

BCS Young Professionals Information Security Group

Securing a solid career path in Information Security – Part 1

Infosecurity Europe 2010

29th April 2010

Can you keep IT a secret?

BCS London, 26th May 2010

Penetration testing training day

Warrington, 15th July 2010

BCS-ISSG AGM

IBM, Bedfont, 16th September 2010

Privacy Day

BCS London, 24th November 2010

Annual Conference 2011

Bletchley Park, 17th and 18th March 2011

YPISG Workshop – Morning Session



- 11:15 – 11:40 Workshop introduction, Mike Westmacott
- 11:40 – 12:00 Mike Case – The Recruiters Perspective
- 12:00 – 12:20 Paul Midian – Consulting with a Director
- 12:20 – 12:40 Jon Hall – Charting your way with Education and Accreditation
- 12:40 – 13:15 SFIPlus Skills Gap Analysis Part 1 – Self Assessment

YPISG Workshop – Afternoon Session



- 14:00 – 14:05 Workshop introduction, Mike Westmacott
- 14:05 – 14:10 Gap analysis reports explanation
- 14:10 – 14:40 Gerry O’Neill –
- 14:40 – 14:45 Breakout group allocations
- 14:45 – 15:55 Breakout groups
- 15:55 – 16:00 Workshop close

What's important in an Infosec career?



Why is getting certification
and accreditation most
important?

Why is getting valid
experience most
important?

The recruiter's perspective

Mike Case



Mike Case

MBCS

Director, Red Top Resources Ltd

mike.case@red-top.co.uk
01256 890100

Recruiting in IT since 1987
Started Red Top in 2002
Specialising in InfoSec since 2005

The recruiter's perspective

Mike Case



Entry Level

- **Employers**

- **All companies in Private sector, Security Consultancies.**
- **1st / 2nd Line Support of Firewall / Email Security**
- **BSc / MSc Information Security. Royal Holloway, Open and many other Universities now have reputable courses**

- **Average Salary**

- **£20,000 – £30,000**

The recruiter's perspective

Mike Case



Technical Security

- **Employers –**
 - **All companies in Private sector, Security Consultancies.**
 - **CISSP**
 - **Internet & Network Security**
 - **Firewall Installation & Design**
 - **Intrusion Detection**
 - **Perimeter Security**
 - **3rd Line Support**

Average Salaries

- **£30,000 – £40,000 (Support)**
- **£35,000 – £45,000 (Installation / Design)**

The recruiter's perspective

Mike Case



Security Consultancy

- **Employers** – Security Consultancies, Big 4 Consultancies, Government Departments / Public Sector, Large Bluechips.
 - CESG CLAS Consultant (Security Cleared)
 - Security Audit & Compliance – ISO27001 Lead Consultant
 - Security Architect / Infrastructure Design
 - PCI Security – PCI-DSS, PA-DSS (QSA)
 - PKI / Encryption Specialist
 - CESG CHECK Team Leader / Member (Security Cleared)
 - Penetration Test Consultant (CREST / TIGER)
- **Average Salary** – £40,000 – £80,000 / £450-800 per day (contract)

The recruiter's perspective

Mike Case



- **How to get the best out of a recruiter**

- Remember

- Recruiters are not perfect!
- Recruiter does not have 100% control over the process
- Recruiter is paid by the employer

- Tips

- Convince Recruiter that you are serious about the opportunity
- Covering letter
- Relationship
- Reliability
- Honesty/Integrity

The recruiter's perspective

Mike Case



- **InfoSec Career Advice**

- Clear Commitment
- Build personal network - stay in touch
- Linked In + Social Networking
- Reputation/Profile – References, Articles, Conferences

Consulting with a Director

Paul Midian

Paul Midian

MBCS

Director of Consultancy, Information Risk Management plc

paul.midian@irmplc.com

15 years of experience in InfoSec
CLAS consultant
CHECK team leader
CISSP
ISEB Business Continuity Practitioner
Chair of the CREST standards committee

Jon Hall
FBCS CITP
Senior Researcher and Lecturer, The Open University

J.G.Hall@open.ac.uk

25 year academic career
CITP Assessor

Editor-in-chief: The Journal of Software Advances
Editor-in-chief: Expert Systems – The Journal of Knowledge Engineering

SFIPlus Skills Gap Analysis – Part 1

• SFIA – Skills Framework for the Information Age



BrowseSFIPlus™

[Home](#) [SFIPlus](#) [Search SFIPlus](#)

Browse SFIPlus

Version: 4

To view details click on:-

- one of the 86 Skills (eg Corporate governance of IT) or
- a Level number (ie 1,2,3,4,5,6 or 7) or
- one of the 290 Tasks available (eg Corporate governance of IT at Level 6)

	Code	Tasks available						
		1	2	3	4	5	6	7
Strategy and architecture								
Information strategy	☆☆☆ Corporate governance of IT	GOVN					6	7
	☆☆☆ Information management	IRMG			4	5	6	7
	☆☆☆ Information systems coordination	ISCO					6	7
	☆☆☆ Information policy formation	DPRO				5	6	
	☆☆☆ Information security	SCTY		3	4	5	6	
	☆☆☆ Information assurance	INAS				5	6	7
	☆☆☆ Information analysis	INAN				4	5	6
	☆☆☆ Information content publishing	ICPM		2	3	4	5	6

SFIPlus Skills Gap Analysis – Part 1



- **Skills gap analysis**
 - Identify where your skills are
 - Rate them
 - Compare to target roles
 - Create a training and development plan

SFIPlus Skills Gap Analysis – Part 1



- **SFIA covers the whole IT industry**
 - Light in certain areas of security
- **IISP – Institute of Information Security Professionals**
 - Security Skills Framework

The IISP Security Skills Framework is copyright © The Institute of Information Security Professionals. All rights reserved.

The Institute of Information Security Professionals®, IISP®, M.Inst.ISP®, and various IISP graphic logos, are trademarks owned by The Institute of Information Security Professionals and may be used only with the express permission of the Institute.

SFIPlus Skills Gap Analysis – Part 1



- **How to measure your capability?**
 - Don't understand the examples – probably low rating
 - Finding faults and things missing – probably high rating!
- **Don't worry too much**
 - It's not a test

0 – no experience at all

1 – minimal, awareness only

2 – practical experience

3 – good experience

4 – absolute expert – why are you here?!

SFIA Skills Gap Analysis

Skills Descriptions



Corporate Governance of IT – GOVN

- Establishing frameworks to develop and maintain appropriate information security expertise within an organisation.
- Gaining management commitment and resources to support the governance structure.
- Incorporating physical, personnel and procedural issues into the overall security governance process.
- Relating an organisation's business needs to their requirements for information security.
- Encouraging an information risk awareness culture within an organisation. For example, raising awareness of how the various forms of social engineering can be used to compromise information.
- Establishing frameworks for maintaining the security of information throughout its lifecycle

SFIA Skills Gap Analysis

Skills Descriptions



Information policy formation – DPRO

- Developing and maintaining organisational security policies, standards and processes using recognised standards (such the ISO 27000 family) where appropriate.
- Developing and maintaining standards for appropriate personnel screening.
- Developing and maintaining standards for appropriate physical storage of information.
- Providing advice on the interpretation of policy.
- Undertaking a gap analysis against relevant external policies, standards and guidelines, and initiating remedial action where appropriate.

Information security – SCTY

- Balancing of cost against security risk for the business.
- Interpreting external requirements and standards in terms relevant to an organisation.
- Balancing technical, physical, personnel and procedural controls to address information risks in the most effective way.

SFIA Skills Gap Analysis

Skills Descriptions



Research – RSCH

- Defines research goals and generates original and worthwhile ideas in a specialised field within information security.
- Presents papers at conferences, writes journal papers of publication quality and/or presents reports of an equivalent technical standard to research clients
- Contributes to the development of the employing organisation's research policy and supervises the work of research functions.
- Development of new crypto algorithms, improved theories of information, secure development tools, such as formal methods tools
- Development of new ways for protecting information in specific environments (e.g. when being communicated).
- Investigation of vulnerabilities in current and potential technologies and techniques.

SFIA Skills Gap Analysis

Skills Descriptions



Innovation – INOV

- The capability to recognise and exploit business opportunities provided by IT, (for example, the Internet), to ensure more efficient and effective performance of organisations, to explore possibilities for new ways of conducting business and organisational processes, and to establish new businesses.
- Exploits opportunities for introducing more effective secure business and operational processes.

Business process improvement – BPRE

- The identification of new and alternative approaches to performing business activities. The analysis of business processes, including recognition of the potential for automation of the processes, assessment of the costs and potential benefits of the new approaches considered and, where appropriate, management of change, and assistance with implementation.
- Recognises potential strategic application of information security and initiates investigation and development of innovative methods of protecting information assets, to the benefit of the organisation and the interface between business and information security.

SFIA Skills Gap Analysis

Skills Descriptions



Business risk management – BURM

- Identification of assets that require protection.
- Identification of relevant threats to the assets.
- Assessing the level of threat posed by potential threat agents.
- Producing an information security risk assessment.
- Determining the business impact of a risk being realised.
- Developing information risk management strategies to reduce the risk.
- Gaining management commitment to the support of the information risk elements of business risk management.

SFIA Skills Gap Analysis

Skills Descriptions



Solution architecture – ARCH

- Interpreting relevant security policies and risk profiles into secure architectural solutions that mitigate the risks and conform to legislation.
- Presenting security architecture solutions as a view within broader IT architectures.
- Working with recognised security architectures.
- Delivering the security architecture that supports the risk management strategy using current security technologies and techniques.
- Designing and developing processes for maintaining the security of an asset or product through its full life cycle.

SFIA Skills Gap Analysis

Skills Descriptions



Continuity management – COPL

- Establishing the need for a Business Continuity Management (BCM) Process or Function.
- Providing cost-benefit analysis to justify investment in controls to mitigate risks.
- Determining and guiding the selection of possible business operating strategies for minimising disruption.
- Designing, developing, and implementing Business Continuity and Crisis Management Plans.
- Establishing and managing an Emergency Operations Centre to be used as a command centre during the emergency.
- Mounting pre-plan and co-ordinate plan exercises, and evaluating and documenting plan exercise results.
- Co-ordinating, evaluating, and exercising plans to communicate with internal stakeholders, external stakeholders and the media.

SFIA Skills Gap Analysis

Skills Descriptions



Methods and tools – METL

- Maintain awareness of the security advantages and vulnerabilities of common products and technologies.
- Selecting the most appropriate information interchange protocols that meet the security requirements.
- Selecting the appropriate security products, components and technologies to meet a security requirement.
- Designing robust and fault-tolerant security mechanisms and components appropriate to the perceived risks.

SFIA Skills Gap Analysis

Skills Descriptions



Systems development management – DLMG

- Implementing secure systems, products and components using an appropriate methodology.
- Defining and implementing secure development standards and practices including, where relevant, formal methods.
- Defining and implementing appropriate secure change and fault management processes.
- Analysing problem reports for signs of anomalous security issues, coordinating research into vulnerabilities and instigating corrective action where necessary.
- Specifying and/or implementing processes that maintain the required level of security of a component, product, or system through its lifecycle.

SFIA Skills Gap Analysis

Skills Descriptions



System design – DESN

- Translation of business analysis products (such as data structures, data flows and process models) from 'logical' to 'physical' models
- Minimising the risk to an asset or product through the 'standard' design and development processes.

Network design – NTDS

- Analysis of business goals and constraints, including business strategies, scope of network design, an understanding of current and new network applications, the organisational politics, decision makers and any budgetary and staff constraints
- Analysis of technical goals and constraints in respect of scalability, availability, performance, security, usability, adaptability and affordability
- Design of network topology and architectural models to include traffic backup paths, load balancing, redundancy and network security design topologies
- Selection of appropriate routing, switching and bridging protocols
- Determination of network security and network management strategies, to include asset and risk identification, security policy definition, network management architecture and processes

SFIA Skills Gap Analysis

Skills Descriptions



Testing – TEST

- Selecting and implementing appropriate test strategies to demonstrate security requirements are met.
- Verifying that a developed component, product or system meets its security criteria (requirements and/or policy, standards & procedures).
- Managing a system or component through a formal security assessment.

Systems installation/ decommissioning – HSIN

- Defining and implementing appropriate processes for transfer of a product/system to operation/sale/live use.
- Fully documenting the original system and mapping all transactions and functionality to the new environment
- Testing of the new system in an isolated environment including performance and capacity testing
- Ensuring data integrity in the new environment. This will include security settings, access controls and resilience
- Ensuring business continuity requirements are met through backups procedures and redundancy provision

SFIA Skills Gap Analysis

Skills Descriptions



Configuration management – CFMG

- The lifecycle planning, control and management of the documentation, software, hardware and firmware assets of an organisation, system and/or service(s), including information relating to those assets and their dependencies and relationships.
- The identification, classification and appropriate specification of all configuration items (CIs) and the interfaces to other processes and data through techniques such as federation.
- Required information relates to storage, access, service relationships, versions, problem reporting and change control of CIs.
- The application of status accounting and auditing, often in line with acknowledged external criteria such as ISO 9000 and ISO 20000, throughout all stages of the CI lifecycle, including (importantly) the early stages of system development.
- Use of sniffers that use the corporate network to identify hardware and software components and integrated Configuration, Change and Release Management tools

Change management – CHMG

- The management of change to the service infrastructure including service assets, configuration items and associated documentation, be it via request for change (RFC), emergency changes, incidents and problems, so providing effective control and mitigation of risk to the availability, performance, security and compliance of the business services impacted

SFIA Skills Gap Analysis

Skills Descriptions



Security administration – SCAD

- Securely configuring information and communications equipments in accordance with relevant security policies, standards and guidelines.
- Maintaining security records and documentation in accordance with Security Operating Procedures.
- Administering logical and physical user access rights.
- Monitoring processes for violations of relevant security policies (e.g. acceptable use, security, etc.)

Network control and operation – NTOP

- Securely configuring information and communications equipments in accordance with relevant security policies, standards and guidelines.
- Maintaining security records and documentation in accordance with Security Operating Procedures.
- Administering logical and physical user access rights.
- Monitoring processes for violations of relevant security policies (e.g. acceptable use, security, etc.)

SFIA Skills Gap Analysis

Skills Descriptions



Problem management – PBMG

- Engaging with the overall organisation Incident Management process to ensure that security incidents are handled appropriately.
- Defining and implementing processes and procedures for detecting breaches of security policy.
- Defining and implementing processes for carrying out investigations into breaches of security policy.
- Establishing and maintaining a Computer Security Emergency Response Team or similar to deal with breaches of security policy.
- Co-ordinating the response to a breach of security policy.
- Providing a full security response where third parties, managed service providers, etc. are involved.

SFIA Skills Gap Analysis

Skills Descriptions



Supplier relationship management – SURE

- Identifying and advising on the technical, physical, personnel and procedural risks associated with third party relationships.
- Assessing the level of confidence that third party security capabilities/service operate as defined.

Compliance review – CORE

- Carrying out security compliance audits in accordance with an appropriate methodology.
- The independent assessment of the conformity of any activity, process, deliverable, product or service with the criteria of specified standards, such as ISO 27001, local standards, best practice, or other documented requirements.

Technology audit – TAUD

- Verifying that information processes meet the security criteria (requirements or policy, standards and procedures).
- Defining and implementing processes to verify on-going conformance to security requirements.

SFIA Skills Gap Analysis

Skills Descriptions



Learning and development management - ETMG

- Identifying security awareness and training needs in line with security strategy, business needs and strategic direction.
- Gaining management commitment and resources to support awareness and training in information security.
- Identifying the education and delivery mechanisms needed to grow staff in information security awareness and competence.
- Managing the development or delivery of information security awareness and training programmes.

SFIA Skills Gap Analysis

Skills Descriptions (non SFIA)



Legal and Regulatory Environment

- Familiar with legal and regulatory requirements that could affect organisation security policies, and where to turn for specific detail as needed.
- Relating the legal and regulatory environment within which the business operates to the risk management and security strategy tasks.
- Ensuring security policies comply with all personal data protection laws and regulations relevant to the business.
- Ensuring security policies support compliance with corporate governance practices.
- Identifying where security can provide business advantage by addressing specific legal or regulatory needs.

SFIA Skills Gap Analysis

Skills Descriptions (non SFIA)



Secure Operations Management

- Establishing processes for maintaining the security of information throughout its existence.
- Establishes and maintains Security Operating Procedures in accordance with security policies, standards and procedures.
- Coordinating penetration testing on information processes against relevant policies.
- Assessing and responding to new technical, physical, personnel or procedural vulnerabilities.
- Managing implementation of information security programmes, and co-ordinating security activities across the organisation.

SFIA Skills Gap Analysis

Skills Descriptions (non SFIA)



Vulnerability Assessment

- Analysing internal problem reports for signs of anomalous security issues.
- Monitoring, collating and filtering external vulnerability reports for organisational relevance, ensuring that relevant vulnerabilities are rectified through formal change processes.
- Engaging with the Change Management process to ensure that vulnerabilities are mediated.
- Ensuring that disclosure processes are put in place to restrict the knowledge of new vulnerabilities until appropriate remediation or mitigation is available.
- Producing warning material in a manner that is both timely and intelligible to the target audience(s).

SFIA Skills Gap Analysis

Skills Descriptions (non SFIA)



Incident Investigation

- Working within the legal constraints imposed by the jurisdictions in which an organisation operates.
- Carrying out an investigation into a breach of information security using all relevant sources of information including access logs, systems logs, camera footage, etc.
- Assessing the need for Forensic activity, and coordinating the activities of specialist Forensic personnel within the overall response activities.
- Engaging with the organisational Problem Management processes to ensure that Forensic services are deployed appropriately.
- Providing a full security investigation capability where third parties, managed service providers, etc are involved.

SFIA Skills Gap Analysis

Skills Descriptions (non SFIA)

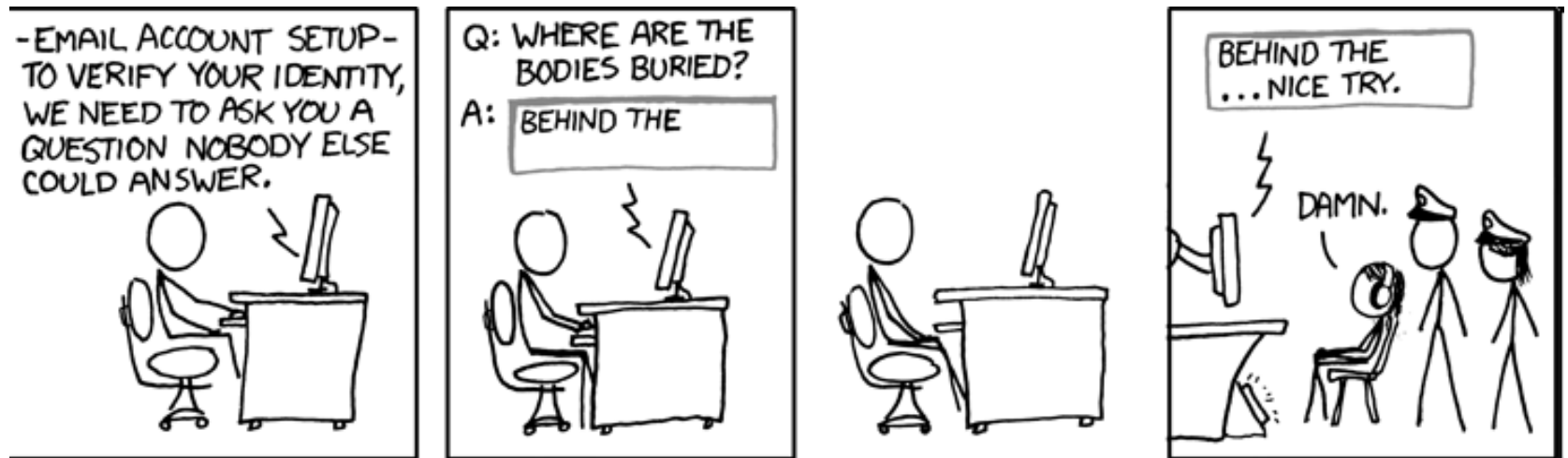


Forensics

- Seizing evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business and maintaining evidential weight.
- Deploying specialist equipment to monitor for attempted system compromise.
- Analysing system information (e.g. system logs, network traffic, hard disks, virtual memory, etc.) for evidence of breaches of security policy or law.
- Analysing software for malicious intent (malware).

End of Session 1

- Please fill in session 1 feedback sheets
- CPD receipts available – please ask
- Thank you!



<http://xkcd.com/565/>