Professionalism and Frameworks

Moira De Roche

Professionalism and frameworks

Moira de Roche[1]

[1] Chair IFIP IP3, South Africa
mderoche@ipthree.org

Abstract. In two sessions the International Professional Practice Partnership (IP3) of IFIP addressed a number of frameworks that provide definitions of ICT competences and typical profiles. These frameworks contribute to establishing an ICT profession that consists of competent and responsible professionals who can demonstrate the necessary skills and competences.

Keywords: professionalism, competences, skills frameworks, certification, e-CF, SFIA, ACS Cyber Security Framework

1 Professionalism and IP3

1.1 The importance of ICT professionalism

Information and communication technologies (ICT) impact almost every facet of personal and business life. Such technologies are key drivers of innovation and of both economic and social progress, making enormous contributions to prosperity and to the creation of a more open world, enabling pluralism, freedom of expression, and allowing people and organisations to share their culture, interests and undertakings worldwide.

Such powerful technologies, and their application, must be driven by competent and reliable professionals who can demonstrate the necessary competences (including knowledge), integrity, responsibility and accountability, and public obligation.

Recognising that ICT is now a global industry, the ICT profession must also be global. It must have clear international standards that accommodate cultural differences in the regulation of professions, which is enhanced by strengthened competence requirements.

1.2 International Professional Practice Partnership – IP3

Through IP3, the International Professional Practice Partnership [1], IFIP established a global partnership that promotes professionalism. By doing so it strengthens the ICT profession and contributes to the development of strong international economies by creating an infrastructure that will:

- encourage and support the development of both ICT practitioners and employer organizations;

- give recognition to those who meet and maintain the required standards for knowledge, experience, competence and integrity; and
- define international standards of professionalism in ICT.

IP3 defines and maintains global standards for ICT and recognises and certifies professionalism. Frameworks underpin the accreditation process, and their use is essential to the maintenance of professional standards at any IT Society or body that is certified.

To carry out its' mission, IP3 works closely with partners who share a commitment to creating a sound global ICT profession. IP3 encourages employing organisations, governments, commercial enterprises and IFIP member societies to join in this partnership through their membership.

IP3 in 2016 launched iDOCED, the IFIP Duty of Care for Everything Digital campaign which promotes trust in ICT, and the duty of care that everyone should have in the digital world. Duty of care goes hand in hand with professionalism, as trustworthiness is an essential element.

2 Professionalism and frameworks

A number of frameworks has been developed that provide definitions of ICT competences and typical profiles. These initiatives are characterised by an open and inclusive approach, and accredit valuable qualification elements, either national, regional or global. In two workshops at the IFIP World Computer Congress (WCC) 2018 an overview was provided of some frameworks in use, as well as the practical implementations of the frameworks.

2.1 e-CF overview

[2]: "The European e-Competence Framework (e-CF) provides a reference of 40 competences as applied at the Information and Communication Technology (ICT) workplace, using a common language for competences, skills, knowledge and proficiency levels that can be understood across Europe. The European e-Competence Framework provides a common language to describe the competences including skills and knowledge requirements of ICT professionals, professions and organisations at five proficiency levels, and is designed to meet the needs of individuals, businesses and other organisations in public and private sectors."

Mary Cleary [3], Deputy Chief Executive of the Irish Computer Society and former chair of the e-CF workshop, explained the state of the ICT profession in Europe, focussing on maturing the profession, with a short-term aim of a fully professionalised sector. The profession must be committed to a relevant body of knowledge, with standardised competences, a commitment to continuous professional development and a clear code of ethics. Progress has been made in achieving these goals.

e-CF is now a European standard (EN 16234-1, April 2016), and work is underway to establish a standardised Body of Knowledge (BoK), education and certification, and a code of professional ethics. There is a standardised set of 30 ICT professional role

profiles, which are fully incorporated into the EC ICT Rolling Plan for ICT Standardisation.

2.2 SFIA overview

[4]: "The Skills Framework for the Information Age (SFIA) describes skills and competencies required by professionals in roles involved in information and communication technologies, digital transformation and software engineering. It provides a framework consisting of professional skills on one axis and seven levels of responsibility on the other. It describes the professional skills at various levels of competence and it describes the levels of responsibility, in terms of generic attributes of autonomy, influence, complexity, knowledge and business skills."

Ian Seward [5], General Manager of the SFIA Foundation, (Skills Framework for the Information Age), explained the history of SFIA and how the framework is used in the Skills and Competency Management Cycle. A useful description of the structure of the framework was included, which comprises: six categories; 17 subcategories; 102 skills names with associated skills descriptions; and 388 skills level descriptors in the professional skills component. There are seven levels of responsibility, five generic attributes, and 35 attribute level descriptors in the behaviours and knowledge component.

SFIA is developed by industry and business for use by industry and business in the real world. At its heart is experience. A practitioner has a skill or competence because of the experience of practicing the skill in a real-world situation.

2.3 e-CF in an academic environment

Marek Bolanowski [6], representing the Faculty of Electrical and Computer Engineering Rzeszow University of Technology and the Polish Information Processing Society IT Competence Council, considered the e-CF in an Academic setting.

An overview was provided of the typical University of Technology graduate, and considerations of the employers' needs. The university explored "Who is the modern IT Specialist?". They needed to consider the legal issues ruling university education in Poland. The e-CF was examined considering the point of views of all stakeholders: the student, the university and the employer. Questions to be answered were: What are the possibilities of implementing the e-CF in the university environment in relation to the needs of the job market; How can the students use the e-CF to build and develop their careers; and What are the difficulties associated with the implementation of the e-CF in the university environment?

The technical competences and business/soft competences, required by the job market, were explored. The issue is complicated by the lack of a definition for an IT specialist. Common definitions and terminology are required, and it is hoped that the e-CF will provide at least part of the solution.

From a students' perspective e-CF helps in organizing the requirements of the job market, it creates a common terminology dictionary, it helps to determine competences

and it can help in career planning. For teachers it allows to periodically verify the content of the educational module and to focus not only on technical skills. It may also help to internationalize the education process.

For employers it can improve communication between companies, students and universities, it can help to organize the employment structure. It might also allow a company to prepare internship programs and to actively participate in the educational process. An additional benefit may be a reduction in the costs of the recruitment process.

2.4 ACS Cyber-Security Framework overview

This framework, developed by the Australian Computer Society (ACS) as the basis for an extension of the ACS professional certifications scheme and adopted by IP3, was presented by Anthony Wong [7], IFIP IP3 Director, and Immediate Past President of ACS.

The following points were covered: Cybersecurity, Privacy and Technological challenges – what are Organisations and Governments seeking; How can we align Business and Organisational priorities with those of security professionals; The Professionalisation of Cybersecurity and Privacy practitioners; Challenges & key issues – is EU GDPR transforming the landscape; What are the repercussions of doing nothing?

The Duty of Care that is requisite for governments was examined, and the rationale illustrated. This includes: Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means; The implications for government perspectives on cyber law, cyber policy both local and international, how issues and attacks are communicated, offensive cyber security, the cyber economy, cyber intelligence and forensics. Furthermore, there is a global shortage of Cyber-Security professionals, which runs into millions.

Cyber Security, Privacy and Technological challenges include: Definitions of 'Cyber security' still unclear; There is a strong demand for Cyber security practitioners but understanding of 'professionalism' not explicit; Pseudo Professional Standards proliferate; Cyber security and privacy issues are now mainstream in the boardroom. These challenges together with urging from government, resulted in the development of the Cyber Security frameworks. These are "specialisms" which are in addition to the standard IP3 Technologist (IP3T) and IP3 Professional (IP3P) certifications. In response to this, the frameworks were developed in Australia by the ACS. They are designed to provide a level of Assurance and Trust, and to address the growing shortage of cyber security expertise. The frameworks and related certifications will raise professional standards for cyber security specialists and highlight the Duty of Care for cyber security professionals.

3 Frameworks implementation

The second workshop included sessions which explored the practical implementation of the frameworks. Liesbeth Ruoff [8], KNVI (Netherlands) explored the usage of the new e-CF profiles and role documents in different settings. She provided an overview

of the Professional ICT workforce in the EU, as at 2016. The purpose of the e-CF is to provide a shared language which can be used to address the Skills gap. She provided information about the building blocks of the Framework and went on to explore these in detail. She demonstrated the mapping of the e-CF to SFIA. To tie it all together, she shared several use cases:

- Job profiles for information security 2.0, PvIBQIS
- Supplier Management: KPN consulting IT-CMF –e-CF
- Data Science, EU-Edison project, University of Amsterdam
- E-CF© NEXT, profile tool / assessment of EXIN
- Rake-Shape, blockchain f.e. UWV, LRWA

Tony Parry, IITPSA, explained how SFA is used for membership grading. He explained that IITPSA uses SFIA as a standardised approach, that is consistent, fair and aligns to IP3 and the South African Qualifications Authority requirements. It is used for: the Professional Designation (PMIITPSA) which is IP3 accredited and SAQA registered; peer reviews; Critical Skills Assessments (foreign worker work permit requirement). The philosophy is ”Assessing each case on its merits”.

Bogusław Dębski [9], PTI-IT Competence Council, Ministry of Digital Affairs examined how the e-CF can be used in the education system for ICT Professionals. The e-CF should be considered in Computer Science Education for high school and vocational school students, as the foundation of the creation of the future ICT Professionals, as well as their development. Having discussed the skills requirements with all stakeholders, they were very pleased to discover the e-CF. Using the e-CF and its 40 competences helped to speed up the work of developing curricula. They took the competence framework, went through its 40 competences and on this base we actually created a common language. The power of the e-CF is that it relates to real life and real labor market.

Anthony Wong [10] provided insights of the Cyber Security Framework in Action. He examined the situation around the world, especially the effects of GDPR. The biggest threat is the sever shortage of skills in the Cyber Security space globally, citing examples showing the estimates of 1.8 million people. The EU is leading the world in legislating to protect and provide access to personal data with its EU General Data Protection Regulation (GDPR), which replaced the 1995 Data Protection Directive in May 25, 2018.The implications are far-reaching, affecting with an establishment in the EU or that offer goods and services to business or citizens of the EU, or that monitor the behaviour of individuals in the EU may need to comply. There are significant penalties for non-compliance with fines up to €2million, or 4% of global turnover. GDPR specifies job designations related to compliance officers, and the requisite skills for those in these roles. The ACS developed the Cyber Security Framework:

- Designed to provide a level of Assurance, Trust and to address the growing shortage of cyber security expertise.
- Launched by Australian Minister Assisting the Prime Minister for Cyber Security, the Hon Dan Tehan in Canberra in Sept 2017.
- Adopted by IFIP IP3 as a new specialism certification for member societies around the world.

- ACS support for the implementation of the Australian International Cyber Engagement Strategy announced by the Hon Julie Bishop MP, Minister for Foreign Affairs in October 2017.
- Raise professional standards for cyber security specialists.
- Highlight the Duty of Care for cyber security professionals.

Reflecting the multi-disciplinary nature of Cyber Security, flexibility is built into the certification for Technologists (SFIA Level 3) and Professionals (SFIA Level 5). Professionals who have achieved the Cyber Security Professional certification come from the aviation, banking and finance, audit and risk, consulting, and healthcare industries.

Adrian Schofield, Chair IP3 Standards and Accreditation Committee, explained how frameworks are used to ensure the trust aspect of accreditation (video presentation). Framework ensure that levels are benchmarked – irrespective of the framework used the skills levels and competencies are at a similar level.

4 Follow up

At the end of the workshop, the speakers and audience considered how it can be ensured that all frameworks are mapped to each other, and the work that needs to be done to realise this goal. We accept that more than one framework is being utilised but encourage new entrants to use something that already exists, rather than create a new framework. Having too many frameworks causes confusion and it duplicates work. Mapping and customisation are better options.

An IP3 task force has been created to develop a project plan to carry out this work in collaboration with all key players. It is hoped that this project will be funded. IP3 call for all interested parties to join us in this work to ensure that the process is inclusive and representative. Contact mderoche@ipthree.org for more.

References

1. IFIP IP3, https://www.ipthree.org/
2. http://www.ecompetences.eu/, accessed 18 January 2019
3. Mary Cleary, https://www.ipthree.org/wp-content/uploads/Mary-Cleary-e-CF-and-TC-428.pdf
4. https://www.sfia-online.org/en, accessed 18 January 2019
5. Ian Seward, https://www.ipthree.org/wp-content/uploads/SFIA-Overview-Ian-Seward.pdf
6. Marek Bolanowski, https://www.ipthree.org/wp-content/uploads/MB-Frameworks-in-an-Academic-setting.pdf
7. Anthony Wong, https://www.ipthree.org/wp-content/uploads/Cyber-security-Framework-overview-Anthony-Wong.pdf
8. Liesbeth Ruoff, https://www.ipthree.org/wp-content/uploads/eCF-Implementation-Liesbeth-Ruoff.pdf
9. Bogusław Dębski, https://www.ipthree.org/wp-content/uploads/e-CF-Education-System-B.Debski.pdf
10. Anthony Wong, https://www.ipthree.org/wp-content/uploads/Cyber-Security-specialism-framework-in-action-Anthony-Wong.pdf