated this as the greatest stimulant for investment.

Conversely increasing profit margins was the least popular motivator to invest in products and services related standards with only 2% and 5% of organisations respectively rating this as their top motivator for investment. Financial gains from investing in standards are hard to quantify which may be a factor in why organisations deem increasing profit as relatively unimportant when investing in product and service focused standards.

Investment in new technologies

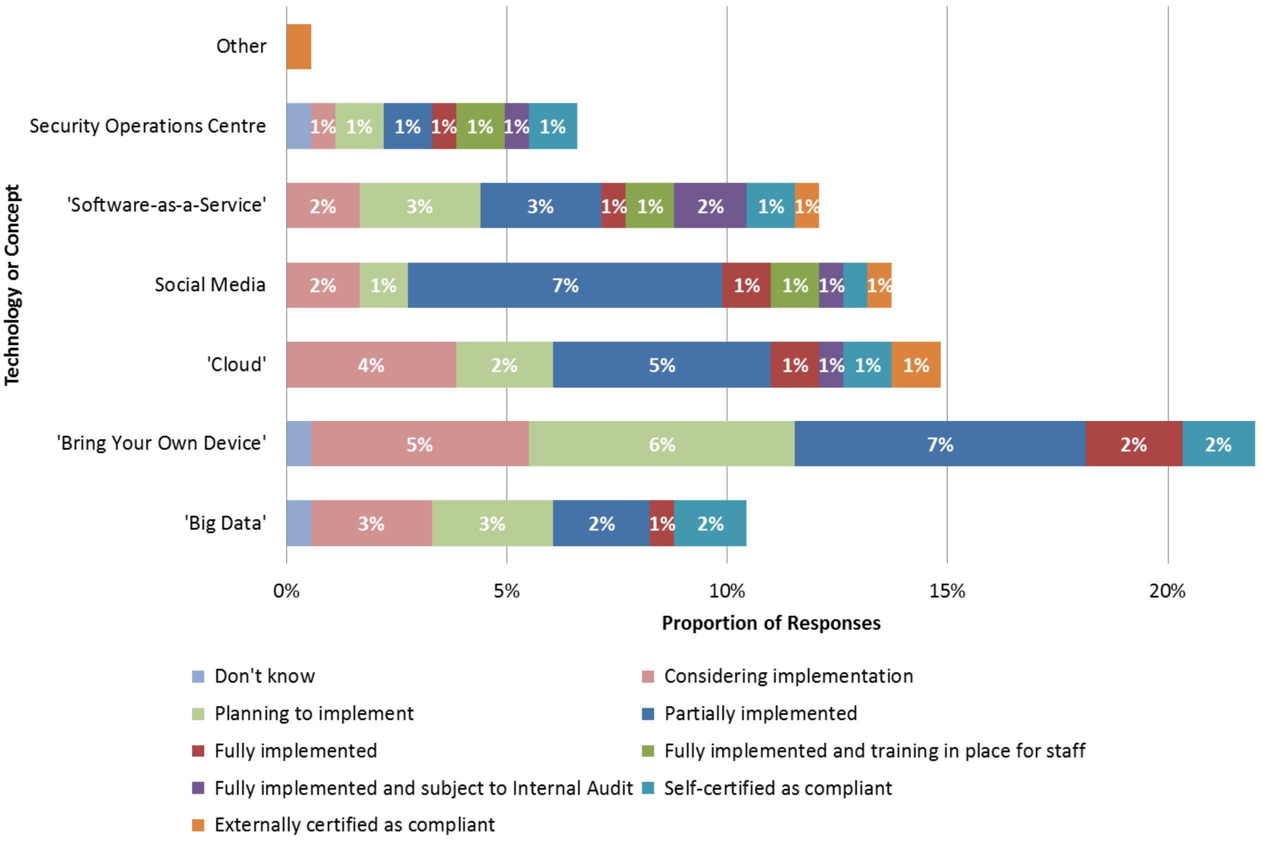


Figure 30: *Level of adoption or consideration for cyber security standards relating to new technologies (based on 78 responses)*

During our research it was important to provide an insight into the appetite for standards in new technologies as these are becoming an increasing focus in the everyday running of organisations in the UK. Bring Your Own Device (BYOD) saw the highest level of investment at 22%, with the greatest level of fully implemented and self-certified organisations. Those that invest in Social media, Cloud and Software in a Service had all gained external certification for compliance while no organisations had done so for BYOD despite this being the most popular standard type.

30% of organisations state relevance and applicability as the most important motivator to invest in new technologies

There was a common factor in constraints for investment in these areas; organisations want to know that a standard relating to a new technology warrants the investment and will be relevant to, and improve, their operational output. Organisations also highlighted that they needed a standard to be relatively easy to install and integrate into their current operational practice. Cyber security technologies need to be user friendly and resource and time agnostic.

1% of organisations felt that investing in new technologies would allow them to compete with other organisations

(based on 65 responses)

22% of organisations felt that price and cost was the main motivator to invest in new technologies

(based on 65 responses)

Alternative approaches to cyber security standards

Having researched the approaches taken by organisations to adopt cyber security standards, a common trend was identified: that many organisations consider investment in protection from cyber security threats more important than implementation of standards and certification. This section investigates the alternative approaches taken by organisations to mitigate cyber risk and protect themselves from cyber security threats so that the motivations and potential incentives may be identified.

Figure 31 illustrates the changes made by organisations in the past 12 months as well as the changes they plan to make over the next 12 months and beyond. Implementation of business continuity plans appear to have been the most popular change (51%) to have occurred in the past 12 months with the creation of new organisational policies following closely behind at 48%. This seems to support the view identified from the interviews, and mentioned in the paragraph above, that internal controls and management are currently deemed more useful and relevant than investment in complying to standards or achieving certification.

This trend changes slightly when looking out to the next 12 months and plans organisations have to develop in cyber security. 33% state that they intend to develop a form of information security management system in accordance with a standard while 39% confirm that they intend to pursue certification to at least one standard, arguably showing that there is indeed an appetite for cyber security standards going forward.

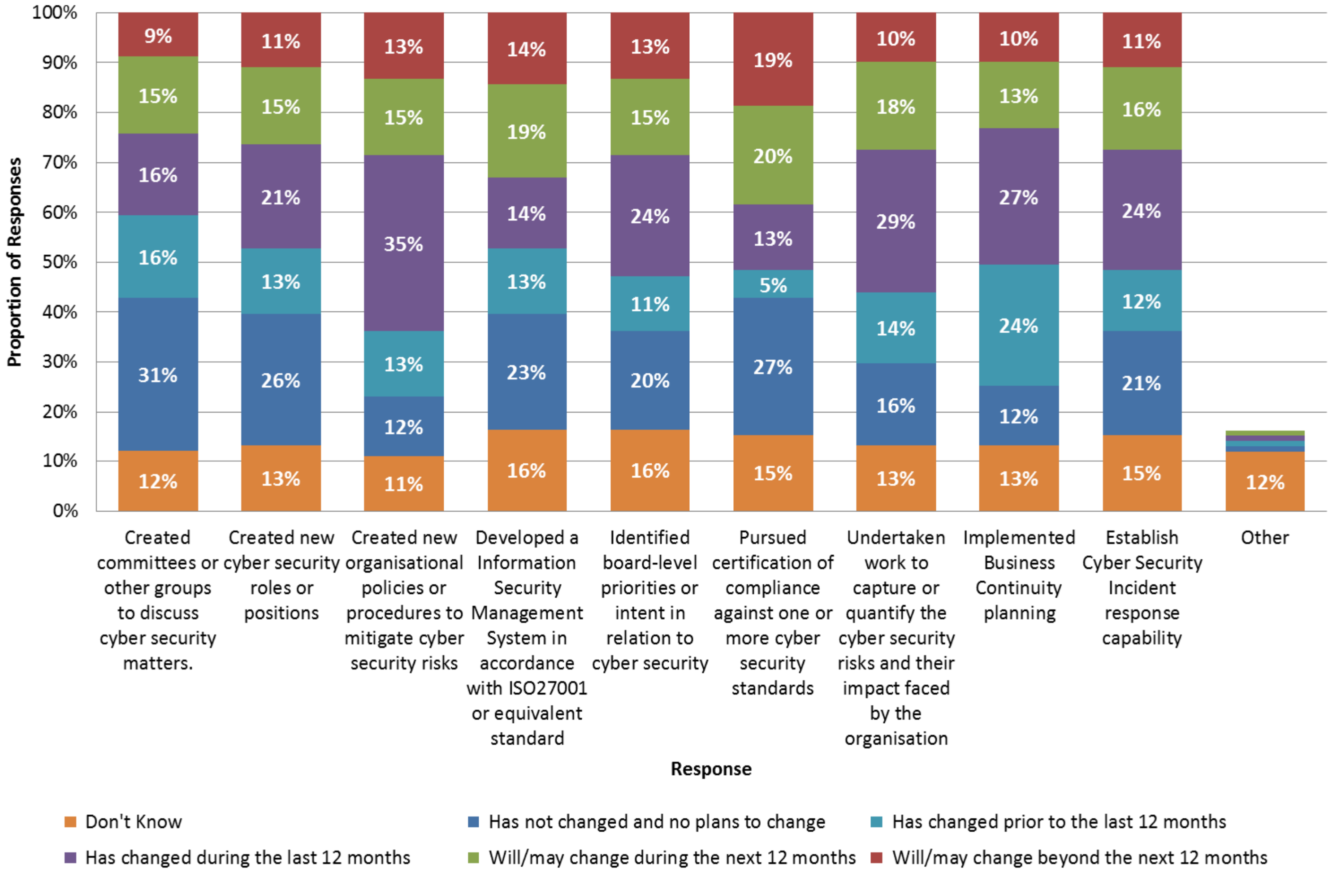


Figure 31: *how organisations have adapted to respond to cyber security challenges (based on 91 responses)*

Further focus on this subject via interviews suggested that despite a perceived increase in appetite and awareness of cyber security risk, there is concern surrounding what or how best to invest in protection against it. As this research highlights, there are numerous publications offering frameworks and controls but a common view is that guidance on the implementation of these various approaches and an idea of 'what good looks like' is missing from the market. This view was particularly strong from small organisations who lacked the internal knowledge to implement an appropriate approach but also lacked the budget to invest in consultants or similar external assistance.

Many larger organisations seem to be increasingly taking a more collaborative approach to cyber security, with the use of third party suppliers to share or transfer the associated risk. There was an accompanying concern however that this approach devalued the importance of cyber security within the organisation and prompted a culture of 'out of sight, out of mind' amongst senior management.

Market drivers for standards adoption

This section concentrates on the market drivers for UK organisations to invest - or not - in cyber security standards based predominantly on the responses from interviews conducted with industry and supported by the research and survey data conducted in parallel. It outlines some of the perceived gaps in the market at present and highlights the constraining factors that may prevent organisations from investing. It also looks at evidencing reasons for investment and the potential incentives.

Current Gaps

- Global organisations, particularly those that operate in a variety of markets, are finding increasing issues with data sharing internationally. This is mainly manifested by the range of differing legislative requirements from nation to nation as well as the complete lack of awareness of risk posed in this area by others.
- There are few cyber security standards relating to products and services as well as a lack of assured products and services available in the UK market. Some organisations are concerned this leaves them to function at risk or mitigate these risks at cost to themselves.
- A perceived lack of information and guidance relating to the implementation of standards as well as a lack of clarity on what standards to comply with to best suit their organisational demographic and needs.
- The lack of mandate or legislation of cyber security for organisations means a lack of incentive to invest for many organisations who find it difficult to identify a business case to do so.
- Many organisations (specifically small and medium sized) struggled to know what standard or guidance to refer to for 'best practice' as the industry is overwhelmed in certain areas – specifically organisational related standards and significantly underwhelmed in other types such as products, services and people.
- There was some awareness of the Government's '10 steps to Cyber Security' guidance particularly from medium sized organisations however an increasing appetite for implementation guidance of these steps was presented throughout this research.
- In terms of new technologies, Bring Your Own Device is the main area for many organisations to focus investment, due to the high levels of adoption of this service. However a lack of clear direction of 'best practice' leaves many organisations unsure of the right approach to take to minimise the associated risk.

Motivators

When looking at what has motivated those organisations who have invested in cyber security standards it was clear (at 24%) that the prevention of an internal breach is the primary motivator attributed to this investment, particularly in organisational standards. However, through interviews it became apparent that while prevention of an internal breach drives this investment, many organisations held concerns that a standard would not necessarily be their first choice to invest in and is more a desirable addition to other controls.

In regards to people related standards, preventing an internal breach was again cited as a main motivator (24%) as well as protecting of customer information (20%). This could suggest that organisations understand the importance of cyber security controls relating to their people and the protection against internally sourced issues.

The motivations start to change when looking at products and services. Investment in product related standards tend to be motivated by maintaining protecting customer information (20%) and data integrity (17%), therefore potentially suggesting a focus on business and customer facing drivers.

Service investment related motivations have a different focus in that they are motivated primarily by compliance with laws and regulations (11% as a main motivator but 32% when focussed on overall motivators) and the protection of own and customer interests (27%). This looks to support similar findings within this report that the use of services tend to aim at transferring or reducing risk through reliance on a third party supplier and ensuring that this service provides compliance for the organisation.

Based on the question ‘what are your organisation's main motivations for investing in cyber security standards compliance?’, receiving 74 responses.

Incentives

The incentive to implement organisational standards is split between a proactive and a reactive stance across the sample. Proactively, 10% of organisations would or have implemented organisational standards as a result of identifying a perceived risk to the organisation. Reactively, 37% would or have implemented organisational standards as a result of the organisation experiencing a cyber security breach. People standards implementation is heavily weighted (43%) to a reactive approach once the organisation has experienced a cyber security breach.

Based on the question ‘what changes or events would incentivise your organisation to invest (further) in cyber security standards?’, receiving 60 responses.

Products and services standards had a broader range of incentives driving their implementation. In addition to perceived risk and reaction to a breach as with organisational and people, products and services were also incentivised by customer demand for them and the ability to secure a business case for their investment. This may suggest a perception that products and services are easier to define the earned value or a return on the investment.

The incentive statistics above provide more of a forced incentive than those desired or attractive to an organisation. As part of the interview process, interviewees were asked to discuss the factors that would incentivise their organisation to invest in cyber security standards of some sort. The following bullet points highlight the common responses:

- Affordable certification achieved through a range of standards that provide a suitable option for the companies needs at a representative price.
- Clear articulation of the return on investment for cyber security standards.
- Clear guidance on how to achieve internal implementation of the right standard.
- Access to new markets and customers through the attainment of certification

Barriers and constraints

Data from the interviewees and online survey identified a variety of reasons that begin to explain why compliance to cyber security standards lack within some organisations in the UK:

- Sub optimal level of awareness of the associated risk
- Cost and difficulty to calculate return on investment
- A lack of incentive or clear business case to invest
- Affordability of standards compliance and certification
- Small organisations generally felt their footprint wasn't big enough and didn't carry enough risk to warrant an extensive expenditure in cyber security standards
- Some large organisations felt that compliance to standards was not the most important indicator in justifying their operational success in cyber security.
- Lack of management direction and suitable support from executive boards
- Global organisations feared that legislating standards could slow down operational output as the process to constantly remain current could be exhaustive and counterproductive in protecting their organisations assets from cyber threats.
- Resource intensive to implement

46% of organisation felt the cost of people standards prohibited investment

15% of organisations felt that it was too hard to calculate a return on the investment and therefore acted as a constraining factor

Annex A – Survey and Interview Approach and Demographics

Survey approach

- The survey took approximately 20 minutes for respondents to complete and was circulated via the PwC Network, BIS Local network and social media and the internet. In order to maximise the response rate and reduce burden on respondents, it was broken down into 4 separate sections with the ability to save and return at a more convenient time. Section one focussed on the demographics of the responding organisations; whilst the second section focused on the standard adoption and approach to cyber security. The remaining 2 sections focused on motivating and constraining factors for cyber security investment.

- In total there were 243 respondents. As with any survey of this kind, we would not necessarily expect every respondent to know the answers to every question. It also needs to be considered that due to time constraints the survey was run from August to -mid September 2013, which could have contributed to a low response rate. For presentational reasons we have removed 'don't know' and 'not applicable' responses from most graphs however if the proportion of 'don't know' answers were significant we have referred to this in the graph or accompanying text.

- The number of responses varied significantly by question, so we've included against each figure in the report the number of responses received.

- The survey was targeted at senior individuals within an organisation responsible for cyber security, IT, risk, or compliance as applicable. Figure 31 below illustrates the sample.

- In terms the strength of the statistical conclusions drawn in relation to the survey data collected the following points need to be considered:

  1) The survey is based on self-selection and therefore, some of the results could potentially be biased. The reason for this is mainly that companies with a particular interest in cyber security (i.e. for example those that have recently suffered from a cyber security incident) are possibly more likely to respond. This can in particular affect results where the number of respondents is particularly low. The extent or direction of this potential bias though is unfortunately not known. Hence the information presented in this report should be seen as more indicative of business views in relation to cyber security standards.

  2) Furthermore, it should be borne in mind that the survey results are not necessarily representative of the UK economy. A good spread across sectors and across company sizes was achieved in the survey but due to the small sample size and the fact that the survey was based on self selection implies that it unfortunately cannot be seen as representative.

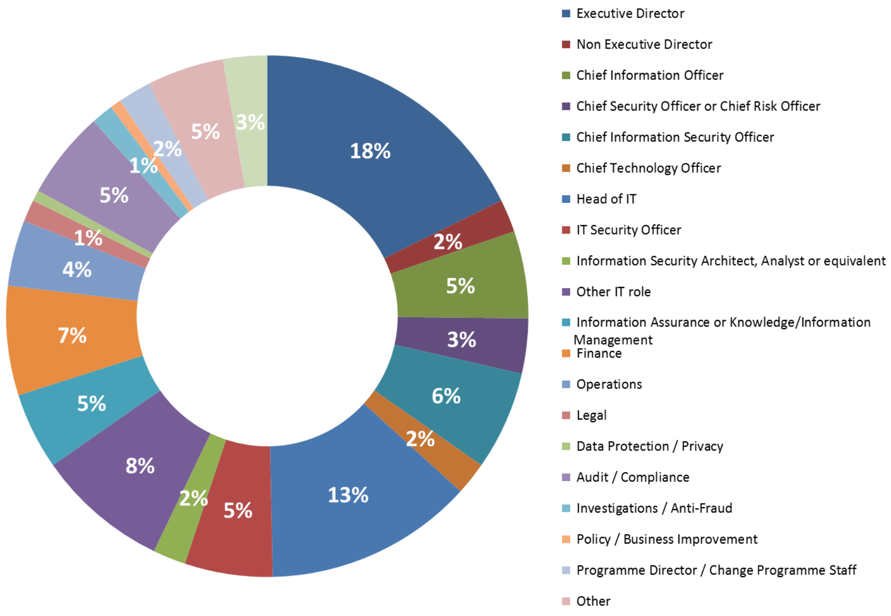


Figure 32: *respondent's role titles (based on 147 responses)*

Interview approach

- The interview samples breadth covered 15 industry sectors, aligning to those in the online survey as illustrated in Figure 2.In terms of depth, the sample ranged from interviews with start up's and SME's through to global organisations. Interviews were arranged through the PwC network. In total, 20 interviews were conducted.

- Interviews were generally 30 minutes respectively and were specifically pitched at Information Security professionals across the UK sectors in large, medium and small organisations.

- The questions focused on gaining a better understanding of what cyber security standards organisations invest in and the main motivators and constraining factors to this. Additional questions focussed on what could be done to improve cyber security awareness and compliance in the UK and specifically within sectors.

Annex B – High-Level Mapping Definitions and Dimensions

Cyber security standards landscape approach and definitions

In order to identify the cyber security standards landscape the following approach was chosen:

- Firstly, identification of the scope of the landscape – i.e. identify which individual standards fall within the landscape and which do not.
- Secondly, the mapping of these ‘in scope’ standards against a number of relevant dimensions.

There are a number of prerequisites to be fulfilled before the scope of the cyber security standards landscape can be identified.

Definition of ‘cyber security’

There are a multitude of terms in general use that relate to the broad set of concepts covered by this report. For example, ‘cyber security’ is sometimes used interchangeably with terms such as ‘IT security’, ‘computer security’, ‘data security’ or ‘information security’; but sometimes these terms can convey subtly different meanings depending on the context and the identities of both writer/speaker and reader/listener. This is particularly pronounced where practices vary according to the medium in which specific types of information are stored, processed or conveyed.

The word ‘security’ may also be supplanted by more loaded terms such as ‘assurance’, ‘superiority’ or ‘dominance’ where the writer means to convey a level of maturity or sophistication alongside identifying the subject matter.

This report, and its associated surveys and interviews, use the term ‘cyber security’ exclusively throughout. The meaning of cyber security in this context is defined as follows:

> *‘Cyber security’ is ‘the preservation of confidentiality, integrity and/or availability of information in cyberspace.’*

Where ‘cyberspace’ is defined as follows:

> *‘Cyberspace’ is ‘the complex environment that results from the interaction of people, software and services on the Internet by means of the technology devices and networks connected to it, which does not exist in any physical form.’*

Note that for the purposes of this document, certain components of cyberspace such as routers and cabling do exist in physical form.

Approach for identifying publications within the landscape

This report will take a similar approach to identifying publications to map against the cyber security landscape as an individual who was responsible for (or at least interested in) improving cyber security within their organisation might take. Specifically, the means by which such an individual might identify cyber security publications for their organisation to consider adopting include:

- **Performing an Internet search.** The landscape mapping exercise will replicate this avenue of research by mapping any publications referred to within the first 30 results returned by the search strings “cyber security standard” and “information security standard” on a popular Internet search engine; and any publications that are linked to the sites returned in the first 30 results. Note that any such publications must pass a relevance test to confirm they are relevant to the field of cyber security.

- **Referring to colleagues or other people responsible for cyber security within their industry.** The landscape mapping exercise will replicate this avenue of research by mapping any and all relevant publications to the landscape that are mentioned by 10 or more online survey respondents or one or more face-to-face interviewees.

Note that overly-specific ‘single issue’ publications were excluded from the landscape where they were deemed to be of limited relevance to the broader cyber security community. For example, one interviewee suggested that IEC61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) was included within the landscape. On close inspection however, this standard was determined to be a means for expressing ‘Mean Time Between Failure’ (MTBF) requirements for safety-critical systems. While cyber security may be a factor affecting the availability and thus MBTF for such a safety-critical system, IEC61508 does not provide any guidance as to how to quantify, mitigate or manage such risks.

Granularity at which publications are mapped

A number of the publications identified for potential placement on the cyber security standards landscape are not individual documents, but are series or ‘families’ of documents. Some of these series are extremely large; for example, the European Telecommunications Standards Institute (ETSI) has published several thousand technical standards in the telecommunications area, of which 425 are flagged with the metadata keyword “security”.

Mapping each of the individual publications within these series would result in the large cyber security standards landscape becoming extremely large; disproportionately so for the purposes of this report. Families of documents have therefore not been broken out into their constituent individual publications unless:

- The individual publication was returned by the initial Internet search, rather than the broader family of documents of which it is a constituent part.

- Ten or more respondents to the online survey mentioned an individual publication within a broader family of documents, rather than identifying the broader series directly.

- One or more face-to-face interviewees mentioned an individual publication within a broader family of documents, rather than identifying the broader series directly.

Note that an intermediate step was taken whereby broad series of publications were broken out into a number of sub-series where this was proportionate (i.e. where there are no more than 10 such sub-series within a series) and informative (i.e. where breaking series out into sub-series in such a manner reveals variation in mapping against the dimensions described below)

Standards category definitions

The following definitions explain the meaning of the Organisational, People, Product and Services categories in the paper.

Category	Definition
Organisation	Publications that relate to how an organisation is structured, and the way in which an organisation governs, manages and reports cyber security matters. Such publications may also define the level of cyber risk management that an organisation should reach in order to be viewed as a trusted or cyber secure business. This is applicable to both suppliers and buyers of cyber security solutions, and such publications will be applicable to the enterprise and operational sides of the organisation. Such publications may specifically relate to: • The creation of new cyber security-specific posts within an organisation. • The creation of new cyber security-specific reporting lines between people within an organisation. • The creation of committees or other groups within an organisation to discuss cyber security matters. • The creation of processes to make cyber security-specific decisions, such as risk acceptance decisions or operational decisions such as taking a system or service offline, within an organisation.
People	Publications that relate to people, how much trust is placed in them and how they undertake their roles. This may include definition of skills and competence levels for cyber security roles; but may also include cyber security awareness training for non cyber security roles within an organisation. Such publications may also relate to: • Segregation of duties between people within an organisation. • The definition of people's roles or functions within an organisation. • The qualifications which people are required to have within an organisation. • The raising of people's competence levels within an organisation through training or awareness campaigns.

Category	Definition
Products	Publications that relate to capabilities that are primarily delivered by technology. Cyber security standards for such products could: • Assure the implementation of products designed to secure a technical service. • Assure the implementation of non-security products so as not to undermine the security of a technical service of which it forms a part (these cyber security components of a broader service are termed as ‘derived security requirements’). • Assure a technical service as a product in its own right (for example, cloud services). Note that products may be implemented in hardware and/or software. Note also that the meaning of ‘products’ in this context does not necessarily relate to products that the adopting organisation manufactures or sells; it could equally apply to products that the organisation utilises to produce goods for sale.
Services	Publications that relate to solutions delivered primarily by people, and may be known as professional services. Cyber security publications for services should identify current best practice in professional cyber security services, and may include: • The formal certification of training providers, Academic Centres of Excellence, training and education courses. • Cyber security services, such as penetration testing. • Secure product (e.g. software) development. • Secure system design (e.g. security architecture). • Other cyber security-related consultancy services. Note also that the meaning of ‘services’ in this context does not necessarily relate to services that the adopting organisation offers to others; it could equally apply to services that the organisation consumes in the course of its business operations or change programmes.

Nature definitions

This report uses the following 7 definitions for the 'nature' of each publication:

Nature	Definition
Publication	A cyber security document, family of documents or other similar artefact(s) that individually or collectively impart knowledge of how cyber security might be managed from its author to the reader. Publication is an abstract term used to refer to each of the 6 specific publication types defined immediately below in the generic (i.e. agnostic of whether the publication is a standard, framework/methodology, maturity model, certification, guidance or legislation).
Standard	A publication which details a series of unambiguous mandatory criteria that the target of the standard must achieve in order to be certified as meeting it. The target of the standard may be an organisation, a person (in the abstract), a product or a service. The criteria in the standard's specification are likely to be primarily objective as opposed to subjective; and quantitatively or qualitatively measurable in nature. Standards typically state what 'must' be done rather than 'may' or 'might' be done. Standards can be readily audited against, with non-conformities easily identified.
Framework / Methodology	A proposed approach to ensuring cyber security; perhaps aligned to other broader topics such as IT project management or IT governance. A framework/methodology outlines the indicative considerations to be weighed, the decisions to be made and perhaps the artefacts to be generated; but provides no definitive, objective and mandatory criteria by which to measure and test achievement. It serves as a (often sequential) aide-memoire that can be tailored by adding or removing elements as required, making it impractical to audit against.
Certification	A certification is a scheme or process that enables an accreditation body to accredit an organisation, person, product or service as providing a recognised level of capability and/or meeting a recognised quality benchmark. It differs from a standard in that certification may be based on documentation that is not available to the subject of the certification, and may include a level of judgement by the accreditation body as to what should be tested and whether the subject's response is acceptable or not. For the purposes of this report, certification may fall into one of two spaces: 1. **In relation to People.** A certification in this sense is a measure of assurance that a given individual is capable of performing a specific role or function. It is usually granted and recorded by a professional membership body, and often comprises elements beyond that of an attendance based-training course. For example, it could additionally require the person seeking certification to pass an examination; meet a minimum experience requirement (often expressed in hours or years); pass a viva (or similar professional interview); complete a practical exercise; undergo an observational assessment; and/or pass an unannounced 'spot-check'. 2. **In relation to Products or Services.** A certification in this sense is a measure of assurance that a given product or service is capable of performing a specific role or function. It is usually granted and recorded by an accreditation body that is trusted to grant such accreditations within a specific industry or field. It often comprises non-destructive and/or destructive testing whereby the accreditation body tests the product or service's ability to deliver the capabilities asserted by its manufacturer or service provider.

Nature	Definition
Maturity Model	Enables the reader to benchmark where their organisation falls on scale of cyber security maturity across a number of different domains or dimensions. It is a tool that allows organisations to be benchmarked against their competitors or peers. It may provide the reader with an indication as to the improvements that would need to be demonstrated in order to move up the maturity scale, but it is unlikely to provide any definitive, comprehensive or testable direction for what needs to be done to ensure this.
Guidance	Offers advice and recommendations, as opposed to setting mandatory criteria. Guidance publications often list considerations that need to be weighed, and propose potential or ‘default’ solutions to common problems. They typically state what the reader/target of the guidance ‘may’ do rather than what it ‘must’ do. Since its suggestions are optional and/or subjective, compliance with guidance is difficult to audit against. Guidance may be standalone, however often supplements or accompany a standard in order to assist the reader of the whole.
Legislation	Likely to be imposed by government or other sovereign entity as law, making adherence mandatory for entities within the legislation’s scope. Legislation is often linked to the geographical location and/or the nationality of the target. Its instructions are mandatory, and are more likely to state negative requirements than other types of documents, dictating what ‘must not’ be done. Very little is usually left to the reader’s discretion. Legislation is novel within this analysis in often stating penalties for non-compliance, which can be severe.

These natures are intended to be mutually exclusive; however there are a small number of instances where individual publications are of one nature and their annexes or other complementary artefacts are of another. Similarly, some families of publications have constituent individual publications of multiple natures. Such publications or families of publications are mapped against all the natures to which they correspond.

Dimensions against which publications are mapped

Publications identified as falling within the scope of the cyber security landscape will be mapped against the dimensions indicated in the table below. Each dimension represents one or more items of metadata that will be gathered in relation to each publication.

Dimension	Possible Values	Mutually Exclusive?	Description/Rationale
Publication nature	• Standard • Framework / Methodology • Certification • Maturity Model • Guidance • Legislation	Yes; except where publications and their annexes are of different natures, or where families of publications have constituent individual publications of multiple natures.	Not all publications within the scope of the identified cyber security landscape are standards in the strictest sense of the term. Differentiating between publications of different natures may be useful in determining whether lack of auditability is a barrier or incentive to adoption.
Content category	• Organisation • People • Product • Service	No.	This dimension may show variation in coverage by subject matter within the cyber security standards landscape.
Target industry sector	• All / Sector Agnostic • Financial Services (including insurance) • Medical / Healthcare • Telecommunications • Energy (extraction or distribution/supply)	Yes.	This dimension may show variation in coverage of subject matter specific to individual industries within the cyber security standards landscape. Flagging publications by industry sector may enable conclusions to be draw as to whether any sectors may have a greater level of maturity in their cyber security coordination, and thus potentially serve as exemplars for other sectors. (Note that the limited range of possible values defined here are as a result of the majority of industry sectors not having any sector-specific cyber security publications.)

Dimension	Possible Values	Mutually Exclusive?	Description/Rationale
Product type	• Encryption Technologies • Telecommunications & Channel Management • Perimeter Defence • Network Access Control • Identity & Access Management (IAM) • Inventory, Configuration & Patch Management • Device Management (Anti-Malware & Anti-Virus) • Security Incident & Event Management • Data & Data Loss Prevention • Operating System & Server Applications	No.	This dimension may show variation in the types of products covered by cyber security publications with a content category of type 'product'. Definitions of each product type follow this table.
Service type	• Security Governance • IT Risk Management • Audit & Compliance • Security Training • Design & Architecture • Software Development • Configuration & Implementation • Security Operations • Incident Response & Crisis Management • Business Continuity & Disaster Recovery	No.	This dimension may show variation in the types of services covered by cyber security publications with a content category of type 'service'. Definitions of each service type follow this table.

Dimension	Possible Values	Mutually Exclusive?	Description/Rationale
Relevance	• Directly security related • Has security elements • Not directly security related	Yes.	This dimension may show variation in the focus of the publications referred to during the survey and interview phases supporting this report.
Prevalence	• Number of online respondent mentions • Number of face-to-face interviewee mentions • On first three pages of Internet search results	No.	This dimension may show variation in market awareness between publications.
Language	• Current version in English • In English, but lags by >24 months • Not available in English	Yes.	This dimension may show variation in region applicability / availability between publications.
Classification	• Not classified / protectively marked • Classified / protectively marked	Yes; except where some publications or their annexes are classified and some are not.	This dimension may show variation in the availability of publications to the private sector due to their government classification.
Status	• Released/available • 50% of more in draft • 50% or more revoked	Yes.	This dimension may show variation in the availability of publications to the private sector due to their status (being in draft or revoked).
Currency	• Current • 50% or more superseded	Yes.	This dimension may show variation in the availability of publications to the private sector due to their currency (being superseded).

Dimension	Possible Values	Mutually Exclusive?	Description/Rationale
Agedness	• Not aged • Aged Note that 'agedness' is determined by comparing the publication's year of last revision with a agedness threshold. For the purpose of this research, any publication last revised prior to 1st January 2003 (i.e. more than 10 full calendar years ago) is regarded as aged.	Yes.	This dimension may show variation in the perceived relevance of publications by the private sector on account of their agedness.
Audience	• Adopters • Certification Bodies / Auditors / Testers	No.	This dimension may show variation in who the intended audience of cyber security publications.
Origin	• UK Government • International • Foreign Government	Yes.	This dimension may show variation in the origin of publications, from which it may be possible to infer how localised they are.

Product type definitions

Product Type	Definition/Scope
Encryption Technologies	All encryption methodologies and technologies; covering data in transit and at rest, key management and encryption protocols etc.
Telecommunication & channel management	All telecommunication channel (analogy, 3G, 4G, wifi, blue tooth, NFC, Ethernet etc.) methodologies and technologies; covering channel management, pairing agreements, promulgation, bandwidth and protocols etc.
Perimeter Defence	All methodologies and technologies employed to define and defend networks; covering intrusion detection and prevention technologies (firewalls), denial-of-service, load balancers and internet filtering and scanning services etc.
Network Access Control	All network (wired or wireless) network access control methodologies and technologies, including their management.
Identity & Access Management	All authentication and authorisation methodologies and technologies; covering account and privilege management and account and access monitoring etc.
Inventory, Configuration & Patch Management	All methodologies and technologies to identify and manage devices on the network; covering the deployment of operating system and application patches, audit and compliance with configuration standards and policies etc.
Device Management (anti-malware & anti-virus)	All methodologies and technologies designed to maintain the integrity of hosts (devices); including configuration policy management, local privilege management, code execution etc.
Security Incident & Event Management	All methodologies and technologies for the collection, monitoring and analysis of network and host activity for security events.
Data & Data Loss Prevention	All methodologies and technologies that assist in the management of information, that resides on the network and its devices. Covers: data classification, sanitisation, distribution and destruction.
Incident Investigation & Forensics	All methodologies and technologies to investigate and obtain information on security events and incidents.

Service type definitions

Service Type	Definition/Scope
Security Governance	To develop information security strategies and policies, oversee their application. To define and set the organisations information technology risk appetite.
IT Risk Management	To assess and quantify the level of information security risk.
Audit & Compliance	The independent assessment of the levels of compliance to the stated polices and standards.
Security Training	User awareness and security professional, training and development.
Design & Architecture	Advice and assistance to design secure systems and solutions.
Software Development	Advice and assistance to build secure software, best practices and a Secure Software Development Lifecycle (SDLC).
Configuration & Implementation	Advice and assistance to build and implement secure systems and solutions.
Security Operations	Advice and assistance to manage the day-to-day security function and services.
Incident Response & Crisis Management	Advice and assistance to respond to security incidents and to provide assist with crisis management. (Public relations, legal advice etc.)
Business Continuity & Disaster recovery	Advice and assistance to develop Business Continuity and Disaster Recovery strategies, policies and process.

NOTE – This page is intentionally left blank. Annex continues on the following page.

Annex C – High-Level Cyber Security Landscape (Tabulated)

Ref	Publication	Publication Nature						Content Category			
		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation / Regulation	Organisation	People	Products	Services
1	American National Standards Institute (ANSI) X9 series	x				x		x		x	
2	Australian Defence Signals Directorate (DSD) Information Security Manual (ISM); formerly known as "ACSI33"	x						x			
3	Basel II						x	x			
4	BITS Shared Assessments	x						x			
5	BS 10008:2008 Evidential weight and legal admissibility of electronic information	x						x			
6	BS25999 Business Continuity	x						x			
7	Bundesamt fur Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security '100 Series'					x		x			
8	Carnegie Melon Capability Maturity Model (CMM)				x			x			
9	CESG Assisted Products Service (CAPS)			x						x	
10	CESG Information Assurance Standards (ISs/IASs) and associated supplements	x						x	x		
11	CESG Tailored Assurance Service (CTAS)			x						x	x
12	Cyber Defence Capability Assessment Tool (CDCAT)		x		x	x		x	x		
13	European Telecommunications Standards Institute (ETSI) Publications - European Standards (EN) series - tagged with keyword 'security'	x				x				x	x
14	European Telecommunications Standards Institute (ETSI) Publications - (Interim) European Telecommunication Standards (ETS/I-ETS) series - tagged with keyword 'security'	x				x		x		x	x
15	European Telecommunications Standards Institute (ETSI) Publications - ETSI Standards (ES) series - tagged with keyword 'security'	x	x			x				x	x
16	European Telecommunications Standards Institute (ETSI) Publications - Technical Specifications (xTS/xGS) series - tagged with keyword 'security'	x				x				x	x
17	European Telecommunications Standards Institute (ETSI) Publications - ETSI Guides (EG) series - tagged with keyword 'security'					x				x	x
18	European Telecommunications Standards Institute (ETSI) Publications - others tagged with keyword 'security', including: (x)TR series - Technical Reports (x)SR series - Special Reports (x)TBR series - Technical Basis for Regulation NET series - Norme Europeenne de Telecommunication MI series - Miscellaneous Work Item AN series - Advisory Note					x		x		x	x

Target Industry Sector					Product Type										Service Type									
All / Sector Agnostic	Financial Services (including Insurance)	Medical / Healthcare	Telecoms	Energy (Extraction and/or Supply)	Encryption Technologies	Telecommunications & Channel Management	Perimeter Defence	Network Access Control	Identity & Access Management (IAM)	Inventory, Configuration & Patch Management	Device Management (Anti-Malware & Anti-Virus)	Security Incident & Event Management	Data & Data Loss Prevention	Operating System & Server Application	Security Governance	IT Risk Management	Audit & Compliance	Security Training	Design & Architecture	Software Development	Configuration & Implementation	Security Operations	Incident Response & Crisis Management	Business Continuity (BC) & Disaster Recovery (DR)
	x				x																			
x																								
	x																							
	x																							
x																								
x																								
x																								
x																								
x					x	x	x	x	x				x	x										
x																								
x						x	x										x							
x																								
x					x	x			x													x		
x						x		x	x				x		x		x		x					
x					x	x		x											x					
x						x			x										x				x	
x					x	x											x			x			x	
x					x	x			x						x	x	x		x					

Ref	Publication	Publication Nature						Content Category			
		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation / Regulation	Organisation	People	Products	Services
19	Factor Analysis of Information Risk (FAIR)		x					x			
20	Federal Information Processing Standards Publication (FIPS) Publication 140-2 Security Requirements for Crytographic Modules	x								x	
21	Gramm–Leach–Bliley Act						x	x			
22	Health Insurance Portability and Accountability Act (HIPPA)						x	x			
23	HMG Baseline Personnel Screening Standard (BPSS)	x							x		
24	HMG Security Policy Framework (SPF)	x						x	x		
25	International Association of Accountants Innovation & Technology Consultants (IIAITC) Information Security Framework		x					x			
26	ICAS Information Security Framework		x					x			
27	Internet Engineering Task Force (IETF) Request For Comments (RFCs)	x				x		x		x	x
28	Information Assurance for SMEs (IASME)	x						x			
29	Information Security Forum (ISF) Standard of Good Practice for Information Security	x						x			
30	Information Systems Security Association Generally Accepted System Security Principles (GAASP)					x		x			
31	Information Technology Security Evaluation Criteria (ITSEC)	x								x	x
32	International Telecommunications Union (ITU) Recommendations - X series (Data Networks, Open System Communication and Security)	x	x			x				x	x
33	ISACA Control Objectives for Information and Related Technology (COBIT)		x					x			
34	ISO 15292 Protection profile registration procedures	x						x			
35	ISO 15489:2001 Records management	x						x			
36	ISO 19011 Guidelines for auditing management systems	x						x			
37	ISO 22301:2012 Societal security - Business continuity management systems - Requirements	x						x			
38	ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002	x						x			
39	ISO 9594-8 Standard for Public Key Infrastructure Cryptography (relates to X.509 as profiled by RFC5280)	x						x			
40	ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview	x								x	

Target Industry Sector					Product Type										Service Type									
All / Sector Agnostic	Financial Services (including Insurance)	Medical / Healthcare	Telecoms	Energy (Extraction and/or Supply)	Encryption Technologies	Telecommunications & Channel Management	Perimeter Defence	Network Access Control	Identity & Access Management (IAM)	Inventory, Configuration & Patch Management	Device Management (Anti-Malware & Anti-Virus)	Security Incident & Event Management	Data & Data Loss Prevention	Operating System & Server Application	Security Governance	IT Risk Management	Audit & Compliance	Security Training	Design & Architecture	Software Development	Configuration & Implementation	Security Operations	Incident Response & Crisis Management	Business Continuity (BC) & Disaster Recovery (DR)
x																								
x					x								x											
	x																							
		x																						
x																								
x																								
x																								
x																								
x					x	x	x	x	x			x		x							x	x		
x																								
x																								
x																								
x					x				x				x		x	x	x							
x					x	x		x	x				x		x	x	x		x			x	x	
x																								
x																								
x																								
x																								
x																								
		x																						
x																								
x									x				x											

Ref	Publication	Publication Nature						Content Category			
		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation / Regulation	Organisation	People	Products	Services
41	ISO/IEC 11770-1:2010 Information technology -- Security techniques -- Key management	x						x		x	
42	ISO/IEC 12207:2008 Systems and software engineering - Software life cycle processes	x						x			
43	ISO/IEC 13335 IT security management (Parts 1 to 5)	x						x			
44	ISO 13485:2003 Medical devices -- Quality management systems -- Requirements for regulatory purposes	x						x			
45	ISO/IEC 13888-1:2009 Information technology -- Security techniques -- Non-repudiation	x								x	x
46	ISO/IEC 15288:2008 Systems and software engineering -- System life cycle processes		x					x			
47	ISO/IEC 15408:2009 Information technology -- Security techniques -- Evaluation criteria for IT security (also known as the Common Criteria for Information Technology Security Evaluation, or simply the 'Common Criteria')	x								x	
48	ISO/IEC 17021 Conformity assessment -- requirements for bodies providing audit and certification of management systems	x									x
49	ISO17024 General Requirements for Bodies operating Certification of Persons	x						x			
50	ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories	x						x			
51	ISO/IEC 17799:2000 Code of Practice for Information Security Management					x		x	x		
52	ISO/IEC 18028:2006 Information technology -- Security techniques -- IT network security	x						x			
53	ISO/IEC 18043:2006 Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems	x						x			
54	ISO/IEC 19770 Software asset management	x						x			
55	ISO/IEC 20000 IT service management	x						x			
56	ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM)	x						x			
57	ISO/IEC 24762:2008 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services					x		x			x
58	ISO/IEC 27001:2005	x						x			
59	ISO/IEC 27002:2005	x						x			
60	ISO/IEC 27003:2010	x						x			
61	ISO/IEC 27004	x						x			

Target Industry Sector					Product Type										Service Type									
All / Sector Agnostic	Financial Services (including Insurance)	Medical / Healthcare	Telecoms	Energy (Extraction and/or Supply)	Encryption Technologies	Telecommunications & Channel Management	Perimeter Defence	Network Access Control	Identity & Access Management (IAM)	Inventory, Configuration & Patch Management	Device Management (Anti-Malware & Anti-Virus)	Security Incident & Event Management	Data & Data Loss Prevention	Operating System & Server Application	Security Governance	IT Risk Management	Audit & Compliance	Security Training	Design & Architecture	Software Development	Configuration & Implementation	Security Operations	Incident Response & Crisis Management	Business Continuity (BC) & Disaster Recovery (DR)
x					x																			
x																								
x																								
		x																						
x									x				x									x		
x																								
x					x	x	x	x	x	x	x	x	x	x										
x																	x							
x																								
x																								
x																								
x																								
x																								
x																								
x																								
x																								
x																							x	x
x																								
x																								
x																								
x																								

Ref	Publication	Publication Nature						Content Category			
		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation / Regulation	Organisation	People	Products	Services
62	ISO/IEC 27005	x						x			
63	ISO/IEC 27006:2011 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems	x						x			
64	ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing					x		x			
65	ISO/IEC 27010:2012 Information technology - Security techniques - Information security management for inter-sector and inter-organisational communications	x						x			
66	ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	x						x			
67	ISO/IEC 27013:2012 Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	x						x			
68	ISO/IEC 27014:2013 (including ITU-T Recommendation X.1054) Information technology - Security techniques - Governance of information security	x						x			
69	ISO/IEC 27015:2012 Information technology - Security techniques - Information security management guidelines for financial services	x						x			
70	ISO/IEC 27017 - Information technology - Security techniques - Code of practice for information security controls for cloud computing services based on ISO/IEC 27002 (DRAFT)	x						x			x
71	ISO/IEC 27018 - Information technology - Security techniques - Code of practice for controls to protect personally identifiable information processed in public cloud computing services (DRAFT)	x						x			
72	ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity					x		x			
73	ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cyber security	x						x			
74	ISO/IEC 27033 Information technology - Security techniques - Network security (parts 1-3 published, parts 4-6 DRAFT)	x						x			
75	ISO/IEC 27034 Information technology - Security techniques - Application security (part 1 published, rest in DRAFT)	x						x			x
76	ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident handling	x						x			
77	ISO/IEC 27036 IT Security - Security techniques - Information security for supplier relationships (DRAFT)	x						x			
78	ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence					x		x		x	x
79	ISO/IEC 27038 Information technology - Security techniques - Specification for digital redaction (FINAL DRAFT)	x						x		x	
80	ISO/IEC 27039 Information technology - Security techniques - Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS) (DRAFT)	x						x			

Target Industry Sector					Product Type										Service Type									
All / Sector Agnostic	Financial Services (including Insurance)	Medical / Healthcare	Telecoms	Energy (Extraction and/or Supply)	Encryption Technologies	Telecommunications & Channel Management	Perimeter Defence	Network Access Control	Identity & Access Management (IAM)	Inventory, Configuration & Patch Management	Device Management (Anti-Malware & Anti-Virus)	Security Incident & Event Management	Data & Data Loss Prevention	Operating System & Server Application	Security Governance	IT Risk Management	Audit & Compliance	Security Training	Design & Architecture	Software Development	Configuration & Implementation	Security Operations	Incident Response & Crisis Management	Business Continuity (BC) & Disaster Recovery (DR)
x																								
x																								
x																								
			x																					
			x																					
x																								
x																								
	x																							
x																						x		
x																								
x																								
x																								
x																								
x																			x	x				
x																								
x																								
x												x											x	
x													x											
x																								

Ref	Publication	Publication Nature						Content Category			
		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation / Regulation	Organisation	People	Products	Services
81	ISO/IEC 27040 Information technology - Security techniques - Storage security (DRAFT)	x						x			
82	ISO/IEC 27041 Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence (DRAFT)					x		x			
83	ISO/IEC 27042 Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence (DRAFT)					x		x			
84	ISO/IEC 27043 Information technology - Security techniques - Digital evidence investigation principles and processes (DRAFT)	x						x			
85	ISO/IEC 27044 Information technology - Security techniques - Guidelines for security information and event management (SIEM) (DRAFT)					x		x			
86	ISO/IEC 38500 Corporate governance of information technology	x						x			
87	ISO/IEC 7498-1:1994 Open Systems Interconnect (OSI) security model	x						x			
88	ISO/IEC 9000/9001	x						x			
89	ISO/IEC 90003:2004 Software engineering -- Guidelines for the application of ISO 9001:291000 to computer software					x		x			
90	ISO/IEC 9594-8:2008 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	x						x		x	
91	ISO/IEC TR 18044 Security incident management	x						x			
92	ISO/IEC TR 27008:2011	x						x			
93	ISO/IEC TR 27016 IT Security - Security techniques - Information security management - Organizational economics (DRAFT)	x						x			
94	ISO/IEC TR 27019 Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry (DRAFT)	x						x			
95	ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management					x		x			x
96	ISO/TR 13569:2005	x						x			
97	IT Baseline Security System (ISKE)					x		x			
98	IT Infrastructure Library (ITIL) v3		x					x			
99	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 Introduction to Computer Security					x		x			
100	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems					x		x			

Target Industry Sector					Product Type										Service Type									
All / Sector Agnostic	Financial Services (including Insurance)	Medical / Healthcare	Telecoms	Energy (Extraction and/or Supply)	Encryption Technologies	Telecommunications & Channel Management	Perimeter Defence	Network Access Control	Identity & Access Management (IAM)	Inventory, Configuration & Patch Management	Device Management (Anti-Malware & Anti-Virus)	Security Incident & Event Management	Data & Data Loss Prevention	Operating System & Server Application	Security Governance	IT Risk Management	Audit & Compliance	Security Training	Design & Architecture	Software Development	Configuration & Implementation	Security Operations	Incident Response & Crisis Management	Business Continuity (BC) & Disaster Recovery (DR)
x																								
x																								
x																								
x																								
x																								
x																								
x																								
x																								
x																								
x					x				x															
x																								
x																								
x																								
				x																				
x																							x	x
	x																							
x																								
x																								
x																								
x																								

Ref	Publication	Publication Nature						Content Category			
		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation / Regulation	Organisation	People	Products	Services
101	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A					x		x			
102	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-35 Guide to Selecting Information Technology Security Services					x		x			
103	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-36 Guide to Selecting Information Technology Security Products					x		x			
104	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 Managing Information Security Risk Organization, Mission, and Information System View					x		x			
105	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations					x		x			
106	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64 Security Considerations in the System Development Life Cycle					x		x			x
107	NIST/NSA/DISA/DoD Security Technical Implementation Guides (STIGs)					x				x	x
108	Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)		x					x			
109	Open Web Application Security Project (OWASP) 'Top 10'					x				x	x
110	PAS-555 Cyber security risk, Governance and management	x	x					x			
111	PAS-56 Business continuity management	x						x			
112	PAS-68 and/or PAS-69 Physical Security Standards	x						x			
113	PAS-97 Mail Screening & Security	x						x			
114	Payment Card Industry Data Security Standard (PCI-DSS)	x						x		x	x
115	Redbook Physical Security Standards (not be confused with the Redbook standard for CD-ROMs) and associated Loss Prevention Standards (LPS)	x								x	x
116	Royal Australian College of General Practitioners (RACGP) Computer Information Security Standards (CISS)	x						x			
117	SANS Top 20 Security Controls: Twenty Critical Security Controls for Effective Cyber Defence					x		x			
118	Sarbanes–Oxley Act						x	x			
119	Security Requirements for 'List X' Contractors	x						x			
120	Sherwood Applied Business Security Architecture (SABSA)		x					x			

Target Industry Sector					Product Type										Service Type									
All / Sector Agnostic	Financial Services (including Insurance)	Medical / Healthcare	Telecoms	Energy (Extraction and/or Supply)	Encryption Technologies	Telecommunications & Channel Management	Perimeter Defence	Network Access Control	Identity & Access Management (IAM)	Inventory, Configuration & Patch Management	Device Management (Anti-Malware & Anti-Virus)	Security Incident & Event Management	Data & Data Loss Prevention	Operating System & Server Application	Security Governance	IT Risk Management	Audit & Compliance	Security Training	Design & Architecture	Software Development	Configuration & Implementation	Security Operations	Incident Response & Crisis Management	Business Continuity (BC) & Disaster Recovery (DR)
x																								
x																								
x																								
x																								
x																								
x															x	x	x		x	x	x			
x					x	x	x	x	x	x	x	x	x	x							x			
x																								
x														x					x	x	x			
x																								
x																								
x																								
x																								
x					x	x		x	x				x		x		x							
x							x												x					
		x																						
x																								
	x																							
x																								
x																								

		Publication Nature	Content Category

		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation / Regulation	Organisation	People	Products	Services
121	South African Government MINIMUM INFORMATION SECURITY STANDARDS					x		x			
122	Special Publication 800-77 Guide to IPsec VPNs					x				x	x
123	The Open Group Architecture Framework (TOGAF) v9		x					x			
124	The Open Group Open Information Security Management Maturity Model (O-ISM3)				x			x			
125	Trusted Computer System Evaluation Criteria (TCSEC / 'The Orange Book')	x						x		x	x
126	UK MOD Joint Service Publication (JSP) 440 Defence Manual of Security					x		x			
127	UK MOD Joint Service Publication (JSP) 541 Information Security Alert Warning and Response Policy and Procedures Manual					x		x			
128	You're Outside looking In / You're Inside looking Out (YOI-YIO): Contextual Risk Analysis		x					x			
		79	14	2	3	38	4	110	5	26	24
	Statistical calculations:	-	-	-	-	-	140	-	-	-	165
		56%	10%	1%	2%	27%	3%	67%	3%	16%	15%

Key: Included on the 'short list' for detailed mapping

Target Industry Sector					Product Type										Service Type									
All / Sector Agnostic	Financial Services (including Insurance)	Medical / Healthcare	Telecoms	Energy (Extraction and/or Supply)	Encryption Technologies	Telecommunications & Channel Management	Perimeter Defence	Network Access Control	Identity & Access Management (IAM)	Inventory, Configuration & Patch Management	Device Management (Anti-Malware & Anti-Virus)	Security Incident & Event Management	Data & Data Loss Prevention	Operating System & Server Application	Security Governance	IT Risk Management	Audit & Compliance	Security Training	Design & Architecture	Software Development	Configuration & Implementation	Security Operations	Incident Response & Crisis Management	Business Continuity (BC) & Disaster Recovery (DR)
x																								
x						x															x		x	
x																								
x																								
x					x	x	x	x	x	x	x	x	x	x			x			x				
x																								
x																								
x																								

Ref	Publication	Relevance			Prevalence		
		Directly security related	Has security elements	Not directly security related	Online respondent mentions	Face-to-face interviewee mentions	On / linked from first 30 search results
1	American National Standards Institute (ANSI) X9 series	x			0	0	x
2	Australian Defence Signals Directorate (DSD) Information Security Manual (ISM); formerly known as "ACSI33"	x			0	0	x
3	Basel II		x		0	0	x
4	BITS Shared Assessments	x			0	0	x
5	BS 10008:2008 Evidential weight and legal admissibility of electronic information	x			0	0	x
6	BS25999 Business Continuity	x			0	0	x
7	Bundesamt fur Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security '100 Series'	x			0	0	x
8	Carnegie Melon Capability Maturity Model (CMM)			x	7	0	
9	CESG Assisted Products Service (CAPS)	x			0	1	
10	CESG Information Assurance Standards (ISs/IASs) and associated supplements	x			14	0	
11	CESG Tailored Assurance Service (CTAS)	x			0	1[1]	
12	Cyber Defence Capability Assessment Tool (CDCAT)	x			0	1[1]	
13	European Telecommunications Standards Institute (ETSI) Publications - European Standards (EN) series - tagged with keyword 'security'	x			0	1[1]	
14	European Telecommunications Standards Institute (ETSI) Publications - (Interim) European Telecommunication Standards (ETS/I-ETS) series - tagged with keyword 'security'	x			0	1[1]	
15	European Telecommunications Standards Institute (ETSI) Publications - ETSI Standards (ES) series - tagged with keyword 'security'	x			0	1[1]	
16	European Telecommunications Standards Institute (ETSI) Publications - Technical Specifications (xTS/xGS) series - tagged with keyword 'security'	x			0	1[1]	
17	European Telecommunications Standards Institute (ETSI) Publications - ETSI Guides (EG) series - tagged with keyword 'security'	x			0	1[1]	
18	European Telecommunications Standards Institute (ETSI) Publications - others tagged with keyword 'security', including: (x)TR series - Technical Reports (x)SR series - Special Reports (x)TBR series - Technical Basis for Regulation NET series - Norme Europeenne de Telecommunication MI series - Miscellaneous Work Item AN series - Advisory Note	x			0	1[1]	
19	Factor Analysis of Information Risk (FAIR)	x			0	1[1]	
20	Federal Information Processing Standards Publication (FIPS) Publication 140-2 Security Requirements for Crytographic Modules	x			0	0	x

Language			Classification		Status			Currency		Agedness			Audience		Origin		
Current version in English	In English, but lags by >24 months	Not available in English	Not classified / protectively marked	Classified / protectively marked	Released / Available	50% or more in draft	50% or more revoked	Current	50% or more superseded	Year of last revision	Not aged	Aged	Adopters	Certification Bodies / Auditors / Testers	UK Government	International	Foreign Government
x			x		x			x		2012	x		x			x	
x			x		x			x		2013	x		x				x
x			x		x			x		2009	x		x			x	
x			x		x			x		2013	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x				x	2007	x		x			x	
x			x		x			x		2013	x		x				x
x			x		x			x		1999		x	x			x	
x			x		x			x		2013	x		x	x	x		
x			x	x	x			x		Various	x		x		x		
x			x		x			x		2012	x		x	x	x		
x			x		x			x		2013	x		x	x	x		
x			x		x			x		Various	x		x	x		x	
x			x		x			x		Various	x		x	x		x	
x			x		x			x		Various	x		x	x		x	
x			x		x			x		Various	x		x	x		x	
x			x		x			x		Various	x		x	x		x	
x			x		x			x		Various	x		x	x		x	
x			x		x			x		2011	x		x			x	
x			x		x			x		2001		x		x			x

Ref	Publication	Relevance			Prevalence		
		Directly security related	Has security elements	Not directly security related	Online respondent mentions	Face-to-face interviewee mentions	On / linked from first 30 search results
21	Gramm–Leach–Bliley Act		x		0	0	x
22	Health Insurance Portability and Accountability Act (HIPPA)		x		0	0	x
23	HMG Baseline Personnel Screening Standard (BPSS)	x			9	0	
24	HMG Security Policy Framework (SPF)	x			7	0	
25	International Association of Accountants Innovation & Technology Consultants (IIAITC) Information Security Framework	x			0	1[1]	x
26	ICAS Information Security Framework	x			2	0	
27	Internet Engineering Task Force (IETF) Request For Comments (RFCs)		x		1	0	
28	Information Assurance for SMEs (IASME)	x			7	0	x
29	Information Security Forum (ISF) Standard of Good Practice for Information Security	x			0	0	x
30	Information Systems Security Association Generally Accepted System Security Principles (GAASP)	x			0	0	x
31	Information Technology Security Evaluation Criteria (ITSEC)	x			3	0	x
32	International Telecommunications Union (ITU) Recommendations - X series (Data Networks, Open System Communication and Security)	x			0	1	
33	ISACA Control Objectives for Information and Related Technology (COBIT)		x		10	1	
34	ISO 15292 Protection profile registration procedures	x			0	0	x
35	ISO 15489:2001 Records management			x	0	0	x
36	ISO 19011 Guidelines for auditing management systems			x	0	0	x
37	ISO 22301:2012 Societal security - Business continuity management systems - Requirements	x			10	0	x
38	ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002	x			0	0	x
39	ISO 9594-8 Standard for Public Key Infrastructure Cryptography (relates to X.509 as profiled by RFC5280)	x			5	0	
40	ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview	x			0	0	x
41	ISO/IEC 11770-1:2010 Information technology -- Security techniques -- Key management	x			0	0	x
42	ISO/IEC 12207:2008 Systems and software engineering - Software life cycle processes		x		0	0	x

Language			Classification		Status			Currency		Agedness			Audience		Origin		
Current version in English	In English, but lags by >24 months	Not available in English	Not classified / protectively marked	Classified / protectively marked	Released / Available	50% or more in draft	50% or more revoked	Current	50% or more superseded	Year of last revision	Not aged	Aged	Adopters	Certification Bodies / Auditors / Testers	UK Government	International	Foreign Government
x			x		x			x		1999		x	x				x
x			x		x			x		2013	x		x				x
x			x		x			x		2009	x		x		x		
x			x		x			x		2013	x		x		x		
x			x		x			x		2011	x		x			x	
x			x		x			x		2012	x		x			x	
x			x		x			x		2013	x		x			x	
x			x		x			x		2013	x		x			x	
x			x		x			x		2013	x		x			x	
x			x		x			x		1999		x	x			x	
x			x		x			x		1991		x	x			x	
x			x		x			x		Various	x		x			x	
x			x		x			x		2012	x		x			x	
x			x		x			x		2002		x	x			x	
x			x		x			x		2001		x	x			x	
x			x		x			x		2011	x			x		x	
x			x		x			x		2012	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		1996		x	x			x	
x			x		x			x		2010	x		x			x	
x			x		x			x		2008	x		x			x	

Ref	Publication	Relevance			Prevalence		
		Directly security related	Has security elements	Not directly security related	Online respondent mentions	Face-to-face interviewee mentions	On / linked from first 30 search results
43	ISO/IEC 13335 IT security management (Parts 1 to 5)	x			0	0	x
44	ISO 13485:2003 Medical devices -- Quality management systems -- Requirements for regulatory purposes			x	0	1	
45	ISO/IEC 13888-1:2009 Information technology -- Security techniques -- Non-repudiation	x			0	0	x
46	ISO/IEC 15288:2008 Systems and software engineering -- System life cycle processes		x		0	0	x
47	ISO/IEC 15408:2009 Information technology -- Security techniques -- Evaluation criteria for IT security (also known as the Common Criteria for Information Technology Security Evaluation, or simply the 'Common Criteria')	x			5	0	x
48	ISO/IEC 17021 Conformity assessment -- requirements for bodies providing audit and certification of management systems			x	0	0	x
49	ISO17024 General Requirements for Bodies operating Certification of Persons			x	0	1[1]	
50	ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories		x		0	0	x
51	ISO/IEC 17799:2000 Code of Practice for Information Security Management	x			0	0	x
52	ISO/IEC 18028:2006 Information technology -- Security techniques -- IT network security	x			0	0	x
53	ISO/IEC 18043:2006 Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems	x			0	0	x
54	ISO/IEC 19770 Software asset management	x			0	0	x
55	ISO/IEC 20000 IT service management		x		7	0	x
56	ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM)	x			0	0	x
57	ISO/IEC 24762:2008 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services	x			0	0	x
58	ISO/IEC 27001:2005	x			47	9	x
59	ISO/IEC 27002:2005	x			0	0	x
60	ISO/IEC 27003:2010	x			0	0	x
61	ISO/IEC 27004	x			0	0	x
62	ISO/IEC 27005	x			0	0	x
63	ISO/IEC 27006:2011 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems	x			0	0	x

Language			Classification		Status			Currency		Agedness			Audience		Origin		
Current version in English	In English, but lags by >24 months	Not available in English	Not classified / protectively marked	Classified / protectively marked	Released / Available	50% or more in draft	50% or more revoked	Current	50% or more superseded	Year of last revision	Not aged	Aged	Adopters	Certification Bodies / Auditors / Testers	UK Government	International	Foreign Government
x			x		x			x		2004	x		x			x	
x			x		x			x		2003	x		x			x	
x			x		x			x		2009	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		2009	x		x			x	
x			x		x			x		2013	x			x		x	
x			x		x			x		2012	x			x		x	
x			x		x			x		2005	x			x		x	
x			x		x			x		2005	x		x			x	
x			x		x			x		2006	x		x			x	
x			x		x			x		2006	x		x			x	
x			x		x			x		2012	x		x			x	
x			x		x			x		2011	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		2005	x		x			x	
x			x		x			x		2005	x		x			x	
x			x		x			x		2010	x		x			x	
x			x		x			x		2009	x		x			x	
x			x		x			x		2011	x		x			x	
x			x		x			x		2011	x			x		x	

Ref	Publication	Relevance			Prevalence		
		Directly security related	Has security elements	Not directly security related	Online respondent mentions	Face-to-face interviewee mentions	On / linked from first 30 search results
64	ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing	x			0	0	x
65	ISO/IEC 27010:2012 Information technology - Security techniques - Information security management for inter-sector and inter-organisational communications	x			0	0	x
66	ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	x			0	0	x
67	ISO/IEC 27013:2012 Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	x			0	0	x
68	ISO/IEC 27014:2013 (including ITU-T Recommendation X.1054) Information technology - Security techniques - Governance of information security	x			0	0	x
69	ISO/IEC 27015:2012 Information technology - Security techniques - Information security management guidelines for financial services	x			0	0	x
70	ISO/IEC 27017 - Information technology - Security techniques - Code of practice for information security controls for cloud computing services based on ISO/IEC 27002 (DRAFT)	x			0	0	x
71	ISO/IEC 27018 - Information technology - Security techniques - Code of practice for controls to protect personally identifiable information processed in public cloud computing services (DRAFT)	x			0	0	x
72	ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity	x			4	0	x
73	ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cyber security	x			0	0	x
74	ISO/IEC 27033 Information technology - Security techniques - Network security (parts 1-3 published, parts 4-6 DRAFT)	x			0	0	x
75	ISO/IEC 27034 Information technology - Security techniques - Application security (part 1 published, rest in DRAFT)	x			0	0	x
76	ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident handling	x			0	0	x
77	ISO/IEC 27036 IT Security - Security techniques - Information security for supplier relationships (DRAFT)	x			0	0	x
78	ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence	x			0	0	x
79	ISO/IEC 27038 Information technology - Security techniques - Specification for digital redaction (FINAL DRAFT)	x			0	0	x
80	ISO/IEC 27039 Information technology - Security techniques - Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS) (DRAFT)	x			0	0	x
81	ISO/IEC 27040 Information technology - Security techniques - Storage security (DRAFT)	x			0	0	x
82	ISO/IEC 27041 Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence (DRAFT)	x			0	0	x

Language			Classification		Status			Currency		Agedness			Audience		Origin		
Current version in English	In English, but lags by >24 months	Not available in English	Not classified / protectively marked	Classified / protectively marked	Released / Available	50% or more in draft	50% or more revoked	Current	50% or more superseded	Year of last revision	Not aged	Aged	Adopters	Certification Bodies / Auditors / Testers	UK Government	International	Foreign Government
x			x		x			x		2011	x			x		x	
x			x		x			x		2012	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		2012	x		x			x	
x			x		x			x		2013	x		x			x	
x			x		x			x		2012	x		x			x	
x			x			x		x		2013	x		x			x	
x			x			x		x		2013	x		x			x	
x			x		x			x		2011	x		x			x	
x			x		x			x		2012	x		x			x	
x			x			x		x		2013	x		x			x	
x			x			x		x		2013	x		x			x	
x			x		x			x		2011	x		x			x	
x			x			x		x		2013	x		x			x	
x			x		x			x		2012	x		x			x	
x			x			x		x		2013	x		x			x	
x			x			x		x		2013	x		x			x	
x			x			x		x		2013	x		x			x	
x			x			x		x		2013	x		x			x	

Ref	Publication	Relevance			Prevalence		
		Directly security related	Has security elements	Not directly security related	Online respondent mentions	Face-to-face interviewee mentions	On / linked from first 30 search results
83	ISO/IEC 27042 Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence (DRAFT)	x			0	0	x
84	ISO/IEC 27043 Information technology - Security techniques - Digital evidence investigation principles and processes (DRAFT)	x			0	0	x
85	ISO/IEC 27044 Information technology - Security techniques - Guidelines for security information and event management (SIEM) (DRAFT)	x			0	0	x
86	ISO/IEC 38500 Corporate governance of information technology		x		0	0	x
87	ISO/IEC 7498-1:1994 Open Systems Interconnect (OSI) security model	x			0	0	x
88	ISO/IEC 9000/9001		x		0	0	x
89	ISO/IEC 90003:2004 Software engineering -- Guidelines for the application of ISO 9001:291000 to computer software	x			0	0	x
90	ISO/IEC 9594-8:2008 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	x			0	0	x
91	ISO/IEC TR 18044 Security incident management	x			0	0	x
92	ISO/IEC TR 27008:2011	x			0	0	x
93	ISO/IEC TR 27016 IT Security - Security techniques - Information security management - Organizational economics (DRAFT)	x			0	0	x
94	ISO/IEC TR 27019 Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry (DRAFT)	x			0	0	x
95	ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management	x			0	0	x
96	ISO/TR 13569:2005	x			0	0	x
97	IT Baseline Security System (ISKE)	x			0	1[1]	
98	IT Infrastructure Library (ITIL) v3		x		0	0	x
99	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 Introduction to Computer Security	x			0	0	x
100	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems	x			0	0	x
101	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	x			0	0	x
102	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-35 Guide to Selecting Information Technology Security Services	x			0	0	x

Language			Classification		Status			Currency		Agedness			Audience		Origin		
Current version in English	In English, but lags by >24 months	Not available in English	Not classified / protectively marked	Classified / protectively marked	Released / Available	50% or more in draft	50% or more revoked	Current	50% or more superseded	Year of last revision	Not aged	Aged	Adopters	Certification Bodies / Auditors / Testers	UK Government	International	Foreign Government
x			x			x		x		2013	x		x			x	
x			x			x		x		2013	x		x			x	
x			x			x		x		2013	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		1994		x	x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		2004	x		x			x	
x			x		x			x		2008	x		x			x	
x			x		x			x		2004	x		x			x	
x			x		x			x		2011	x			x		x	
x			x			x		x		2013	x		x			x	
x			x			x		x		2013	x		x			x	
x			x		x			x		2007	x		x			x	
x			x		x			x		2005	x		x			x	
		x	x		x			x		2012	x		x				x
x			x		x			x		2011	x		x			x	
x			x		x			x		1995		x	x				x
x			x		x			x		1996		x	x				x
x			x		x			x		2004	x		x				x
x			x		x			x		2003	x		x				x

Ref	Publication	Relevance			Prevalence		
		Directly security related	Has security elements	Not directly security related	Online respondent mentions	Face-to-face interviewee mentions	On / linked from first 30 search results
103	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-36 Guide to Selecting Information Technology Security Products	x			0	0	x
104	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 Managing Information Security Risk Organization, Mission, and Information System View	x			0	0	x
105	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations	x			0	0	x
106	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64 Security Considerations in the System Development Life Cycle	x			0	0	x
107	NIST/NSA/DISA/DoD Security Technical Implementation Guides (STIGs)	x			0	0	x
108	Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)	x			0	0	x
109	Open Web Application Security Project (OWASP) 'Top 10'	x			2	0	
110	PAS-555 Cyber security risk, Governance and management	x			1	1	x
111	PAS-56 Business continuity management	x			0	0	x
112	PAS-68 and/or PAS-69 Physical Security Standards	x			0	1[1]	
113	PAS-97 Mail Screening & Security	x			1	0	
114	Payment Card Industry Data Security Standard (PCI-DSS)	x			1	9	x
115	Redbook Physical Security Standards (not be confused with the Redbook standard for CD-ROMs) and associated Loss Prevention Standards (LPS)	x			0	0	x
116	Royal Australian College of General Practitioners (RACGP) Computer Information Security Standards (CISS)	x			0	0	x
117	SANS Top 20 Security Controls: Twenty Critical Security Controls for Effective Cyber Defence	x			0	0	x
118	Sarbanes–Oxley Act		x		0	1	
119	Security Requirements for 'List X' Contractors	x			4	0	
120	Sherwood Applied Business Security Architecture (SABSA)		x		0	1[1]	
121	South African Government MINIMUM INFORMATION SECURITY STANDARDS	x			0	0	x
122	Special Publication 800-77 Guide to IPsec VPNs	x			0	0	x
123	The Open Group Architecture Framework (TOGAF) v9		x		2	0	
124	The Open Group Open Information Security Management Maturity Model (O-ISM3)	x			0	0	x

Language			Classification		Status			Currency		Agedness			Audience		Origin		
Current version in English	In English, but lags by >24 months	Not available in English	Not classified / protectively marked	Classified / protectively marked	Released / Available	50% or more in draft	50% or more revoked	Current	50% or more superseded	Year of last revision	Not aged	Aged	Adopters	Certification Bodies / Auditors / Testers	UK Government	International	Foreign Government
x			x		x			x		2003	x		x				x
x			x		x			x		2011	x		x				x
x			x		x			x		2013	x		x				x
x			x		x			x		2008	x		x				x
x			x		x			x		2013	x		x				x
x			x		x			x		2001		x	x			x	
x			x		x			x		2013	x		x			x	
x			x		x			x		2013	x		x			x	
x			x		x				x	2003	x		x			x	
x			x		x			x		2010	x		x			x	
x			x		x			x		2012	x		x			x	
x			x		x			x		2010	x		x			x	
x			x		x			x		2011	x		x			x	
x			x		x			x		2013	x		x			x	
x			x		x			x		2013	x		x			x	
x			x		x			x		2002		x	x				x
x			x		x			x		2013	x		x		x		
x			x		x			x		2009	x		x			x	
x				x	x			x		1996		x	x				x
x			x		x			x		2005	x		x				x
x			x		x			x		2011	x		x			x	
x			x		x			x		2011	x		x			x	

Ref	Publication	Relevance			Prevalence		
		Directly security related	Has security elements	Not directly security related	Online respondent mentions	Face-to-face interviewee mentions	On / linked from first 30 search results
125	Trusted Computer System Evaluation Criteria (TCSEC / 'The Orange Book')	**x**			**0**	**0**	**x**
126	UK MOD Joint Service Publication (JSP) 440 Defence Manual of Security	**x**			**2**	**1**	
127	UK MOD Joint Service Publication (JSP) 541 Information Security Alert Warning and Response Policy and Procedures Manual	**x**			**0**	**0**	**x**
128	You're Outside looking In / You're Inside looking Out (YOI-YIO): Contextual Risk Analysis	**x**			**0**	**1**[1]	
		107	15	6	2[2]	5[2]	111
	Statistical calculations:	-	-	128	-	-	118
		84%	12%	5%	2%	4%	94%

Key: Included on the 'short list' for detailed mapping

Note 1: These standards were identified by BIS as being of interest where there may be potential for future wider use. It was desired to assess what the current views of them are and they were thus included.

Note 2: Note that this is neither a sum nor or a count of the individual cells in this column. The logic for these values is as follows:

- The value at the foot of the 'online respondent mentions' column is given by the number of rows which contain a value of 10 or greater in this column which **do not** have an 'x' in the corresponding 'on / linked from first 30 search results' column, see Pg 31 for rationale.
- The value at the foot of the 'face-to-face interview mentions column' is given by the number of rows which contain a value of 1 or greater in this column which **do not** have an 'x' in the corresponding 'on / linked from first 30 search results' column **and do not** have a value of 10 or greater in the corresponding 'online respondent mentions' column, see Pg 31 for rationale.

Language			Classification		Status			Currency		Agedness			Audience		Origin		
Current version in English	In English, but lags by >24 months	Not available in English	Not classified / protectively marked	Classified / protectively marked	Released / Available	50% or more in draft	50% or more revoked	Current	50% or more superseded	Year of last revision	Not aged	Aged	Adopters	Certification Bodies / Auditors / Testers	UK Government	International	Foreign Government
x			x		x			x		1985		x	x	x			x
x				x	x			x		2001		x	x		x		
x			x		x			x		2006	x		x		x		
x			x		x			x		2008	x		x		x		
127	0	1	126	3	114	14	0	126	2	-	112	16	120	18	10	99	19
-	-	128	-	129	-	-	128	-	128	-	-	128	-	138	-	-	128
99%	0%	1%	98%	2%	89%	11%	0%	98%	2%	-	88%	13%	87%	13%	8%	77%	15%

Annex D – Detailed Mapping Definitions and Criteria

Criteria for ‘short-listing’ publications within the detailed mapping

The following criteria were used to ‘short-list’ publications within the high-level cyber security standards landscape for inclusion within the detailed mapping analysis:

Dimension	Rule-set for inclusion
Relevance	MUST be overtly and directly orientated towards security **OR** MUST have a discrete and readily identifiable chapter or section that is directly and overtly orientated towards security
Prevalence	MUST be mentioned by at least ten respondents to the online survey **OR** MUST be mentioned by at least one respondent to the telephone/face-to-face interview or have been nominated by BIS as a standard of interest **OR** MUST appear on the first three pages of search results on www.google.co.uk, or be referenced within such results, for the search term “cyber security standard” or “information security standard”
Accessibility (language)	MUST have a English-language version available that ‘lags’ any non-English-language original by no more than 24 months
Accessibility (classification)	MUST NOT carry a national security classification (i.e. must be Unclassified / Not Protectively Marked, or foreign equivalent)
Status	MUST NOT be in draft status (or have 50% or more of its constituent parts in draft for multi-part standards) **AND** MUST NOT have been revoked (or have 50% or more of its constituent parts revoked for multi-part standards)
Currency	MUST NOT have been wholly superseded by or incorporated within subsequent publications (or have 50% or more of its constituent parts superseded for multi-part standards)
Agedness	MUST have been published or revised since 1st January 2003 (i.e. not more than 10 full calendar years old at the time of writing)

Dimension	Rule-set for inclusion
Intended audience	MUST be aimed at organisations wishing to adopt the standard directly; NOT solely at organisations wishing to certify other organisations as being compliant (e.g. the standard must not be aimed solely at certification bodies or testing/evaluation facilities)
Coverage – industry sector	MUST NOT be specific to one industry sector (note: can still be specific to one broader ‘sector’, i.e. public or private)
Coverage – products and vendors	MUST NOT be specific to one particular product or vendor (e.g. a hardening guide for how to secure a particular operating system or make of smart-phone)
Coverage – domains	MUST NOT be obviously and intentionally focused at one specific domain within the cyber security framework (e.g. a ‘digital forensics’ standard which intentionally only covers the Respond domain)

Cyber Security Framework

The framework below was used in the production of the detailed mapping. The coverage level of each publication within the detailed mapping was assessed against these domains and sub-domains.

Domain	Criteria	Sub-Domain 1
Governance	A standard qualifies as covering the Governance domain if it details the identification of information assets and the policies, processes and procedures that are required to provide/prove governance over the organisation's information assets.	Processes: The standard identifies the need for the organisation to have processes in place to protect information.
People	A standard qualifies as covering the People domain if it explains what an organisation's cyber security team might compromise in terms of structure, resourcing and how it integrates into the broader organisation, whilst defining the roles and responsibilities of personnel within this department. It should outline the security training requirements of both security practitioners and general employees.	IS/IA Organisation: The standard identifies the need for the organisation to have an IS/IA organisation in place.
Prepare	A standard qualifies as covering the Prepare domain if it explains what physical and logical information technology assets might be needed to defend an organisation's networks and systems, and/or if it is describes processes to catalogue non-security IT resources and maintain them to a known secure baseline configuration.	Environment: The standard identifies the need for the organisation to define an appropriate environment to protect against Cyber security risks.
Operations	A standard qualifies as covering the Operations domain if it explains the day-to-day management activities that need to occur in order to ensure the security of an organisation's systems and networks.	Administration: The standard identifies the need for the organisation to detail the administrative processes in place to support against Cyber security risks and threats.
Intelligence	A standard qualifies as covering the Intelligence domain if it explains the need to collect and process monitoring information, if it proposes a model for identifying what monitoring should occur and when, and/or if it directly proposes what monitoring should take place. Such standards are also likely to address considerations such as demand, capacity and performance management; plus how situational awareness might be obtained in relation to the threat an organisation faces.	Situational Awareness: The standard identifies the need for the organisation to identify what situational awareness capabilities it needs and/or has in place.
Respond	A standard qualifies as covering the Respond domain if it explains the activities required for an organisation to react to cyber security events in a timely and effective manner.	Business Continuity: The standard identifies the need for the organisation to detail its business continuity plan.

Sub-Domain 2	Sub-Domain 3	Sub-Domain 4
Risk Assessment: The standard identifies the need for the organisation to have a strategy in place to assess cyber risks.	Strategy & Policies: The standard identifies the need for the organisation to have a strategy and policies in place to govern its cyber security.	Audit & Compliance: The standard identifies the need for the organisation to have in place a means of auditing and assessing compliance with its cyber security regime.
Human Resource: The standard identifies the need for the organisation to implement cyber security controls within its recruitment and on-going HR processes.	Training: The standard identifies the need for the organisation to plan and deliver cyber security training and exercise programmes to its employees / members.	
Equipment: The standard identifies the need for the organisation to have equipment in place with which to manage and maintain its Cyber security.	Applications, Systems and Network: The standard identifies the need for the organisation to manage its applications, systems and network in a manner conducive to maintaining its Cyber security.	Research & Development: The standard identifies the need for the organisation to conduct research and development activities to improve its Cyber security position.
Authentication & Authorisation: The standard identifies the need for the organisation to assert the authentication and authorisation processes it has.		
Security Monitoring: The standard identifies the need for the organisation to detail what procedures it needs and/or has in place to monitor security.	Risk Assessment (tactical): The standard identifies the need for the organisation to detail what risk assessments it should conduct at a tactical level.	Key Performance Indicators: The standard identifies the need for the organisation to detail what its key performance indicators are for cyber security and whether there is a strategy in place to deliver these.
Incident Management: The standard identifies the need for the organisation to detail its incident management plan.		

Coverage level definitions

Coverage Level 1

The standard has no content relevant to this domain, or may:

- State high-level security outcomes to be achieved, but not the means for achieving them.
- List relevant security considerations to be addressed; but not identify the specific controls that an organisation must implement or the criteria that a person, product or service must meet in order to address them.
- Not attempt to define a precise specification that an organisation, person, product or service must meet in order to be certified as being compliant with the standard.
- Attempt to define the specification that must be met; but does not do so in an explicit, detailed, objective, unambiguous and otherwise testable/auditable manner. There is considerable scope for subjective interpretation of whether a specification within the standard has been met on behalf of the reader and/or an auditor or certification body.
- Not consider or reflect the dimensions of geography (the ‘where’) or time (the ‘when’) applicable to the standard’s purpose and scope.
- Not indicate who should be accountable, responsible, consulted or informed (as applicable) for a given activity, process or outcome described in the standard.
- Lack detail, such that the reader is likely to need additional advice, guidance and/or reference material in order to interpret the standard and meet its aims.
- Lack breadth, covering less than 50% of the sub-domains within a given domain.

Coverage Level 2

The standard may (as applicable to its purpose and scope):

- Identify the high-level security outcomes to be achieved and partial, high-level and/or indicative solutions for achieving them.
- Specify to a moderate level of detail the controls that an organisation must/should implement or the criteria that a person, product or service must/should meet in order to address relevant security risks.
- Specify a process by which the reader can identify and quantify the security risks applicable to their organisation, and/or the controls that their specific organisation should implement to mitigate these risks from a range of candidate controls.
- Define the specification that an organisation, person, product or service must meet in order to be certified as being compliant with the standard; but does not comprehensively and consistently do so in an explicit, detailed, objective, unambiguous and otherwise testable/auditable manner. There is some scope for subjective interpretation of whether a specification within the standard has been met on behalf of the reader and/or an auditor or certification body.
- Differentiate between what must, should, could, should not and must not be done; but does not does not give definitive and comprehensive direction to follow.

- Partially consider or reflect the dimensions of geography (the ‘where’) and time (the ‘when’) applicable to the standard. The standard may be vague in this regard, using terms such as ‘regularly’ instead of defining precise time periods.

- Indicate who must/should be accountable and/or responsible for a given activity, process or outcome; but provides little to no detail regarding such persons’ roles, seniorities, skills, qualifications, reporting lines and/or escalation routes.

- Provide coverage against the majority, but not all, of the sub-domains within a given domain.

Coverage Level 3

The standard consistently and comprehensively (as applicable to its purpose and scope):

- Defines the precise specifications that an organisation, person, product or service must meet in order to be certified as being compliant with the standard in an explicit, detailed, objective, unambiguous and otherwise testable/auditable manner. There is very little scope for subjective interpretation of whether a specification within the standard has been met on behalf of the reader and/or an auditor or certification body.

- Specifies a process by which a decision can be made for each instance where the standard identifies that a decision is required (rather than prescribing the result);

- Gives precise directions for the reader to follow in an objective, measurable and readily auditable manner; for example, providing checklists, decision trees or process maps.

- Not only differentiates between what must, should, could, should not and must not be done; but also defines these key words. The standard may also use terms such as ‘AND’ or ‘OR’ to clarify where requirements are cooperative, mutually exclusive or overlap.

- Gives definitive stipulations in terms of geography (the ‘where’) and time (the ‘when’) applicable to the standard. The standard is precise in this regard, using auditable criteria such as ‘not less than annually’ rather than vague terms such as ‘regularly’.

- Indicates who must be accountable, responsible, consulted and/or informed for a given activity, process or outcome; including coverage against dimensions such as roles, seniorities, skills, qualifications, reporting lines and/or escalation routes where pertinent.

- Provides coverage against the vast majority, if not all, of the sub-domains within a given domain.

- May additionally identify where applicability to different organisations, sectors, technologies or use case varies or where special cases exist.

Annex E – Detailed Mapping

Detailed Mapping Overview

Publication Name	Accessibility	Type						Category				Dependencies/ Touch-points	Content/Context
		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation	Organisation	People	Product	Services		**Purpose/Objective** What was the specific reason for the creation of this standard? What does it aim to achieve?
Australian Defence Signals Directorate (DSD) Information Security Manual (ISM); formerly known as "ACSI33"	Freely available					x		x				N/A	This publication suite targets different stakeholders with different variants of the publication's volumes to ensure that key decision makers across government are made aware of and involved in countering threats to their information and ICT systems.
Bundesamt fur Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security '100 Series'	Freely available					x		x				N/A	The set of four documents in the BSI 100 series are aimed at persons responsible for IT operations and information security in small, medium and large companies, government agencies and other public and private organisations. It is a standard for establishing and maintaining an appropriate level of protection for all information in an organisation.
HMG SPF (Security Policy Framework)	Freely available		x					x	x			N/A	SPF aims to provide a standardised baseline level of protection for all UK Government assets (people, information and infrastructure) across HMG. It specifies a series of Mandatory Requirements that all HMG Departments must comply with in order to ensure that systems/services provide an adequate level of protection to the information they store and process, and that such systems/services function as they need to, when they need to, under the control of legitimate users.
IASME (Information Assurance for Small & Medium-sized Enterprises)	Freely available	x						x				Derived from ISO27001/2	IASME is a flexible Information Assurance management standard derived from ISO27001:2005 that is aimed to be more proportionate to the needs and capabilities of SMEs. One of its overarching objectives is to prevent SMEs from being the weakest link in a given supply chain.
ISF (Information Security Forum) Standard for Good Practice for Cyber Security (SGP)	Freely available to ISF members	x						x				N/A	The ISF SGP addresses information security from a business perspective, providing a practical basis for assessing an organisation's information security arrangements.

Content/Context	Applicability / Coverage			Domain Mapping					
Focus Is there any particular area of cyber security at which the standard is targeted?	**Geographical Applicability**	**Industry/Sector Applicability**	**Intended Audience**	**Governance**	**People**	**Prepare**	**Operations**	**Intelligence**	**Respond**
The Australian DSD ISM covers a range of information security arrangements. It is available as a suite of three documents, relating to different degrees of detail and aimed at increasing seniority of role within the company when providing a broader overview. The most detailed document, The Controls manual, is the most specific with regards to exactly what needs to be implemented by the agency. Each of its sections is separated into Objective, Scope, Context and finally Controls, where the specific recommendations are made.	Original written for Australian readers, but with international applicability	Relevant to all sectors	Aimed at the Australian Government, but has utility across all sectors and industries. It comes in 3 variants: 1. The Executive Companion is targeted towards the most senior executives. 2. The Principles document is aimed at senior decision makers, such as CISOs. 3. The Controls manual is aimed at IT Security Managers and security practitioners in general.	3	2	3	3	2	2
The BSI 100 series of documents cover the following broad topics, focussing on one per document: Information Security Management Systems, Methodology, Risk Analysis, and Business Continuity Management.	Originally written for German readers, but with international applicability (English language version available)	Relevant to all sectors	Aimed at the German Government, but has utility across all sectors and industries.	2	1	2	1	2	3
SPF's Mandatory Requirements primarily focus on the establishment of key roles and processes for the identification of information assets and the risks associated with them. It also reflects perceived specific vulnerabilities within HMG around Personnel Security; specifically vetting and the need for broad awareness campaigns.	Prescriptive for UK government departments, although potentially suitable for adoption internationally	Relevant for all HMG Departments and Agencies, and those third parties / other bodies that are obliged to adhere as part of the broader HMG supply chain.	HMG and its supply chain.	2	2	2	2	2	2
IASME's breadth is similar to that of ISO27001 from which it is derived, but the depth is intentionally shallower in order to make it more relevant and achievable in the context of SMEs.	International	Relevant to all sectors	Aimed at any small to medium sized businesses.	2	1	1	1	1	1
The ISF SGP covers the complete spectrum of information security arrangements that need to be made to keep the business risks associated with information systems within acceptable limits, and presents good practice in practical, clear statements.	International	Relevant to all sectors	Targeted to meet the needs of large national and international organisations.	3	3	3	2	3	3

Publication Name	Accessibility	Type						Category				Dependencies/ Touch-points	Content/Context
		Standard	Framework / Methodology	Certification	Maturity Model	Guidance	Legislation	Organisation	People	Product	Services		**Purpose/Objective** What was the specific reason for the creation of this standard? What does it aim to achieve?
ISO27001:2005	Available at cost	x						x				Successor to BS7791 Part 2 (superseded)	ISO27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organisation.
ISO27002:2005	Available at cost	x						x				Successor to BS7791 Part 1 (later ISO17799) (both superseded)	ISO27002:2005 is the code of practice for information security management which elaborates upon ISO27001:2005.
Payment Card Industry Data Security Standard (PCI-DSS)	Freely available	x						x		x	x	N/A	The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.
Publicly Available Specification (PAS) 555:2013 (including Annexes)	Available at cost	x	x					x				Identifies relevant aspects of other cyber security publications, such as ISO standards 9000, 20000, 27001, 22301 and 31000.	PAS555 aims to provide the reader with the freedom to identify their own solutions to achieve the outcome-focused objectives it details. The rationale for this approach is that popular existing standards often detail how organisations should address cyber security, rather than what they should achieve; thus 'solutionising' for the reader in a way that may not be approachable, scalable or stand the test of time as technology advances. PAS555 aims to avoid such 'solutionising'.

Note: ISO27032 has been omitted from this analysis, despite being the only ISO publication to have 'cyber' in its title, due to awareness of this standard across the marketplace being much lower than that for ISO27001/27002. This is likely to be a factor of its relatively recent publication (the first finalised edition of ISO27032 was published in 2012).

Content/Context	Applicability / Coverage			Domain Mapping					
Focus Is there any particular area of cyber security at which the standard is targeted?	**Geographical Applicability**	**Industry/Sector Applicability**	**Intended Audience**	**Governance**	**People**	**Prepare**	**Operations**	**Intelligence**	**Respond**
ISO27001:2005 focuses on the establishment of a system of governance around cyber security within an organisation. It focuses on management taking full ownership of cyber security across the enterprise and the establishment of decision-making processes, rather than the specification of what the outcomes of such decisions may be. It comprehensively covers aspects such as human resources, physical assets, access control and governance.	International	Relevant to all sectors	Targeted to meet the needs of large national and international organisations. An ISMS implementation can be scaled in accordance with the needs/size of the organisation.	2	1	2	3	1	2
ISO27002:2005 includes best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS). All organisations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant.	International	Relevant to all sectors	Applicable to all organisations, regardless of size.	3	2	3	3	2	3
PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data.	International	Relevant to all sectors that handle confidential cardholder data or sensitive authorisation data including magnetic stripe data or equivalent on a chip.	All entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.	2	1	3	2	2	1
PAS555 describes a governance process by which organisations can perform on-going management of cyber security risks and controls. In addition to identifying the high-level business outcomes required of this governance, PAS555 also identifies an relevant controls detailed within other leading cyber security publications (such as such as ISO standards 9000, 20000, 27001, 22301 and 31000) as an 'informative' (as opposed to directive) annex.	International	Relevant to all sectors	Applicable to all organisations, regardless of size.	2	2	1	1	1	2

Australian Defence Signals Directorate (DSD) Information Security Manual (ISM)

Version:	Controls Version 1.4
Publisher:	Australian Defence Signals Directorate (DSD)
Date published:	Nov-12
URL:	http://www.dsd.gov.au/infosec/ism/

Cyber Security Domain	Reference 1	Reference 2
Governance	Australian Government Information Security Manual Controls: Information Security Documentation containing sub-sections including Documentation Fundamentals, Information Security Policy, Security Risk Management Plan, System Security Plan each containing a set of controls that specify what the reader must ensure for their organisation's development of a security policy and corresponding documentation. "Control: 0890: The ISP should cover topics such as: accreditation processes; personnel responsibilities; configuration control; access control; networking and connections with other systems; physical security and media control; emergency procedures and cyber security incident management; change management; information security awareness and training."	Australian Government Information Security Manual Controls: Information Security Documentation containing sub-section Standard Operating Procedures. The section describes the development of security related procedures and Controls 0790, 0055 and 0056 give tables that clearly define which procedures need to be included in the various security documentation.
People	Australian Government Information Security Manual Controls: Roles and Responsibilities containing sub-sections related to each of the recommended roles corresponding to cyber security. Each role is defined with an Objective, a Context and Controls that indicate what tasks the given role is "typically responsible for".	Australian Government Information Security Manual Controls: Personnel Security for Systems containing sub-sections including Information Security Awareness and Training, and Using the Internet. Information as to what an agency must do with regards to training is given by the controls within the Information Security Awareness and Training heading, and listed extensively. "Control: 0252: Agencies must provide ongoing information security awareness and training for personnel on information security policies including topics such as responsibilities, consequences of non-compliance, and potential security risks and counter-measures."
Prepare	Australian Government Information Security Manual Controls: Physical Security for Systems containing Facilities and Network Infrastructure, Servers and Network Devices and ICT Equipment and Media. These sections provide controls to be followed for the physical security of the assets of the agency, for example: "Control: 0159: AH Agencies must account for all sensitive and classified ICT equipment and media." and Control: 1053: Agencies must ensure that servers and network devices are secured in either security containers or rooms as specified in the Australian Government Physical Security Management Protocol."	Australian Government Information Security Manual Controls: Information Technology Security containing sub-sections Product Security, Media Security and Software Security. Detailed areas on Selection, Installation, Usage, Maintenance, Sanitation and Disposal, among others all have their own set of controls that must be followed. "Control: 0311: When disposing of ICT equipment containing sensitive or classified media, agencies must sanitise the equipment by either: sanitising the media within the equipment; removing the media from the equipment and disposing of it separately; destroying the equipment in its entirety." A flowchart is also included in the Product Selection and Acquisition sub-section.
Operations	Australian Government Information Security Manual Controls: Privileged Access section gives details on what must be done by agencies in order to limit the potential security risk from the targeting of privileged accounts with heightened access. "Control: 1175: Agencies must not allow privileged accounts access to the Internet or to email."	Australian Government Information Security Manual Controls: Identification and Authorisation section is very detailed on what agencies must do, and make their users do in order to limit security risks. Detail is given with regards to passphrases and their character length and expiration, multi factor authentication, session and screen locking, and the suspension of access after a number of failed attempts to prevent brute force attacks. For example, "Control: 0417: Agencies must not use a numerical password (or personal identification number) as the sole method of authenticating a user."
Intelligence	Australian Government Information Security Manual Controls: Information Security Monitoring containing sub-sections Vulnerability Management and Change Management. Objectives, Contexts and Controls are given for these sections, which aim to inform a user how to address new vulnerabilities and identify the need for change. "Control: 1163: Agencies should implement a vulnerability management strategy by: conducting vulnerability assessments on systems throughout their life cycle to identify vulnerabilities; analysing identified vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost and existing security controls; using a risk-based approach to prioritise the implementation of identified mitigations or treatments; monitoring new information on new or updated vulnerabilities in operating systems, software and devices as well as other elements which may adversely impact security.”	Australian Government Information Security Manual Controls: Cyber Security Incidents containing sub-sections Detecting, Reporting and Managing Cyber Security Incidents. In particular, the Detection sub-section details ways in which "agencies may consider" improving their chances of detection by giving the reader a table of options. Further controls also tell the reader what must be implemented in their organisation, for example, "Control: 0120: Agencies must develop, implement and maintain tools and procedures covering the detection of potential cyber security incidents, incorporating: counter-measures against malicious code; intrusion detection strategies; audit analysis; system integrity checking; vulnerability assessments."
Respond	Australian Government Information Security Manual Controls: Incident Response Plan outlines the Objective and Context of the need for an IRP. Under the Controls heading, there is a clear and definitive list (Control 0058) of what "Agencies must include, as a minimum" and a further list (Control 0059) of what "Agencies should include". However, within these lists the points are not expanded upon significantly, for example the agency must include "the steps necessary to ensure the integrity of evidence supporting a cyber security incident" but the standard does not inform the reader what these steps might be, allowing for subjective interpretation.	Australian Government Information Security Manual Controls: Business Continuity and Disaster Recovery Plans is a fairly brief section on how an agency can prepare itself for continuity in the wake of a cyber security incident. Although it makes some recommendations, such as "Agencies should: back up all information identified as critical to their business; store backups of critical information, with associated documented recovery procedures, at a remote location secured in accordance with the requirements for the sensitivity or classification of the information; test backup and restoration processes regularly to confirm their effectiveness." it is otherwise limited to instructing the reader to produce a comprehensive recovery plan.

Reference 3	Comments	Coverage Level
Australian Government Information Security Manual Controls: System Accreditation containing the sub-section of Conducting Audits. The section defines clearly the difference stages of the audit process, who should be in charge of the audit, "Control: 0902: Agencies should ensure that assessors conducting audits are not also the system owner or certification authority."	The ISM Controls document provides an extensive context as to why risk management must be undertaken. It states the need for this process and lists a few areas and general methodologies that must be implemented for identifying, analysing, evaluating and treating risk. The coverage of risk management is wide and the various controls within the document tell the reader what they must or should do. The standard also identifies the need for a strong governance framework to assist management in implementing a standardised security policy, with details of what is to be included again given by the controls. Audit and compliance are also covered in the System Accreditation section, expanded into various stages and requirements. Overall, this domain scores '3' for coverage.	3
N/A	The ISM Controls gives detailed context of why roles, responsibilities and training are important. The key roles in the security team are given (including ISO, Information Technology Security Advisor, IT security managers, IT security Officers etc.) as well as scope, context and controls of their responsibilities. However, there is room for subjective interpretation in the exact responsibilities of each role as these are classified as "usually responsible for:" which lacks complete clarity. More detail is given into what exactly should be included in training, with numerous controls that specify what the manner and content of training must be. However, there is a lack of comprehensive detail in this section over the cyber security team roles. Overall, this domain scores '2' for coverage.	2
Australian Government Information Security Manual Controls: Information Technology Security containing sub-sections Email Security, Cryptography and Network Security. These give controls that the agency needs to follow in order to be prepared for any cyber security attack. For example, "Control: All changes to the network configuration should be documented and approved through a formal change control process."	The ISM Controls standard identifies the need for systems and physical security. It is very broad in the subjects it covers, from Physical Security and Environments, to the security of Software, Email Clients and Networks. Divisions are further split into considerations such as Selection, Usage and Disposal, and other topics such as Policy and Infrastructure. Each of these has their own set of Objectives, Contexts and Controls so the reader can be instructed through the process of preparing their organisation. Overall, this domain scores '3' for coverage.	3
N/A	The ISM Controls document is very detailed in the steps that an agency must implement in order to safeguard the security of its user accounts, and its privileged access accounts. It explains the risks in allowing potential access to the privileged accounts, and the steps that should be taken to mitigate these. For general user accounts, the controls manual gives a larger list of measures that agencies must implement in order to reduce the risk of user accounts being compromised. Overall, this domain is very detailed and scores '3' for coverage.	3
N/A	The ISM Controls standard recognises the potential threats that an agency could face, and lists controls that should/must be adopted by the agency in order to react to, or detect, a threat. However, especially in the case of incident detections, the recommendations by the standard are simply options that the agency may consider. The standard is slightly limited in its definitive control requirements in this domain. Overall, this domain scores '2' for coverage.	**2**
Australian Government Information Security Manual Controls: Reporting Cyber Security Incidents details what agencies should do in order to encourage personnel to report weaknesses or threats, and to establish mechanisms to do so. The Controls also instructs what to do in reporting incidents as soon as possible after they occur, although it references reporting through the "Cyber Security Incident Reporting scheme" without specifics on how to do so.	The ISM Controls standard details the need for a structured response system to counter security breaches. There are several aspects of this reporting mechanism listed as well as some detail of what this must entail as well as connections to other standards and documentation such as the DSD-established Cyber Security Incident Reporting Scheme. A list of controls are given which agencies should act on and include in their incident response plans and business recovery, but the standard does not go into comprehensive detail on what exactly needs to be included in these plans, or how they might vary for different organisations. Overall, this domain scores '2' for coverage.	2

Bundesamt fur Sicherheit in der Informationstechnik (BSI) 100 Series: Parts 1 to 4

Version:	Standard 100-1 Version 1.5 Standard 100-2 Version 2.0 Standard 100-3 Version 2.5 Standard 100-4 Version 1.0
Publisher:	Bundesamt fur Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security
Date published:	May-08
URL:	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards

Cyber Security Domain	Reference 1	Reference 2
Governance	BSI 100-1 8.1 Development of the Security Concept: Classifying risks and damages, Risk assessment, Developing a strategy for dealing with risk; 9.2.1 Risk assessment: Structure analysis, assessing the protection requirements, Development of the security concept.	BSI 100-1 7.3 Performance review and improvement of the security concept: Detection of information security incidents during routine operation, Checking that the requirements are being complied with, Checking the suitability and effectiveness of information security safeguards.
People	BSI 100-2 3.4 Organisation of the security process including detailed sections on The IT Security Officer, The IS Management Team, Area IT Security Officer, Project Security Officer, IT System Security Officer, IT Co-ordination Committee and The Data Protection Officer. Each section lists Responsibilities and tasks, Requirements profile and other skills that a suitable candidate should possess.	BSI 100-4 7.1.4 Tasks and authorities of the crisis team: Information on the crisis team and what they should do in the event of a situation arising, and the potential issues that might be faced by the crisis team.
Prepare	BSI 100-2 4.3.2 Determination of the protection requirements for applications, 4.3.3 Determination of the protection requirements for systems, 4.3.4 Determination of the protection requirements for rooms has some guidance and recommendations on the security that should be in place including Action Points to follow and several examples.	N/A
Operations	N/A	N/A
Intelligence	BSI 100-2 4.2 Structure analysis, BSI 100-4 5.3 Determining the current state: Information given to help the reader to assess the current state of their security systems, in standard operations, when in danger of attack or when recovering from an attack.	BSI 100-4 5.2 Risk Analysis: The risk analysis performed in the context of business continuity management serves to identify threats that could lead to the disruption of business processes and to evaluate the associated risks. The goals of the risk analysis are the following: Make the risks present clear to the decision-makers; If necessary, to develop suitable strategies and countermeasures for reducing these risks in advance and increase the robustness of the organisation; Identify the scenarios for which individual business continuity plans need to be developed.
Respond	BSI 100-4 Business Continuity Management: The whole fourth document in the standard is based around achieving business continuity in response to a security breach. It has a high level of detail from an overview of the Business Continuity process to the finer details that need to be considered when preparing an organisation.	BSI 100-4 5.4 Continuity strategies: Business continuity and the recovery of the business processes can be realised in different ways. The alternative paths to a solution, i.e. the strategy options, differ in terms of their parameters such as the recovery time objective, the costs, and the reliability of the solution. The goal now is to identify the main alternatives and then selected the best approach for the organisation. To do this, the basic organisation-wide business continuity strategy, developed in the framework of initiating business continuity management and specified in the business continuity management policy, is applied to the process and resource levels in a top-down approach and then detailed.

Reference 3	Comments	Coverage Level
BSI 100-4 9.2 Examinations: The ability of the organisation to handle emergencies and crises can only be determined through regular examination of the business continuity management process and the contingency measures. The goal of such examinations is to ensure the operability, effectiveness, appropriateness, and efficiency of the business continuity management process. To do this, deficiencies as well as potential improvements are pointed out, and recommendations are provided.	The BSI documents give good recommendations and guidelines to be followed for the development of a risk management strategy and the processes that need to be undertaken. However, in this area, the standard lacks clear definitive instructions to follow. On audit and compliance the standards go into reasonable detail about the different levels of audits that should be performed and who should do them, but is not specific enough to achieve green status. Overall, this domain scores '2' for coverage.	2
BSI 100-4 4.6.1 Training and raising awareness, BSI 100-2 3.6.1 Training and raising awareness: Both sections identify the need for training for employees but give no more than basic guidance as to what this training might be or contain.	The BSI documents give very good specifications for the cyber security roles that should be found within an organisation, detailing extensively the tasks that they will be required to do, and the skills that they must possess. In addition, there is a less detailed section in 100-4 on the need for a crisis team, but this is not covered in the same depth as the day to day roles are in 100-2. However, documentation on training is severely lacking, with only the most basic guidance that training should be done. Despite the detailed section on cyber security team roles, that lack of information on training or human resources means that overall this domain scores '1' for coverage.	1
N/A	Although the BSI Standards recognise the need for protection requirements in order to be prepared against the risks of cyber security, they only present recommendations on what the reader could do to put these in place. The recommendations are also reasonably broad and no specific instructions about how to implement them are given. Overall, this domain scores '2' for coverage.	2
N/A	The BSI Standards do not address the issues of operations significantly, failing to consider administration or authentication concerns such as restricted accounts and access or passwords. Overall, this domain scores '1' for coverage.	1
N/A	The BSI Standards give reasonable guidance towards identifying the current state of the security system in the organisation and steps to be taken to do so, however they lack an exact guide to follow. The section BSI 100-4 5.2 on Risk Analysis is more detailed, and can be followed to a greater extent. Complete and defined standards for recognising the current state of the security systems, self-assessing the controls in place, and realising the applicable risks are not present, though. Overall, this domain scores '2' for coverage.	2
N/A	The BSI Standards' whole fourth document is centred around responding to cyber security attacks and business continuity strategies, covering in high detail what an organisation should do in order to prepare itself to deal with such an event. It details the conception and implementation of a response plan, and who is responsible for it, along with many sections on more specific aspects of response such as the use of a crisis team and immediate measures to be taken after a breach. Overall, this domain scores '3' for coverage.	3

HMG Security Policy Framework (SPF)

Version:	Version 10.0
Publisher:	Developed by: - The Government Security Secretariat (GSS); - The Centre for the Protection of the National Infrastructure (CPNI); - The National Technical Authority for Information Assurance (CESG); - The Office for Cyber Security and Information Assurance (OCSIA); and - The Civil Contingencies Secretariat (CCS).
Date published:	Apr-13
URL:	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200552/HMG_Security_Policy_Framework_v10_0_Apr-2013.pdf

Cyber Security Domain	Reference 1	Reference 2
Governance	Security Risk Management: Points 17 (Identify Assets, Assess Threats, Assess Vulnerabilities, Risk Tolerance, Implement Controls) Points 18+19 Mandatory Requirement 2	Assurance and Reporting: Point 27: Self Assessment/ Central reporting/ Parliamentary Oversight. MANDATORY REQUIREMENT 5 Departments and Agencies must have an effective system of assurance in place to satisfy their Accounting Officer / Head of Department and Management Board that the organisation's security arrangements are fit for purpose, that information risks are appropriately managed, and that any significant control weaknesses are explicitly acknowledged and regularly reviewed
People	Roles, accountability and responsibilities: Points 15 + 16 MANDATORY REQUIREMENT 1: Departments and Agencies must establish an appropriate security organisation (suitably staffed and trained) with clear lines of responsibility and accountability at all levels of the organisation. This must include a Board-level lead with authority to influence investment decisions and agree the organisation's overall approach to security.	Culture, Education and Awareness: Points 21, 22 +23 MANDATORY REQUIREMENT 3 Departments and Agencies must ensure that all staff are aware of Departmental security policies and understand their personal responsibilities for safeguarding assets and the potential consequences of breaching security rules.
Prepare	Risk Treatment – Technical, Procedural and Physical: MANDATORY REQUIREMENT 9 Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.	Security Risk Assessment: MANDATORY REQUIREMENT 16 Departments and Agencies must undertake regular security risk assessments for all sites in their estate and put in place appropriate physical security controls to prevent, detect and respond to security incidents.
Operations	Procedural Measures: MANDATORY REQUIREMENT 10 Departments and Agencies must implement appropriate procedural controls for all ICT (or paper-based) systems or services to prevent unauthorised access and modification, or misuse by authorised users.	Risk Assessment and Accreditation of ICT Systems: page 26: Record relevant information, the accreditation status and any risk management decisions in a Risk Management and Accreditation Documentation Set (RMADS) using „HMG IA Standard No. 2 - Risk Management & Accreditation of ICT Systems & Services□; Comply with specific requirements for the protection and handling of personal data as set out by the Data Protection Act (DPA)'
Intelligence	Culture, Education and Awareness: MANDATORY REQUIREMENT 3 Departments and Agencies must ensure that all staff are aware of Departmental security policies and understand their personal responsibilities for safeguarding assets and the potential consequences of breaching security rules.	Risk Assessment and Accreditation of ICT Systems: MANDATORY REQUIREMENT 8 All ICT systems that handle, store and process protectively marked information or business critical data, or that are interconnected to cross-government networks or services (e.g. the Government Secure Intranet, GSI), must undergo a formal risk assessment to identify and understand relevant technical risks; and must undergo a proportionate accreditation process to ensure that the risks to the confidentiality, integrity and availability of the data, system and/or service are properly managed.
Respond	Managing and Recovering from Incidents: MANDATORY REQUIREMENT 4 Departments and Agencies must have robust and well tested policies, procedures and management arrangements in place to respond to, investigate and recover from security incidents or other disruptions to core business.	Managing and Reporting Security Incidents: MANDATORY REQUIREMENT 12 Departments and Agencies must have clear policies and processes for reporting, managing and resolving Information Security Breaches and ICT security incidents.

Reference 3	Comments	Coverage Level
Information Security Policy: MANDATORY REQUIREMENT 6 Departments and Agencies must have an information security policy setting out how they and any delivery partners and suppliers will protect any information assets they hold, store or process (including electronic and paper formats and online services) to prevent unauthorised access, disclosure or loss. The policies and procedures must be regularly reviewed to ensure currency.	The SPF provides a very clear guide on risk management. It identifies a guideline for approaching the whole cycle of risk. This alone is slightly brief (it includes general expectations of how to deal with each area of risk.). These expectations are then explained and methods of how they can be implemented are highlighted with reference to other HMG risk assessment documents (e.g. HM Treasury Orange Book, National Risk Register etc). SPF outlines a detailed assurance policy including a set p by step process to optimise compliance with the standard. It identifies what procedures need to be followed and how to implement them (e.g.. what reports/assessments need to occur). the governance in SPF also identifies the principles that will aid the organisation to implement an information security policy. It explicitly identifies the criteria this policy must meet however the depth of detail is lacking, e.g. it fails to specify what should be included in the policy. While this standard includes a huge breadth of coverage it is lacking in detail in key areas such as policy and processes so scores '2' overall.	2
Security Policy No.3: Personnel Security: Recruitment Checks and National Security Vetting, Ongoing Personnel Security Management: MANDATORY REQUIREMENT 13 Departments must ensure that personnel security risks are effectively managed by applying rigorous recruitment controls, and a proportionate and robust personnel security regime that determines what other checks (e.g. national security vetting) and ongoing personnel security controls should be applied.	The SPF clearly identifies where the accountability of information security lies and outlines the need for a comprehensive security organisation with a clear set of responsibilities. It then goes on to list the roles that are to be filled within this organisation and that the responsibilities for each should be clearly defined. The expectations of staff members are extensively covered including awareness of risk and policies with reference to signing the Civil Service Code, Official Secrets Act, Data Protection, Freedom of Information Act as mandatory requirements. While training of staff is mentioned in a practical light (when, how often etc.) this standard is missing the depth you would expect with regards to what the training might contain. A fully detailed approach to employment vetting is listed including government checks such as BPSS, NSV, CTC,SC,DV. Overall, this domain scores '2' for coverage.	2
N/A	This standard recognises the need treat risk the organisation faces in the physical and technical environment. It clearly lays out the context and objectives for this domain. Furthermore it compliments these objectives by identifying a list of mandatory requirements that must be met along side other government procedures (e.g. Government Secure Intranet) which will help to make the policy monitorable. Overall, this domain scores '2' for coverage.	2
N/A	The SPF understands the importance of valuing the assets and restricting access appropriately, it achieves this by outlining a comprehensive policy with regards to controlling and protecting information assets. The policy must comply with other HMG standards such as Annex One, GPMS and PIA which would allow this category to be easily auditable and controlled. Overall, this domain scores '2' for coverage.	2
Preparing for Critical Incidents: 59. Departments and Agencies need to put in place effective arrangements to increase the security posture of their estate in the event of an increased threat, along with appropriate management controls and contingency plans to respond to critical security incidents including terrorist attack, incursions or break-ins. Specific measures are mandated for protection against terrorist attack, particularly for establishments that are assessed as likely terrorist targets (i.e. HIGH or MODERATE risk).	There is a focus on understanding and assessing the risks that the IT system faces and handling that risk accordingly. This is especially prevalent in the face of Counterterrorism threats where a strict monitoring and assessment criteria must be in place at all times. The SPF identifies the need for the organisation's staff to be acutely aware of their responsibilities and of the risk and thetas which they could pose to cyber security. However the standard is lacking on implementing procedures to monitor and assess cyber threat the whole organisation could face (i.e. an external threat). While this standard is detailed in some areas of this domain, it lacks the breadth it would need to be completely comprehensive. Overall, this domain scores '2' for coverage.	2
N/A	The SPF identifies both the expectations of the organisation and a clear policy on Business Continuity management. This is auditable against BS25999/ISO23201. It also identifies the need for a clear incident recovery strategy that defines detecting, reporting and responding to security breaches. While the standard identifies the need for this mechanism it doesn't include sufficient detail for the reader to formulate a comprehensive plan. Overall, this domain scores '2' for coverage.	2

Information Assurance for Small & Medium-sized Enterprises (IASME)

Version:	Version 2.3
Publisher:	IASME Consortium
Date published:	Mar-13
URL:	http://www.iasme.co.uk/images/docs/IASME%20Standard%202.3.pdf

Cyber Security Domain	Reference 1	Reference 2
Governance	4.2 Assessing the Risk Annex D: The Risk Assessment process: Fact Finding, Risk Analysis, Risk Profiling, Profile Assessment	4.3 Policy and Compliance: Objectives: - To provide management direction and support for information security in accordance with business requirements - To identify the organisation’s 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 - To ensure that organisational records are protected from loss, destruction or falsification in accordance with the organisation’s legal and other obligations - To prevent or deter the use of an organisation's information systems from misuse. - To ensure compliance of information systems with organisational policies and standards. - To ensure that system audits are effective and minimise impact on the business - To limit access to audit tools and audit information
People	4.1 Organisation: a. Ensuring commitment and funding agreement from the top of the organisation b. Appointing a senior, well informed person – often referred to as Chief Information Officer and/or Risk Owner – who will lead. c. Forming a group from across the organisation to coordinate and implement activities. d. Maintain knowledge of emerging threats and countermeasures using expert advice.	4.5 People (With mentions of screening, security briefings and obligations, security team training, termination procedures)
Prepare	4.6 Physical and Environment Protection: ('Protection of an organisation’s cyber security extends to the physical protection of information assets, to prevent theft, loss or damage. Usually this is no more than the common sense approach to door locks, window bars, video surveillance and so on, as dictated by the organisation’s physical environment. However, in some cases, physical protection may be dictated by HMG or legal requirements.')	4.4.2 BYOD Assets: Organisations should ensure that the devices have corporate-level protection, detection and recovery processes in place and that users follow the business security procedures at all times. The template IASME Policy includes asset management and disposal procedures and the Assessor will help to identify the important assets if required.
Operations	4.7 Operations and management	4.8 Access Control,: ('Users should be given access to all the data necessary for their duties, but no more (sometimes referred to as ‘least privilege’). Although most access would be user initiated, in some cases autonomous applications with user privileges may be employed.')
Intelligence	4.4 Assets: One of the key factors in both risk assessment and recovery from a cyber security incident is a good understanding of your key information assets.	4.10 Monitoring: 'Most operating systems include logging of various forms of activity on the networks. Where necessary and appropriate, these logs should be monitored for evidence of unauthorised activity. Employees should consent to regular monitoring of their business-related activities.'
Respond	4.12 Incident Management: 'Ensure breaches of confidentiality, integrity or availability of your systems are detected and dealt with; learn the lessons.'	4.13 Business Continuity: 'Plans for the management of such events should be drawn up and reviewed regularly, and tested in whole or in part so that participants in the plan understand their responsibilities.

Reference 3	Comments	Coverage Level
Assurance and Reporting: Point 27: Self Assessment/ Central reporting/ Parliamentary Oversight. MANDATORY REQUIREMENT 5 Departments and Agencies must have an effective system of assurance in place to satisfy their Accounting Officer / Head of Department and Management Board that the organisation's security arrangements are fit for purpose, that information risks are appropriately managed, and that any significant control weaknesses are explicitly acknowledged and regularly reviewed.	The IASME provides a very comprehensive outline of how to manage risk, it specifies the area of the business risk needs to be monitored and how this can be done which is given in Annex D. It priories managing risk in a way that would help to mitigate cyber threats as well as identifying a detailed guideline which would provide an organisation with sufficient detail to implement an action plan. IASME includes a guideline of what a cyber security policy must do but it is lacking in how to implement this policy. It only goes as far as recognising that it is the responsibility of management. Chapter 4.3 only briefly recognises the need for a compliance mechanism but it does not develop further on this point. Because of its lack of detail, this domain can only score '2' for coverage.	2
N/A	The IASME recognises the need for a cyber security team but does not identify the roles or the duties that are expected of them within the enterprise. Chapter 4.5 determines what human recourses security procedures are required and why these procedures are important. This is followed by suggestions of how this can be achieved (e.g. references should be checked or employees should be made aware of their security responsibilities). While it recognises the need for a procedure there is no guidance as to the requirement analysis process or implementation criteria for employment or training. Overall, this domain scores '1' for coverage.	1
N/A	the IASME briefly outlines a list of risks and threats the standard aims to mitigate . However after suggesting some examples of how this can be achieved it fails to outline clear cyber security policy requirements. Whilst it touches on some solutions there are no mandatory requirements that can be audited against. Overall, this domain scores '1' for coverage.	1
N/A	The standard briefly analyses the management's role in operating and maintaining the security system. It mentions the need to keep the operating system updated with patching, third party agreements and PCI-DSS (where applicable). While some of this is auditable against there is insufficient detail to constitute a comprehensive policy. The standard identifies a procedure for access control of information, this is outlined in enough detail for the reader to form a policy but does not specify mandatory requirements. Due to lack of detail this domain scores '1' for coverage.	1
4.9. Malware and technical intrusion: 'Malware formats are continually evolving, so it is important that the supplier includes both malware signatures and heuristic detection facilities which are supported by research and updated as frequently as possible.	The IASME identifies some areas where intelligence relating to cyber threats can be gathered. It discusses the need for risk assessments on information assets and to detect malware and technical intrusions. It also outlines the need to put in place a monitoring system to increase awareness of information threats. While it covers a lot of context an auditable policy and minimum information set are not included. Therefore this domain scores '1' for coverage.	1
4.11. Backup and Restore: 'Key information should be backed up regularly and the backups preferably kept in a secure location away from the business premises. Restores should be tested regularly in order to test the performance of the backup regime.'	In IASME several avenues of how to respond to cyber threats are explored. This is limited to being aware that the organisation should have a plan in case there is an information breach but is silent on how to implement this plan. Overall, this domain scores '1' for coverage.	1

Information Security Forum (ISF) Standard of Good Practice for Information Security

Version:	Version 5
Publisher	ISF
Date published:	May-12
URL:	https://www.securityforum.org/ (log-in required)

Cyber Security Domain	Reference 1	Reference 2
Governance	SG1.1.5: The information security governance framework should include a process that requires the governing body to direct information security activity overall by determining the organisation's overall risk appetite, endorsing the information security strategy and policy, and allocating sufficient resources. SG2.3 Information Security Assurance Programme: 'Principle: The organisation should adopt a consistent and structured approach to information risk management.' SR1.1.1: 'There should be formal, documented standards / procedures for performing information risk assessments, which apply across the organisation.'	AREA SG2 – Security Governance Components: SG2.1.1 'Information security governance should be supported by a documented information security strategy that states how information security activity will be aligned with the organisation’s overall objectives.'
People	SG1.2.1: 'A full-time Chief Information Security Officer (or equivalent) should be appointed at executive management level, with overall responsibility for the organisation’s information security programme.'	AREA CF2 – Human Resource Security: CF2.1.1 Information security responsibilities for all staff throughout the organisation should be specified in job descriptions, terms and conditions of employment (e.g. in a contract or employee handbook) and performance objectives.
Prepare	CF8.3 Critical Infrastructure: Principle Information systems that support or enable critical infrastructure should be protected by comprehensive security arrangements, which include security planning, information risk assessment and control selection, deployment, and monitoring.	AREA CF19 – Physical and Environmental Security. CF19.1 Physical Protection: Principle All critical facilities (including locations that house computer systems such as data centres, networks, telecommunication equipment, sensitive physical material and other important assets) should be physically protected against accident or attack and unauthorised physical access.
Operations	CF2.5 Roles and Responsibilities: 'Principle: Ownership of critical and sensitive target environments (e.g. critical business environments, critical processes, critical business applications, critical information systems and networks) should be assigned to capable individuals, with responsibilities for key tasks to protect critical information clearly defined and accepted.'	AREA CF3 – Asset Management: CF3.1 Information Classification: 'Principle: An information classification scheme should be established that applies throughout the organisation, based on the confidentiality of each piece of information. CF3.2 Document Management: Principle: ' Documents should be managed in a systematic, structured manner, and information security requirements met throughout the document lifecycle.
Intelligence	SR1.1.7: 'Information risk assessments should be supported by reviewing intelligence information about: a) emerging and changing threats (e.g. cybercrime, identity thief, spear phishing, watering holes and cyber-espionage attacks' etc.	CF10.2 Malware Awareness. Principle: All individuals who have access to information and systems of the organisation should be made aware of the risks from malware, and the actions required to minimise those risks.
Respond	AREA CF10 – Threat and Vulnerability Management. CF10.1 System and Software Vulnerability Management: Principle: 'A process should be established for the identify action and remediation of system and software vulnerabilities in business applications, information systems and network devices.'	AREA CF11 – Incident Management. CF11.1 Information Security Incident Management Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Reference 3	Comments	Coverage Level
AREA SR2 – Compliance: SR2.1 Legal and Regulatory Compliance: 'Principle: A process should be established to identify and interpret the information security implications of relevant laws and regulations.' AREA SI1 – Security Audit. SI1.1 Security Audit Management: Principle: 'The information security status of target environments (e.g. critical business environments, business processes, business applications (including those under development), information systems and networks) should be subject to thorough, independent and regular security audits.'	The ISF provides guidance on the content material and layout of a cyber strategy but does not go as far as outlining what these policies would be or how they would be implemented. It tackles the whole cycle of risk management in a very comprehensive way, describing a strategy to analyse the organisation's risk appetite and a way of structuring how this can be dealt with. It also provides a very comprehensive plan how to ensure compliance through a very regimented audit process. Overall, this domain scores '3' for coverage.	3
CF2.2 Security Awareness Programme Principle Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the organisation. CF2.4 Security Education / Training Principle Staff should be educated / trained n how to run systems correctly and how to develop and apply information security controls.	The ISF identifies the need for a committed security team to deal with cyber security. The standard clearly outlines the roles and suggested positions that should be taken up. The standard also clearly identifies the need for an employee cyber security awareness programme. The format and how it should be dispensed are given in great detail as well what the training should include and who it should be given too. The level of detail given throughout this domain would allow the reader to formulate a policy based on this information and to audit against it. Overall, this domain scores '3' for coverage.	3
AREA CF7 – System Management: CF7.1 Computer and Network Installations Principle Computer system, network and telecommunication installations (e.g. data centres) should be designed to cope with current and predicted information processing requirements, and be protected using a range of in-built security controls.	The ISF standard contains guidelines on best practice for protecting information held on firm's hardware as well as protecting the firm's applications. It a gives detailed context including why this protection is important and what you are protecting against as well as what the security policy should contain. This includes infrastructure and equipment and environmental protection. Overall, this domain scores '3' for coverage.	3
AREA CF6 – Access Management: CF6.1 Access Control. Principle: 'Access control arrangements should be established to restrict access to business applications, information systems, networks and computing devices by all types of user, who should be assigned specific c privileges to restrict them to particular information or systems. CF6.2 User Authorisation. Principle: 'All individuals with access to business applications, information systems, networks and computing devices should be authorised before they are granted access privileges.'	The ISF standard identifies the day-to-day responsibilities of management in order to ensure the maintenance of an acceptable level of cyber security. It provides clear guidance on policies regarding the management of information (e.g. Classification) and provides a detailed best policy outline. It also identifies the need for access management (including biometrics, tokens and sign in procedures) and provides an auditable process to protect the organisation from threats. It does not have a clear policies on management documentation and administration of the security system, while it mentions the need to documentation (particularly relating to security breaches) it does not outline the method or what to include. Overall, this domain scores '2' for coverage.	2
CF10.5 System / Network Monitoring Principle Business applications, information systems and networks should be monitored continuously, and reviewed from a business user’s perspective.	The ISF standard has comprehensive coverage on gathering intelligence on the cyber environment and how to perform a risk assessment based on that information. In this respect, the breadth would be sufficient to enhance protection from potential threats. It also includes policy on why and how monitoring of security threats and events should be contained within the security policy. Overall, this domain scores '3' for coverage.	3
AREA CF20 – Business Continuity. CF20.1 Business Continuity Strategy. Principle: A business continuity strategy covering the whole organisation should be established, which promotes the need for business continuity management, embeds business continuity management into the organisation’s culture, and is implemented in the form of a business continuity programme.	Incident and threat management are fully covered in the ISF. It documents clear guidelines covering the whole cycle of threat management: from monitoring and prevention, to response and resolution. A clear context, description, and policy suggestions are included which would be auditable against if implemented within an organisation. The Business continuity plan is equally as detailed. Overall, this domain scores '3' for coverage.	3

ISO27001:2005

Version:	2005
Publisher	ISO
Date published:	Jun-05
URL:	Not freely available

Cyber Security Domain	Reference 1	Reference 2
Governance	"4.2 Establishing and managing the ISMS. b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology; c) Define the risk assessment approach of the organization; d) Identify the risks; e) Analyse and evaluate the risks; f) Identify and evaluate options for the treatment of risks." (All followed by a more detailed plan of how this can be achieved.)	"A.5.1 Information Security Policy: Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations."
People	A.8.11 Human Resource Security.	A.8.1.2: Screening.
Prepare	A:9 Physical and Environmental Security: A.9.1.1 Physical Security Parameter, A.9.1.2 Physical Entry Controls, A.9.2.1 Equipment sitting and Protection, A.9.2.2 Supporting Utilities, A.9.2.2 Cable Security etc.	N/A
Operations	4.3 Documentation requirements: 4.3.1 General: Comprehensive list of documents that demonstrate the compliance and assessment of the ISMS and 4.3.2.: Control of Documents	A.11 Access Control (e.g. A.11.4 Network Access Control, A.11.5.1 Operating System Access Control, A.11.6 Application and Information Access Control)
Intelligence	A.10.10.1 Audit logging - "Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring."	A.10.10.2 Monitoring system use - "Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly."
Respond	A.13 Information security incident management: A.13.1 Reporting information security events and weaknesses communicated in a manner allowing timely corrective action to be taken.	A.14 Business continuity management A.14.1 Information security aspects of business continuity management. Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Reference 3	Comments	Coverage Level
"4.2.3 Monitor and review the ISMS... b) Undertake regular reviews of the effectiveness of the ISMS c) Measure the effectiveness of controls to verify that security requirements have been met."	ISO 27001 includes a clear step by step approach to risk management with a detailed outline of the full risk management lifecycle; from identifying to mitigating risk (as detailed in reference 1). It identifies a clear approach to managing risk and guideline on how to manage it. The need for comprehensive policy is outlined, as well as general considerations for what to include; but ISO27001 is not specific as to how such policy should be developed, what its minimum mandatory content must cover, or in what form it should be represented. It is notably less detailed in relation to audit and compliance considerations that on the risk management aspects of the Governance domain, so scores '2' for the domain overall.	2
5.22 Training, Awareness and Competence - "The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks"	Human resource security is mentioned outline; specifically, that there is a requirement to ensure that appropriate vetting, training and awareness activities take place. However there is insufficient detail to assure that an organisation which certifies to ISO27001 is sufficiently robust in this area; for example there is no indication of either mandatory minimum requirements or the thought process that the organisation should follow in order to identify its specific requirement (e.g. who should be trained, on which subjects, and to what level). Annex A.8 highlights the need for employment and termination policy, and the expectations of the management and staff whilst they are employed. There is a list of cyber security roles that should be introduced as part of the ISMS, however there is no indication of mandatory or indicative roles or responsibilities. Due to limited breadth in relation to the People domain, this domain scores '1' overall.	1
N/A	ISO 27001 Annex 9 identifies the security considerations that need to be addressed to protect information assets. It clearly specifies a list of physical and environmental controls that need to be put in place. However these controls are articulated as objectives; ISO27001 could add grater value by describing a process for making a risk assessment, a framework by which risks and risk appetite can be articulated, and the precise controls the organisation is going to adopt as a result. ISO27001 also doesn't provide a view on how access control can be implemented differently between infrastructure, domains, applications and data domains - it treats access control as a 'black box'. Due to inconsistency in the level of detail provided, ISO27001 scores '2' for the Prepare domain.	2
N/A	ISO27001 has a clear focus on how to control and administrate the ISMS. It also has a strong focus on the generation and maintenance of system design and configuration documentation. There are comprehensive instructions on how management can document their actions for consistency and evaluation purposes as well as which controls can be put in place to restrict the access and use of these documents. This is developed in Annex 11 which specifies ongoing access control processes to protect a system after its deployment into live use. The breadth and depth of coverage against the Operations domain give the reader a clear direction for operating the ISMS; consequently ISO27001 scores '3' for this domain.	3
N/A	While ISO27001 lists controls for logging and reviewing security events via system audit logs, there is no guidance provided as to what should be logged and how such logs should be analysed. There is also very little reference to the organisation requiring broader situational awareness of the cyber threat environment and thus the threats that the organisation faces. It contains instructions on risk assessment, but not on a specific method to understand or estimate the identities, capabilities and motivations of threat actors or the threat vectors they may utilise. Overall, this domain scores '1' for coverage.	1
N/A	ISO 27001 Annex 13 and 14 lay out how to respond to security incidents. The standard identifies the need to lay out a clear and comprehensive guideline to identify, learn from and correct breaches. The list of how to go about this has great breadth but lacks depth. There is a list of situations that need a response (under "opportunities for information leakage shall be prevented") but not how these situations should or could be managed. Overall, this domain scores '2' for coverage.	2

ISO27002:2005

Version:	2005
Publisher	ISO
Date published:	Jun-05
URL:	Not freely available

Cyber Security Domain	Reference 1	Reference 2
Governance	Compliance, 15.1 Compliance with legal requirements: Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.	ISO 27002: 5: Security Policy: 5.1.1 Information Security Policy Document. Control: An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. management commitment to information security.
People	ISO 27002: 8. Human Resources Security:8.1.1 Roles and responsibilities, 8.2 During employment, 8.2.2 Information security awareness, education, and training	N/A
Prepare	ISO 27002: 9. Physical and Environmental Security: Objective: To prevent unauthorized physical access, damage, and interference to the organization’s premises and information.	ISO 27005: 11 Information Security Risk Acceptance, pg 21
Operations	ISO 27002: 6 Organization of information security: 6.1.1 Management commitment to information security. Control: Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.	ISO 27002: 10 Communications and operations management:10.1 Operational procedures and responsibilities: 10.1.1 Documented operating procedures 'Control: Operating procedures should be documented, maintained, and made available to all users who need them.'
Intelligence	10.10 Monitoring: Objective: To detect unauthorized information processing activities. Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified.	10.4.1 Controls against malicious code: Control: Detection, prevention, and recovery controls to protect against malicious code and appropriate user
Respond	14 Business continuity management: 14.1 Information security aspects of business continuity management	13 Information security incident management: 13.1 Reporting information security events and weaknesses.

Reference 3	Comments	Coverage Level
ISO 27002:7 Asset management (including: 7.1.1 Inventory of assets,7.1.2 Ownership of assets,7.1.3 Acceptable use of assets,7.2 Information classification)	ISO 27002 chapter 5 details the requirements of a cyber security policy as well as a comprehensive list of what needs to be included in this policy. Without actually writing the policy on behalf of the enterprise this standard gives as much detail as could be expected. ISO 27002 chapter 6 and 7 show how management must implement the policy and how information assets should be controlled. ISO 27002 fully covers all aspects of governance including risk management, policy and processes. While chapter 15 covers legal and policy compliance and identifies the need for specific audit and self assessments its coverage is very vague. Details of what areas audits would be needed are not specified. Despite this slight omission the high level of detail and coverage allows this domain to score '3' overall.	3
N/A	ISO 27002 Chapter 8 identifies clear security guidelines for the whole cycle of human resources management. It gives clear objectives of what and why restrictions need to be imposed which is followed on by giving suggestions of how this can be achieved. There is a keen focus on employee security roles, responsibilities and awareness however the same level of detail is not available in regards to a formal training system nor are the expected roles of the security team mentioned or described. Because of the lack of detail in these key areas this domain scores '2' overall.	2
	ISO 27002 outlines what aspects physical and environmental security need to be considered as well as giving a detailed list of implementation guidelines (e.g. How to protect the security perimeter, the work procedures for maintaining a secure area internally etc). Overall, this domain scores '3' for coverage.	3
11 Access control:11.1 Business requirement for access control: Objective: To control access to information. Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.	ISO 27002 has a chapter containing information on how management can control the day-to-day running of the cyber security system. This includes how the SMIS should be coordinated, reported, allocating responsibilities, authorisation and reviewed. Chapter 10 develops the documentation and change management procedures within the firm and with third parties to a greater extent. Overall, this domain scores '3' for coverage.	3
N/A	The ISO27002 does not have a strong focus on gathering intelligence on cyber threats. It identifies the need for a monitoring policy as well as outlining the content but this is limited to in the event of a cyber security threat and how to deal with it within the ISMS. Throughout the standard, the need for situational awareness is stressed. Both in the employee training chapter as well as in order to mitigate potential threats (such as reference 3). I this respect the breadth is huge but the depth in this domain is lacking. Overall its scores amber.	2
N/A	The ISO 27002 lays out a clear procedure with regards to reporting and remedying a cyber security breach. This includes the responsibilities of staff members, the correct information to include and actions to take in the event of a breach. The importance of business continuity is also stressed. ISO 27002 includes a comprehensive guideline of how this policy should be designed, monitored and implemented. Because of the wide coverage and exact detail in the instructions, this domain scores '3' overall.	3

Payment Card Industry Data Security Standard (PCI-DSS)

Version:	Version 2.0
Publisher:	PCI Security Standards Council
Date published:	Oct-10
URL:	www.pcisecuritystandards.org

Cyber Security Domain	Reference 1	Reference 2
Governance	Scope of Assessment for Compliance with PCI DSS Requirements: 'The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope.'	Maintain an Information Security Policy Requirement 12: Maintain a policy that addresses information security for all personnel
People	N/A	N/A
Prepare	Build and Maintain a Secure Network Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	Protect cardholder data: Requirement 4: Encrypt transmission of cardholder data across open, public networks
Operations	Build and Maintain a Secure Network, Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. Implement Strong Access Control Measures, Requirement 7: Restrict access to cardholder data by business need to know To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.	Requirement 6: Develop and maintain secure systems and applications. 6.4.5.1 Documentation of impact. 6.4.5.1 Verify that documentation of impact is included in the change control documentation for each sampled change. 6.4.5.2 Documented change approval by authorized parties.
Intelligence	Maintain a Vulnerability Management Program Requirement 5: Use and regularly update anti-virus software or programs	Regularly Monitor and Test Networks Requirement 10: Track and monitor all access to network resources and cardholder data. Requirement 11: Regularly test security systems and processes: Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.
Respond	12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	N/A

Reference 3	Comments	Coverage Level
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	The PCI-DSS identifies the need for compliance by the organisation, it lists the areas and the tests that it expects the organisation to undertake. It also gives 'Instructions and Content for Report on Compliance' which give a step by step contents requirement detailed enough for the reader to audit against the documentation. The standard has both broad and deep coverage of the inclusion of a security policy. The comprehensive detail would allow the reader to set up and maintain an auditable policy. Risk management is only briefly mentioned, it identifies the need to evaluate risk in the face of threats but if goes into little or not detail as to how or why. Overall, this domain scores '2' for coverage.	2
N/A	No information on cyber security roles or responsibilities of staff are given. There is also no mention of implementing training or awareness exercises for staff. Overall, this domain scores '1' for coverage.	1
Requirement 9: Restrict physical access to cardholder data. 9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	The PCI-DSS gives a very detailed list of requirements with regards to making the organisation's systems are security. Each requirement and how to achieve it are listed in a table where they can be checked off under the heading 'in place or 'not in place'. The physical environment is identified as a risk to cyber security, measures to mitigate this risk from the organisation's premise and people are fully detailed. Testing procedures are included to ensure full compliance. Overall, this domain scores '3' for coverage.	3
N/A	PCI-DSS details the authorisation process that is required for members of the organisation and vendors to protect sensitive information. The need for an administrative procedure is mentioned along with the need for documenting policy and test results. The jurisdiction of this along with the content are not mentioned. Due to the broad coverage of day to day management operations but the lack of detail, this domain scores '2' for coverage overall.	2
N/A	The PCI-DSS identifies the need for monitoring and mitigating threats to the system. It covers how this can be instigated in depth but the information it contains is restricted, not encompassing all aspects of information security, only those relating to sensitive data protection. It is also lacking information in gathering and assessing intelligence in the form of situational awareness and risk assessment. Overall, this domain scores '2' for coverage.	2
N/A	PCI-DSS recognises the need for an incident response plan. It details the minimum requirements for this plan including Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands and specific incident response procedures. However it does not mention how these procedures should be implemented. Neither does it detail a Business continuity strategy. Overall, this domain scores '1' for coverage.	1

Publically Available Standard (PAS) 555 (including Annexes)

Version:	2013
Publisher:	British Standards Institute (BSI)
Date published:	May-13
URL:	http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030261972

Cyber Security Domain	Reference 1	Reference 2
Governance	Clause 12 (Risk Assessment): The organisation shall… 12.2) ...categorise its assets according to their value… register, track and manage [them]… with suitable controls over who has access. 12.3) ...identify the actual and potential threats and hazards to assets. 12.4) ...identify new and existing vulnerabilities so that remediation... can be carried out.	Clauses 7-9 (Strategy): The organisation shall… 6) …include cyber security in the through-life management of the organisation… 7) …have cyber security awareness programmes, training and development… 8) …manage its cyber security risk across the organisation and its business partners, suppliers and customers... 9) ...include cyber security as part of [IT procurement] choices... as part of its change impact assessment... implement practices that identify new vulnerabilities... control access to assets... [and take] the opportunity to enhance cyber security where the assessed risks demonstrate the need.
People	Clause 3 (Management Structure): The organisation shall: a) Have an owner of cyber security within the organisation at a level of seniority commensurate with the size and scope of the organisation and the exposure to security risk. b) Clearly define and allocate cyber security responsibilities, authority and resources within the organisation.	Clause 7 (Capability Development Strategy): The organisation shall have cyber security awareness, training and development, so that all individuals in the extended enterprise have the awareness and competence to fulfil their cyber security role and contribute to an effective cyber security culture.
Prepare	Clause 13.2 (Physical Security): The organisation shall identify physical vulnerabilities and susceptibilities, and implement physical security controls in accordance with the risk assessment…	Clause 13.3 (Technical Security): The organisation shall implement technical security controls to protect itse assets.
Operations	Clauses 12.2 (Asset Management): The organisation shall identify, and understand, its assets… so that... c) Access to assets is known, understood and managed with suitable controls over who has access (in use, in storage, during transportation, configuration, etc.	N/A
Intelligence	Clause 14.1 (External Awareness): The organisation shall collect, monitor, analyse and share (with trusted partners) information/intelligence on any new, existing or changing cyber security threats…	Clause 14.2 (Internal Monitoring): The organisation shall… a) Define and maintain its capability to detect that a cyber security event or incident has occurred and what action it takes in response. b) Maintain an audit trail of its internal monitoring activities and actions taken.
Respond	Clause 10 (Business Resilience): The organisation shall idenitfy and implement the level of resilience it needs commensurate with the types of services it provides and the assessed risks.	Clause 14.4 (Cyber Security Incident Management): The organisation shall identify how it prepares for, and is able to take command and control of, an incident and how it determines an effective response…

Reference 3	Comments	Coverage Level
Clause 11 (Compliance): The organisation shall: a) Identify the regulations that it needed to comply with… b) Identify the standards and guidelines that the organisation could comply with to minimise its vulnerability to cyber security threats… c) implement regulations, legislation, chosen standards and guidelines in a way that enhances cyber security.	PAS555, being a standard aimed at stipulating what governance arrangements organisations need to put in place in order to decide how to achieve a set of cyber security business objectives (rather than stipulating the controls required to achieve those objectives directly within the standard), is more detailed in the Governance domain than any other. Approximately a third of the document is dedicated to the issues of risk assessment, strategy formulation and compliance tracking; all of which are sub domains within the Governance domain. PAS555 indicates high-level business objectives within the main body of the text, supplemented by the identification of a relatively large number of indicative controls from other well-known cyber security standards within Annex A. It (deliberately) gives little details as to methodologies for assessing risk or implementing good audit practices however. Overall, this domain scores '2' for coverage.	2
Clause 13.1 (People Security): The organisation shall identify and take steps to minimise, mitigate or manage risk to the organisation posed by people from both inside and outside the organisation…	PAS555 maintains a strong emphasis on management buy-in and direction in order to deliver a cross-organisation security culture. It mentions that ownership of cyber security should be given at a 'appropriate' level of seniority, but does not give an indication as to the likely role(s) involved. PAS555 also mentions that a training strategy is required, but not what form this could take. Overall, this domain scores '2' for coverage.	2
Clause 16 (Compliance Analysis and Continual Improvement): The organisation shall demonstrate how it learns from and improves its cyber security and resilience position so it can respond to developing and dynamic (active) threats and hazards.	PAS555 states that vulnerabilities associated with the organisation's physical environment must be identified and mitigated, but provides no guidance as to what the reader should look for or what process they should follow to gain comfort that their residual risk position is acceptable. Overall, this domain scores '1' for coverage.	1
N/A	PAS555 covers Operations to the least extent of any of the domains. With the exception of stating that asset management and access control must occur, it is silent on operational issues. Overall, this domain scores '1' for coverage.	1
Clause 14.3 (Protective Monitoring): The organisation shall determine and collect information available from diverse sources, both within and outside the organisation, that allows the identification of trends and anomalies that might indicate breaches of security and inform the threat assessment.	PAS555 emphases that the organisation must gather (and where appropriate share) intelligence regarding the prevailing threat that it faces through system monitoring, and then apply this knowledge through its continuous improvement processes. It does not indicate what information should be gathered, what process should be followed for the organisation to determine what should be gathered, or who should analyse it and how. Overall, this domain scores '1' for coverage.	1
Clause 15 (Recovery): 15.1 Investigation 15.2 Data Integrity Reassurance 15.3 Business-As-Usual Restoration 15.4 Legal Process	PAS555 dedicates approximately a third of its substantive word count to clauses that address the Respond domain. Resilience is strongly reenforced as a key requirement; along with the organisation's ability to restore services as quickly as possible and investigate what happened after an incident. There is more detail provided regarding specifically what the organisation must do compared to the Prepare, Operations or Intelligence domains. Overall, this domain scores '2' for coverage.	2

This publication is available from www.gov.uk/bis

Any enquiries regarding this publication should be sent to:
Department for Business, Innovation and Skills
1 Victoria Street London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000

BIS/13/1294