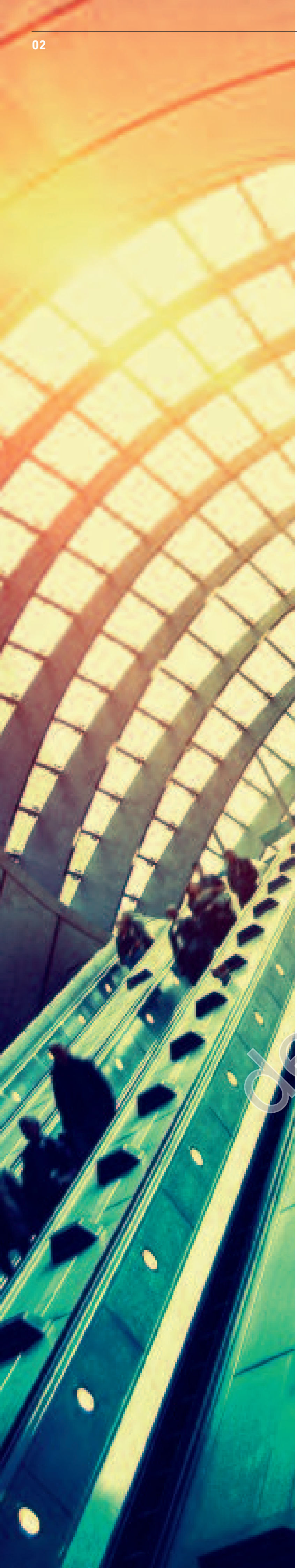
bcs
The
Chartered
Institute
for IT

Standards that
create the outstanding

Information security

The case for a global skills framework

enterprise.bcs.org



Information security

The case for a global skills framework

Introduction

The explosive growth of digital communications since the advent of the internet has been accelerated by the evolution of web 2.0 (social computing) and the pervasive availability of mobile computing technologies. This has led to a societal expectation of being ‘always connected’ in our personal and professional lives.

The explosive growth has reduced the barriers of distance, time, language and culture, enabling information to be shared by anyone at global scale at a moment’s notice and at negligible cost.

It has also brought with it a cornucopia of threats to information security, and spawned a new domain of the IT profession dedicated to protecting the confidentiality, integrity and availability of IT services.

The information assurance/information security (IA/IS) domain of the profession lacks a unified and global skills framework with a common taxonomy or consistent method of assessing competence (knowledge, skills, experience and behaviour) at progressive levels.

The situation is not helped by the myriad of qualifications, frameworks and awarding and professional bodies operating in the IA/IS arena. Neither is it aided by the widespread overuse of the imprecise word ‘cyber’ as an epithet for all manner of risks, threats, events and measures in the IA/IS domain of IT. The word cyber is popularly and widely used by the press and media to add an aura of deeply technical subject matter and drama to a news story, e.g. cyber security, cyber defence, cyber attack, cyber warfare and cyber bullying, yet nobody can define what it means.

For the purposes of clarity, this whitepaper uses the acronym IA/IS throughout and refers to the confidentiality, integrity and availability (CIA) of data and the security of the IT systems and networks that store, retrieve, transmit and process that data. Experts may argue that the subject of information risk should also be in the scope of that definition; in this whitepaper the term IA/IS will suffice to embrace that topic as well.

The case for a global skills framework for IA/IS practitioners

The IA/IS domain of the IT profession is truly global in reach. It affects all aspects of IT from strategy to operations, scientific research to product design and development, and most importantly the behaviour of all who interact with IT systems from kernel hackers to consumers.

Increased IA/IS awareness, knowledge, skills and desirable behavioural change are required from the top to bottom of organisations, in all industries and sectors. The IA/IS domain of IT is not just for cryptographers and government intelligence agencies. Rather it is for all who value the information they are entrusted with, whether it be the PIN for their bank card, their employer's latest patent, or their nation's blueprint for a new strategic nuclear submarine.

Given the ubiquitous nature of computing and IT, and the need for IA/IS to be considered in all aspects of the profession, the knowledge and skills required of an IA/IS practitioner are not limited to a specific country, job role, career path, industry or application of IT; rather they are pervasive and range from broad generalist skills to very deep specialist skills. As such IA/IS skills are needed in the profession at all levels and throughout society in general, since we are all personally responsible for the security of information with which we are entrusted.

No matter which skills framework an organisation might choose, the responsibility for developing IA/IS knowledge and skills is one we all share. All of us in the information society must raise our awareness of the risks of operating in cyberspace, and develop new skills and change our behaviour to meet the ever evolving range of threats.

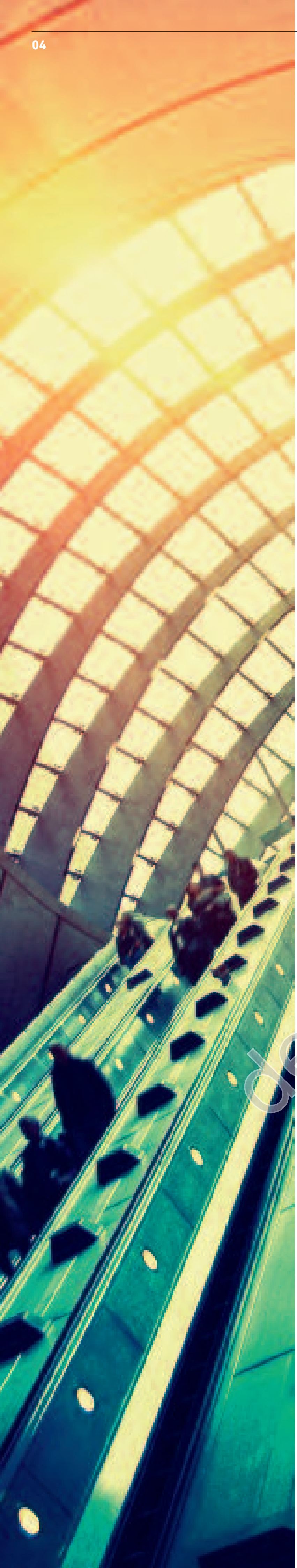
This sort of society-wide educational program is now commonly referred to as cyber-hygiene. The UK has such a programme underway at present in the Cyber Streetwise campaign.

Why the IA/IS practitioner must be both technologist and humanist?

IA/IS practitioners must possess not only technical skills, but also exceptional skill in dynamic thinking. They must be prepared to challenge the status-quo if the organisations they support are to have a hope of keeping ahead of the ever changing spectrum of threats to information security. If we rely on technical countermeasures alone, those intent on doing us harm in cyberspace will constantly be ahead of our ability to counter new and evolving threats.

An effective IT security strategy must employ not just the reactive and defensive measures that can be offered from technical solutions; it must also encourage proactive and anticipatory measures borne of understanding human behaviour and motivations of those intent on doing us harm.

Learning about human behaviour and motivation will enable the IA/IS practitioner to understand the attacker as an individual; and in doing so, they may be able to find solutions outside of the realm of a conventional technical defence – such as wasting the attacker's time or distracting their attention to false targets (technical honey traps and goldfish bowls).



Developing skills in understanding human behaviour and motivation will allow the IA/IS practitioner to anticipate and adapt to emerging and evolving threats while developing new technical skills that will allow them to design and implement an effective IT security defence.

What benefits would a global skills framework offer, and to whom?

A global skills framework for IA/IS practitioners will offer tangible benefits to stakeholders across the IA/IS domain and to society as a whole.

For employers, who have a need for IA/IS practitioners to cope with increasing security threats, it will provide a flexible structure for training and development programmes to support employees in this rapidly expanding area.

For recruiters, it will provide an independent and objective assessment of the competence of potential candidates at various level of seniority.

For educators and awarding bodies, it will provide a consistent definition of competency levels and shared vocabulary that can be used to create courses and qualifications that may be objectively compared and aligned with the needs of employers.

For policy makers, it will provide a method of identifying skills needs in the market and availability of those skills in the workforce at both national and global scale.

For job seekers looking for an exciting and challenging career with excellent rewards, it will provide a comprehensive career path in the IA/IS domain.

For existing IA/IS practitioners seeking further development, it will provide a structured career path with assessment of competence at progressive levels.

Finally, for society, a unified IA/IS skills framework will assist governments, businesses, professional bodies and individuals in being better prepared to tackle the security challenges that are an inherent characteristic of the information society.

What skills would be in such a framework?

In order for practitioners to deal with the ever evolving IA/IS challenges, the framework will need to cover critical skills that allow for the practitioner to adapt to the latest technological and sociological advances.

As such, the framework will need to include, but not be limited to, the following subjects:

- consulting
- cyber ethics

- digital forensics
- compliance, governance and regulation
- IA methodologies and testing
- IA/IS hygiene
  (best practice for all in the information society e.g. effective patching regime and access control etc.)
- implementation of secure systems
  (including physical security)
- incident management
- information risk management
- operational management
- research and development
  (to ensure we have security and privacy by design)
- strategic planning
  (extra-national, national and organisational levels)

Each of the above subject areas will require a core body of knowledge that can be built upon at different levels. This modular design will reflect the need for different skills within and without the profession at varying levels.

With the increasing governance of the IT sphere, it is critical that any framework includes knowledge of relevant governance and regulation requirements (such as the Data Protection Act and ISO 27000).

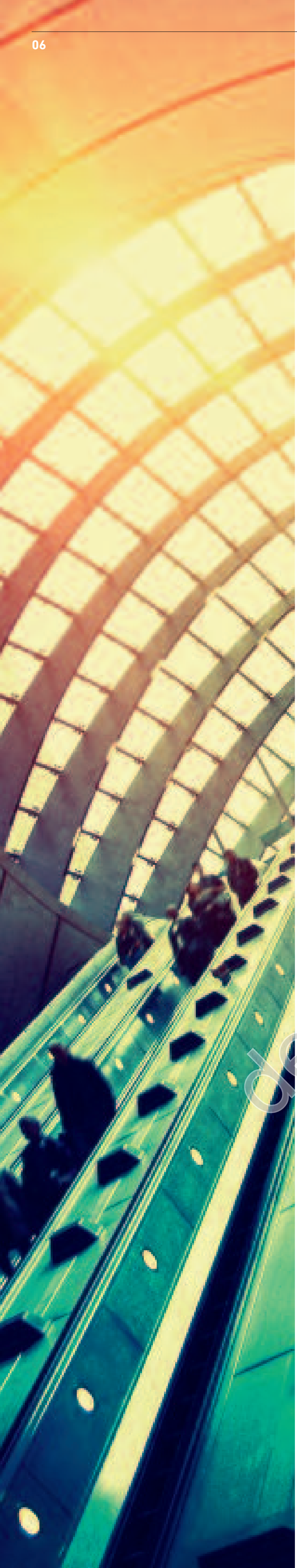
BCS, The Chartered Institute for IT, has already developed a successful model for assessing a breadth of IT knowledge in the second stage of their three-stage Chartered IT Professional (CITP) registration process – a professional competence assessment for senior IT practitioners. A similar IA/IS-specific breadth of knowledge test might be envisaged to assess knowledge of the subject area list above.

What frameworks are already operating in the field of IA/IS skills and qualifications?

There are a huge number of organisations currently engaged in IA/IS skills and qualifications, reflecting the explosive growth in demand for skills and formal qualifications among employers, job seekers and recruiters.

Some of the most notable organisations and frameworks include:

- the Institute of Information Security Professionals (IISP) Skills Framework
- the UK Government's Communications-Electronics Security Group (CESG) Information Assurance Role Definitions based upon the IISP framework
- the US National Initiative for Cyber Education (NICE) Cybersecurity Workforce Framework
- the e-skills UK National Occupational Standards for Cyber Security
- the joint initiative between two US-based professional bodies: the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronic Engineers (IEEE) Computing Society's programme



for undergraduate Computer Science degrees (CS2013) includes IA/IS concepts

- (ISC)^2 provides a range of qualifications emphasising different aspects of IA/IS skills

These models tend to be influenced by the security priorities of the countries in which they are developed – leading to the various models emphasising different aspects of IA/IS, sometimes in context of wider IT professionalism but in most cases treating IA/IS either as a distinct and separate discipline or only loosely coupled to IT.

None of these frameworks fully address the need for a model that identifies progressive levels of competence from foundation to the most senior levels in business. Neither do they integrate with other IT/computing skills in any consistent manner; rather they treat IA/IS as if it were a specialist skill, set apart from the wider IT profession.

This separation of IA/IS from IT is a fundamentally flawed approach since IA/IS skills are an integral aspect of IT and computing, needed at all levels of competence and applicable globally. While there are areas of specialism in the IA/IS domain, they do not sit clean and apart from IT, at least not unless the IA/IS skills are deployed in an entirely paper-based economy!

How can such a framework be implemented?

What is needed is a unifying model that brings together the best of the existing IA/IS skills frameworks and integrates them into a single framework with well defined levels of increasing functional skill mapped to the skills required of an IT professional. Thankfully the IT profession has such a model in the Skills Framework for the Information Age (SFIA), a mature and proven model that is now used in over 100 countries and is entering its 6th major iteration at the time of writing.

SFIA is well placed to integrate IA/IS skills across the framework. One recent analysis identified that the SFIA framework would need only about 20 new skills to be defined at various levels in the framework in order to fully envelope the need for IA/IS skills.

SFIA also lends itself to segmentation, hence there is no reason why an organisation could not extract from SFIA just the sub-set of IA/IS skills and level descriptions required for a specialist 'single track' career path, as currently specified by some professional bodies operating in the IA/IS domain.

Whether SFIA or some other model is adopted, we should be mindful that an ever evolving, amorphous and sprawling spectrum of threats will require constant evaluation of the skills required of the IA/IS practitioner. Fortunately SFIA is an open standard that is reviewed regularly and updated frequently, based upon the needs of industry and led by the profession.

How would existing qualifications fit into such a framework?

Existing qualifications could all be mapped to the framework without adaptation if SFIA were simply expanded to include the skills defined by existing IA/IS frameworks. Doing so would also help identify gaps and overlap in the skills definitions currently employed, and bring uniformity to the way that IA/IS skills are defined.

New qualifications would likely be necessary at the lower levels, especially for IA/IS operational technicians, since existing qualifications tend to aim at a level of influence, autonomy, complexity and business skills commensurate with SFIA level 5 or higher.

A positive step has been taken by the Cyber Security Skills Alliance, a grouping of UK-based organisations including the IET, BCS, e-skills UK, IISP and the Information Assurance Advisory Council (bringing together public and private sector organisations). The alliance has as one of its aims the creation of an identified career path for IA/IS professionals.

What are the risks associated with not embracing such a framework?

The cornucopia of professional bodies, commercial organisations, government agencies and trade associations offering various IA/IS skills frameworks and qualifications feeds on the demand for the skills and opportunities to generate income from a proliferation of new qualifications. This situation will persist until the market matures and common standards are adopted.

Until that time, there are some very clear risks for organisations that have a demand for IA/IS qualified practitioners:

Diluted impact

The existing skills frameworks emphasise different aspects of IA/IS, leading to polarisation of skills into thematic areas driven by the priorities of the localised political, economic, social and technological environment in which the skills framework has been developed.

Divergent qualifications

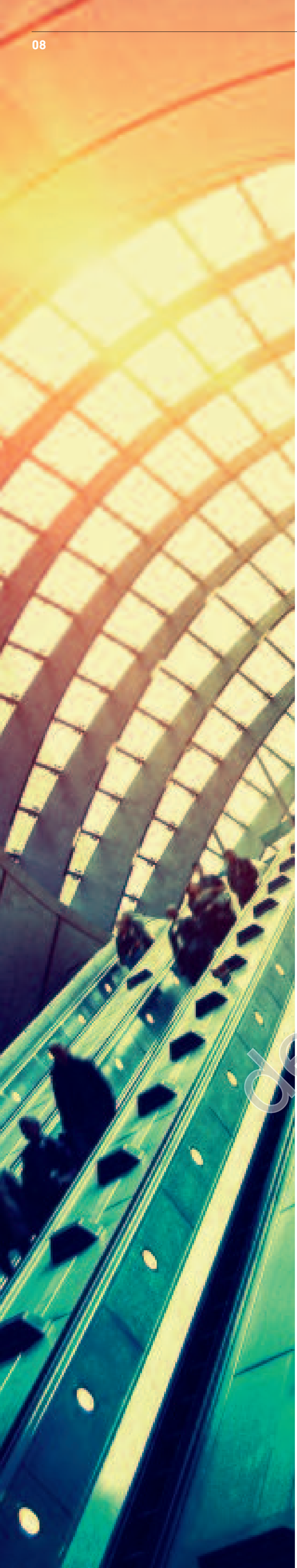
Most of the skills frameworks have associated qualifications that evaluate knowledge, skills and possibly even competence, but not in any systematic manner that can be easily compared across qualifications from different providers.

Employer confusion

There is no objective way to compare the relevance or rigour of the various skills frameworks and qualifications, at least not in any readily accessible manner that doesn't involve extensive research, benchmarking, analysis and creation of a mapping model.

Lack of common taxonomy

As is so often the case with any field of expertise, there is little in the way of



consistent understanding of terminology, or definitions of skills and levels among the various entities offering IA/IS skills frameworks and qualifications. The widespread use of the word 'cyber' is the perfect illustration of a commonly used word that has no widely accepted or consistent definition.

What skills and qualification gaps would need to be filled by the framework?

Despite the fact that IA/IS frameworks are currently in existence, many of the existing qualifications, frameworks and professional bodies emphasise different aspects of IA/IS. One thing they all share in common is the perspective of IA/IS being a specialist domain of IT practice. Existing qualifications fall into three broad categories:

- those emphasising deep technical consulting skills
- those focusing on IA/IS management and governance
- those segmenting IA/IS into narrowly defined functional tasks

Two aspects of IA/IS are poorly served by existing qualifications:

- technical operations and support staff
- generalist knowledge of IA/IS for the wider IT profession

This last point reflects the fact that generalist IT qualifications often treat IA/IS as a specialist domain that is not integral to core IT practitioner knowledge and skills at all levels. It is therefore understandable that the professional bodies involved in IA/IS skills and qualifications have responded with their own frameworks and qualifications that present IA/IS as a specialist domain not integrated into wider IT practice.

The inclusion of information risk management, incident management and digital forensics into a unified framework will help fill the gap for small and medium-sized enterprises to develop their own capabilities in-house. The skills framework will also help fill the gap left by poor cyber hygiene, aided by initiatives such as the BCS Cyber to the Citizen campaign. This, in combination with effective risk management techniques, will help professionals identify key vulnerabilities in their systems and respond effectively.

With the increasingly borderless expansion of cyberspace, the need for effective compliance and regulatory control is essential in order to maintain the security of our systems. This is not covered in many IT skills frameworks. By introducing compliance, governance and regulation into a unified framework, it will help IA/IS practitioners increase their awareness of current procedures as well as helping them implement such systems in their organisations.

How would such a framework be supported by professional bodies?

A great advantage of SFIA is that it is freely available and easily adopted and adapted to the needs of different organisations in the public, private and charitable sector. Any professional body may use SFIA, and the model has

already been proven at global scale in academic, government and private sector organisations across many industries. SFIA is backed by a number of key sponsors including BCS The Chartered Institute for IT, The Institution of Engineering and Technology, the IT Services Management Forum (ITSMF) and e-skills UK.

The flexible, scalable and essentially pragmatic nature of SFIA, combined with the fact that it may be freely accessed and used, means it is ideally suited as a skills model for any professional body operating in the IT domain.

Integrating IA/IS skills will strengthen SFIA and offer the attraction of a single framework that could be used by IISP, BCS, ACM, IEEE-CS and others.

Any organisation wishing to embrace SFIA should also develop a code of conduct for IA/IS professionals, and ideally build a community of practice that fosters knowledge sharing, access to expertise, peer review and continuous professional development.

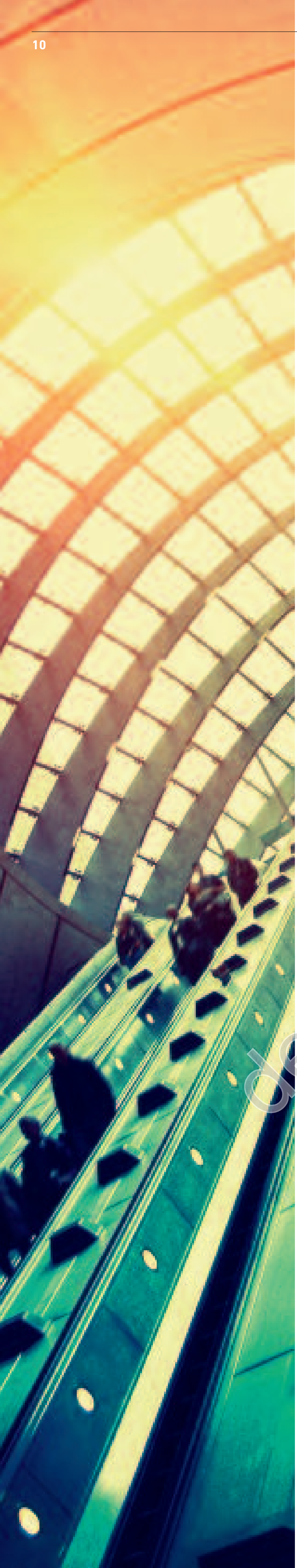
Conclusion

The market for IA/IS skills and qualifications has driven an explosive growth in initiatives of all shapes and sizes, most of them influenced by the needs of governments and big business in Europe and North America.

There are many competing and conflicting skills models, each supporting different qualifications aimed at different aspects of IA/IS; none aligned to a unified model and certainly none that are substantially integrated into the wider IT profession. This situation makes it difficult for employers, recruiters, job seekers, policy makers and educational institutions to navigate and make sense of the different paths to professionalism.

That said, much useful work has been done, especially by professional and awarding bodies, and the time is right to embrace the work of these organisations within an open and flexible framework based upon SFIA.

The next iteration of SFIA (version 6) should combine the work already done by IISP and NICE into SFIA with its well defined level descriptions. Doing so would combine the best of what has already been achieved, while allowing organisations to extract from SFIA a sub-set of skills in the IA/IS domain that provides just the elements needed by professional bodies, governments, educational institutions and businesses to identify the career path for an IA/IS professional.



References

Institute of Information Security Professionals
www.iisp.org

International Information Systems Security Certification Consortium
www.isc2.org

National Initiative for Cyber Education
http://csrc.nist.gov/nice

Skills Framework for the Information Age
www.sfia-online.org

IEEE Computer Society
www.computer.org

Cyber Security Skills Alliance
www.theiet.org/policy/key-topics/cyber-security/skills-alliance.cfm

IEEE Computer Society
www.computer.org

e-skills UK
www.e-skills.com/professional-development/cyber-security

BCS, The Chartered Institute for IT
www.bcs.org

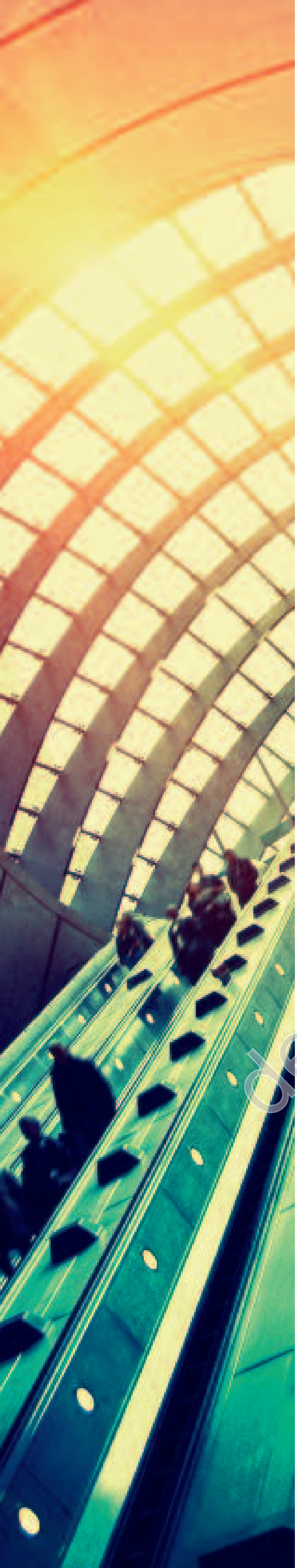
National Technical Authority for Information Assurance
www.cesg.gov.uk

About the authors

Elizabeth Phillips is a doctoral research student at Oxford University's Centre for Doctoral Training in Cyber Security. Elizabeth is researching Social Network Analysis and is working on creating a Cyber Security Skills model for South Africa. Prior to the course, she worked alongside Professor Sadie Creese and Oxford University's Cyber Security Group, developing the education and standards dimensions of the Global Cyber Security Capacity Building Centre.

Paul Jagger is a Chartered IT Professional and Fellow of BCS, The Chartered Institute for IT. He holds an MSc in Management from the University of Hertfordshire and is secretary of the BCS Learning & Development Specialist Group (BCS L&D SG). He is currently employed by IBM United Kingdom Limited in a business development and consulting role.

Christopher Jagger has held key and latterly senior advisory positions within the Metropolitan Police, National Criminal Intelligence Service, NATO and the United Nations. Chris holds an MA in Intelligence and Security Studies and has published in various journals, newspapers and most recently a book on training the intelligence community. He now works as a consultant and education advisor to police, military and intelligence agencies around Europe.



About BCS

We help global enterprise align its IT resource with strategic business goals. We work with organisations to develop people, forge culture and create IT capabilities fit to not only lead business change but to meet companywide objectives and deliver competitive advantage.

IT has been gaining momentum within global business for decades and we've been there from the beginning, nurturing talent and shaping the profession into the powerhouse that's now driving our digital world. Today organisations partner with us to exploit our unique insight and independent experience as we continue to set the standards of performance and professionalism in the industry.

Call us on +44 (0) 1793 417 755 or visit us at enterprise.bcs.org

BCS The Chartered Institute for IT
First Floor Block D North Star House North Star Avenue Swindon SN2 1FA
T +44 (0) 1793 417 755 **enterprise.bcs.org**

If you require this document in accessible format please call +44 (0) 1793 417 600