Cyber Skilling for Secure Australia

Development of Australian Professional Standards in Cyber Security

Professor Jill Slay
ACS Security Task Force and Its role

• To provide recommendations on the establishment of a cyber security specialism certification. Thus creating Australian Professional Standards.
• Identify all job roles and occupations aligned with cyber security.
• Identify national and international best practice for accreditation and certification within cybersecurity
• Establish a baseline of knowledge and skills criteria which represents the minimum expectations of cyber security technician and professional
• Provide recommendations of professional assessment techniques for determining whether an individual has the cyber security knowledge and skills to fulfil the identified baseline requirements.
• Ensure recommendations are aligned with international best practice and comply with appropriate national and international cyber security professional and technical standards.
Overarching Context

1. The approach of contextualizing existing international frameworks identified as best practice by the Taskforce, for appropriate implementation in the domestic Australian market will be taken.

2. University Cyber course accreditation
   • ACS already accredits IT, CS, ICT degrees at undergrad and advanced level
   • Does it need a separate CBOK, or a Cyber Appendix added to the current CBOK
   • Do we need to develop guidance or model curricula

3. What should a Cyber skilling framework look like?

4. What does International Best Practice look like?

5. How can we contextualize it?
How to determine cyber skilling competencies?

• Look to US and Singapore
• Determine types of tasks carried out by Technicians and Managers of Cyber Security
• Map out competencies assessed by common certifications
• Take on board IRAP evaluator criteria

1. CISSP or CISM plus
2. CISA or CRISC or GSNA or ISO 27001 Lead Auditor or PCI qSA

• Department of Defense Directive 8570 provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC certifications are among those required for Technical, Management, CND, and IASAE classifications.

• Who is affected by 8570?

• Any full- or part-time military service member, contractor, or local nationals with privileged access to a DoD information system performing information assurance (security) functions – regardless of job or occupational series. The manual, 8570.01M, specifies that the Department of Defense requires approximately 110,000 identified Information Assurance professionals to be certified within a five year time period. The Defense Information Assurance Program office has divided its Information Assurance workforce into six defined
National Initiative for Cybersecurity Education (NICE)

• The NICE Cybersecurity Workforce Framework (NCWF) is a national resource that categorizes and describes cybersecurity work. It provides employers, employees, educators, students, and training providers with a common language to define cybersecurity work as well as a common set of tasks and skills required to perform cybersecurity work. It:
  • Standardize how positions are managed and described by populating position descriptions with Tasks and KSAs from the Workforce Framework.
  • Incorporate Tasks and KSAs into job advertisements to attract candidates who can perform needed job functions. Develop career paths that outline the Tasks and KSAs staff need to perform to progress to the next level.
<table>
<thead>
<tr>
<th>Role Level</th>
<th>IAT Level I</th>
<th>IAT Level II</th>
<th>IAT Level III</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM Level I</td>
<td>CompTIA Security+</td>
<td>CompTIA Security+</td>
<td>CASP</td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>CAP</td>
<td>GSEC</td>
<td>CISA</td>
</tr>
<tr>
<td>IAM Level II</td>
<td>IAM Level II</td>
<td>IAM Level III</td>
<td></td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>CASP</td>
<td>CASP</td>
<td>GCIH (or Associate)</td>
</tr>
<tr>
<td>IAM Level III</td>
<td>IASAE III</td>
<td>IASAE III</td>
<td></td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>CASP</td>
<td>CISSP (or Associate)</td>
<td>CISSP - ISSEP</td>
</tr>
<tr>
<td>IAM Level III</td>
<td>IASAE III</td>
<td>IASAE III</td>
<td></td>
</tr>
<tr>
<td>CompTIA Security+</td>
<td>CASP</td>
<td>CISSP (or Associate)</td>
<td>CISSP - ISSAP</td>
</tr>
</tbody>
</table>

How does one become MACS CT or CP anyway?

- SFIA, the Skills Framework for the Information Age, describes skills required by professionals in roles involving information and communications technology.

- SFIA is a practical resource for people who manage or work in information systems-related roles of any type. It provides a common reference model in a two-dimensional framework consisting of skills on one axis and seven levels of responsibility on the other. It describes professional skills at various levels of competence. It also describes generic levels of responsibility, in terms of Autonomy, Influence, Complexity and Business Skills.

- We have mapped common certifications using SFIA to develop a potential cyber skilling framework (some available)
### Australian Cyber Professional Standards Framework

<table>
<thead>
<tr>
<th>MACS CT Cyber</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCP</td>
<td></td>
</tr>
<tr>
<td>CISA</td>
<td></td>
</tr>
<tr>
<td>MACS CP Cyber</td>
<td></td>
</tr>
<tr>
<td>CISSP</td>
<td></td>
</tr>
<tr>
<td>CSSLP</td>
<td></td>
</tr>
<tr>
<td>CISM</td>
<td></td>
</tr>
<tr>
<td>GIAC</td>
<td></td>
</tr>
</tbody>
</table>
Outcomes

1. The Taskforce considers that the ACS Core Body of Knowledge would benefit from greater prescription of cyber security within the ACS knowledge areas, but that a future development would include an appendix in the ACS Core Body of Knowledge on Cyber Security.

2. An environmental scan on global certifications held in high esteem has been undertaken via the taskforce and broader industry consultations. It is the Taskforce’s view that those certifications with the greatest global acceptance provide an opportunity to expedite the introduction of an ACS Cyber Specialism.
Outcomes

3. These have been identified for Certified Technologist (Cyber Security) as:
   • Systems Security Certified Practitioner from ISC²
   • Certified Information Systems Auditor from ISACA

4. These have been identified for Certified Professional (Cyber Security) as:
   • Certified Information Systems Security Professional from ISC²
   • Certified Secure Software Lifecycle Professional from ISC²
   • Certified Information Security Manager from ISACA
Outcomes

• A mapping exercise of the nominated ISC² and ISACA certifications have been mapped to SFIA and levels 3 and 5 as required through the ACS certifications.

• These are in many cases higher than the nominated SFIA levels. Reflecting the multi-disciplinary nature of Cyber Security, there is little overlap across these certifications. As a result, the taskforce is of the view that flexibility needs to be built into the specialism process.

• We have recommended three SFIA skills from a limited SFIA list of ten for Certified Technologist and four skills from ten for Certified Professional.
Certified Professional - Cyber Security

- Cyber security specialism assessment requirements are equivalent to existing ACS Certified Professional assessment criteria and pathways with the addition of demonstrating in-depth competence in 4 SFIA skills at SFIA level 5. SFIA skills must be from the following skills:
  - IT Governance
  - Information Management
  - Information Security
  - Information Assurance
  - Business Risk Management
  - Penetration Testing
  - Security Administration
  - Programming/Software Development
  - Systems Software
  - Testing
  - Asset Management
Certified Technologist - Cyber Security

Cyber security specialism assessment requirements are equivalent to existing ACS Certified Technologist assessment criteria and pathways with the addition of demonstrating in-depth competence in 3 SFIA skills at SFIA level 3. SFIA skills must be from the following skills:

- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Systems Development Management
- Asset Management
- Change Management
- Security Administration
- Incident Management
- Conformance Review
Further work

• 1. At this stage, greater research is required to be undertaken on certifications provided by SANS and CREST but similar mappings will also be produced.

• 2. There is ongoing discussion with Defence contractors, vendors and the Big 4 with a view to mapping the learning outcomes of their training courses to those SFIA outcomes recommended above.

• 3. ACS will be developing a repository of open source resources for self-education and running, where necessary, specialized workshops to allow for the development of specific SFIA skills.

• 4. ACS will offer micro-credentialing to test for these SFIA skills.

• 5. ACS will work with government and industry to advise and support the implementation of these Professional Standards.
SECURE CANBERRA 2017

Thank You for Attending.