

# Top 10 Abilities - Expediting Cybersecurity Capability

Authors: [Nina Olesen](#), Senior Policy Manager at ECSO, [Almerindo Graziano](#), CEO Silensec | CYBER RANGES, [Marcello Hinxman-Allegri](#), Head of Marketing [Silensec | CYBER RANGES](#)

## At a glance

- 8 minute read 🕒
- Top 10 Abilities in a nutshell
- Background
- The Top10A rationale
- Conclusions




## Top 10 Abilities in a nutshell

“Top 10 Abilities” is a new ECSO-sponsored project that aims to identify, agree and introduce a more manageable subset of core abilities for each job role in the cybersecurity domain. Such abilities will be agreed upon via the industry community and expert feedback, with the goal of overarching the different competency frameworks initiatives around the world to date.

While competency frameworks continue to provide the fine-grained assessment of specific competencies, Top 10 Abilities (Top10A) shall focus on the top 10 measurable abilities that give employers a reasonable assurance of the suitability of a person for a specific job role.

“Top 10 Abilities” was initially conceived back in 2020 and brought to ECSO and is now promoted as a cross-SWG initiative under the ECSO WG5 leadership.

This article aims to provide in particular CISOs and their HR teams with an effective outcome-driven route to look past the cybersecurity skills shortage and to plan more confidently for the sourcing and development of the cybersecurity capability, including human talent required to support the digital transformation of their organisations.

A large group of graduates in black caps and gowns, seen from behind, filling the background of the text box.

**“The cybersecurity education system currently suffers from the inability to attract more students to study cybersecurity and to produce graduates with the right cybersecurity knowledge and skills.”**

## Background

The cybersecurity skills shortage (CSSS) refers to the lack of qualified cybersecurity professionals in the labour market and represents an issue for both economic development and national security, especially in the rapid digitisation of the global economy.

CSSS poses threats with a high impact on the data, information technology systems and networks that form the dorsal spine of modern societies. This shortage can be further analysed into two concurrent issues: a quantitative one and a qualitative one:


- the CSSS quantitative issue is related to the insufficient supply of cybersecurity professionals to meet the requirements of the job market;
- the CSSS qualitative one is related to the inadequacy of professional skills to meet the market's needs;

- furthermore, “most job descriptions demand specific skill sets that may not be required to perform a role, resulting in the perception of a skills shortage.” – Gartner (Feb-2021).


The cybersecurity education system currently suffers from the inability to attract more students to study cybersecurity and to produce graduates with the right cybersecurity knowledge and skills.

No doubt, many of the current issues in cybersecurity education could be mitigated by redesigning educational and training pathways that define the knowledge and skills that students should possess upon graduation and after entering the labour market.

ECSO SWG 5.2 is already addressing this matter with a Minimum Reference Curriculum, soon out for wider consultation.



“CSSS poses threats with a high impact on the data, information technology systems and networks that form the dorsal spine of modern societies.”



“The ultimate impact of degree certification is to reduce the CSSS through the promotion of cybersecurity education, research and awareness.”

ENISA reports that some countries have attempted to rethink cybersecurity degrees using certifications. These certification schemes have been established for various purposes. The main rationale includes: having more graduates with skills readily deployable by the industry, helping employers understand skills and knowledge that students have developed in their academic careers, and assisting people to choose their degree options.

The ultimate impact of degree certification is to reduce the CSSS through the promotion of cybersecurity education, research and awareness. Currently, over 387 cybersecurity degrees have been certified by the national authorities of those countries. Processes and criteria may differ, but certifications share some commonalities:

- a specific focus and enough credits dedicated specifically to cybersecurity courses and activities;

- a structured curriculum, possibly with a practical/training component or specific types of examinations and activities such as cybersecurity competitions;
- a high-quality teaching faculty, which might include lecturers from industry;
- a broader multi-/inter-disciplinary focus;
- external outreach activities and collaborations with the rest of the national cybersecurity ecosystem;
- information on degrees' educational and employment outcomes.

While ideal in theory, such an ecosystemic approach is however very slow and, one may say, comes with the risk of ending up over-engineered thus unusable also because of the number and variety of mindsets, actors, and interests involved.



## The Top10A rationale

The growing cybersecurity skills shortage requires scalable and flexible solutions to quickly allow organisations to train and upskill their workforce. According to Gartner, 68% of digital organisations have at least one cybersecurity expert on staff. However, they remain incapable of managing digital risk to drive value creation.


On one hand, technology advances in recent years, especially in the area of cloud technology, have allowed the development of flexible learning and assessment solutions based on experiential training and education, where individuals can practice or acquire new skills by interacting with live simulation environments.

On the other hand, a number of national, international and sector-specific initiatives have been working on the development of skills frameworks for the mapping of different job roles to specific

skills and competencies, with a notable and established example being provided by the NIST NICE Workforce Framework for Cybersecurity in the USA. NICE is also the mostly widely used reference framework around the world, while ENISA is currently working on a European cybersecurity skills framework, expected to come out next year.

Experiential training and assessment solutions use competency frameworks by mapping each training and assessment activity to a specific job competency and by building over time a user's competency profile in relation to specific job roles or profiles in order to understand to what level a particular user fulfils all the skills requirements for a specific job role. Such an approach is very formal and exhaustive and builds on the long-standing approach which educational institutions have been using for decades. This approach helps to answer the following question:

“Does the person possess the competencies required for a specific job?”



**“The growing cybersecurity skills shortage requires scalable and flexible solutions to quickly allow organisations to train and upskill their workforce.”**

Let's take the job a professional penetration tester/ethical hacker since it is one professional figure with lots of established international competence-based certifications. Here, the role of such competency frameworks as NIST NICE is that of providing the common taxonomy and structure for performing a Job Task Analysis so that, ideally, new job roles can be defined using the common taxonomy.

However, with a plethora of competency frameworks being developed worldwide, there is no such a thing as a common taxonomy since everyone is trying to define their own and therefore an established profession such as that of the penetration tester can be described in many different ways in terms of the competencies required for the job. Hence, many professional certifications exist, all claiming to certify that an individual possesses the competencies required for the job.

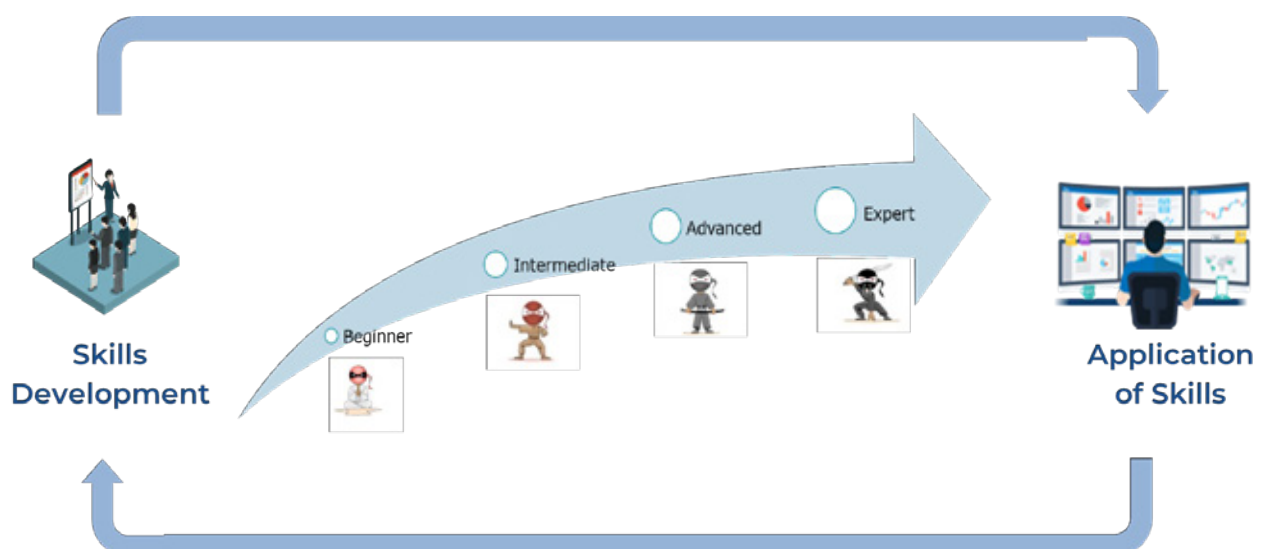
Such fragmentation brings confusion to both professionals and employers. The former look for the most established security certification that is accepted by

employers to invest in in order to secure employment and/or to advance their careers. The latter seek to understand which certification better tells the "truth", i.e., which one is reliable to the extent that the person holding that certification can truly do the job which he/she will be hired to perform. Specifically, the question employers and organisations generally look for the answer to is the following:

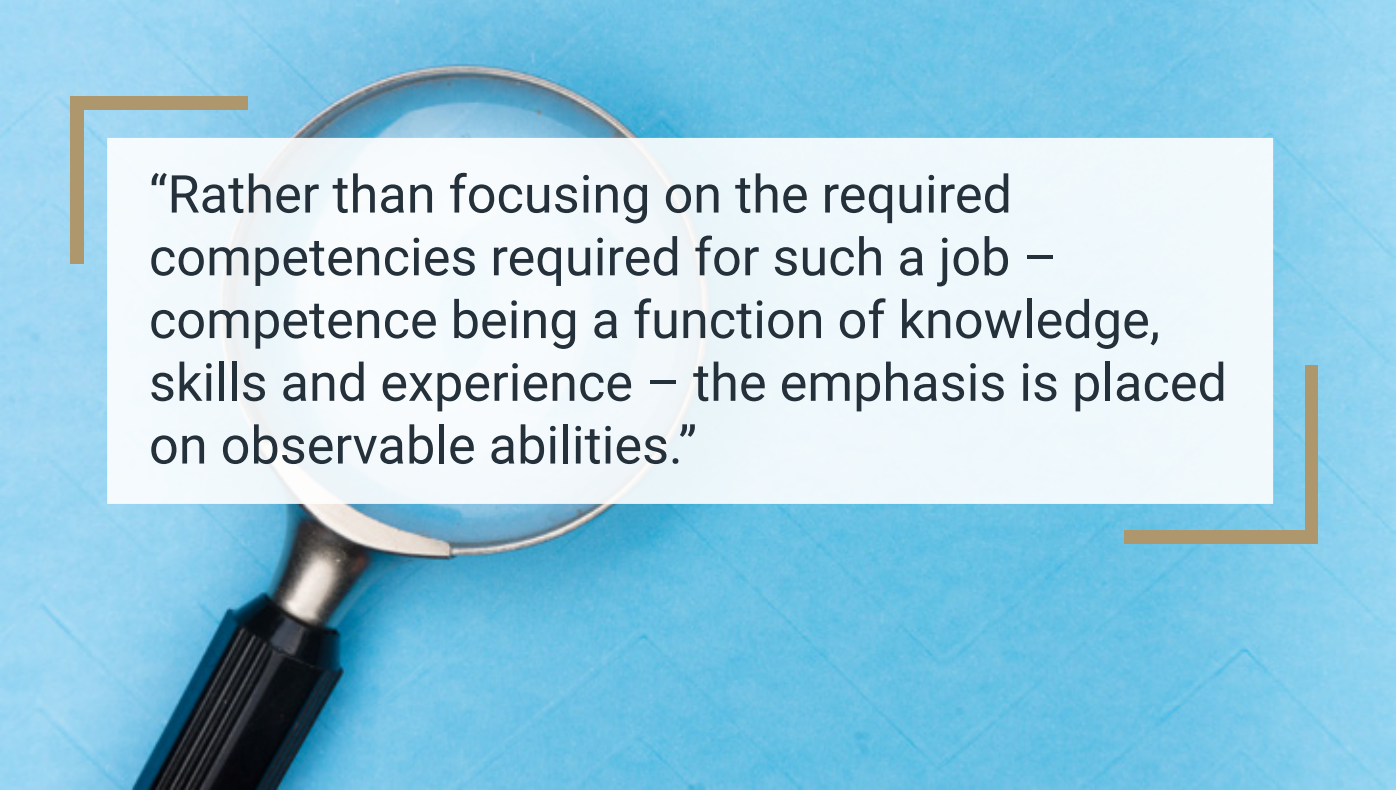
"How can I know if the person can do a specific job?"

One can argue that having the competencies for the job and holding an established certification that proves it should give a company enough assurance that a specific job can be fulfilled. However, as any employer or manager who has looked at potential candidates with relevant professional certifications can testify, this is not always the case.

ECSO's Top 10 Abilities aims to provide immediate answers to employers who try to understand if a specific person can do a specific job.



The continuum between Development and Application of Skills in experiential learning



**“Rather than focusing on the required competencies required for such a job – competence being a function of knowledge, skills and experience – the emphasis is placed on observable abilities.”**

Rather than focusing on the required competencies required for such a job – competence being a function of knowledge, skills and experience – the emphasis is placed on observable abilities (i.e., the measurable core of experience). Such abilities can be assessed through highly realistic situational scenarios which simulate typical job-specific tasks.

The Top 10 Abilities Initiative has the following objectives:

1. Define a list of Top 10 abilities for different security job roles. CISOs can benefit from understanding how others are structuring their teams and at what capacity.
2. Define a list of recommended experiential scenarios which can be used to assess those abilities.

Top 10 Abilities does not aim to replace or undermine the approach of applying competency frameworks, some of which also include the concept of abilities as

observable skills in the context of a job role. Top 10 Abilities does however introduce a more manageable subset of core abilities for each job role, observable and measurable, to agree upon on the basis of industry community and expert feedback, overarching the different competency frameworks initiatives around the world.

It is important to realise though that benchmarking and peer comparison should be taken as reference points from which CISOs can derive more specific talent development tailored to their organisation’s business goals and circumstances, by selecting external candidates or through internal training.

While competency frameworks continue to provide the fine-grained assessment of specific competencies, Top 10 Abilities focuses on the top 10 measurable abilities that will give employers a reasonable assurance of the suitability of a person for a specific job role.

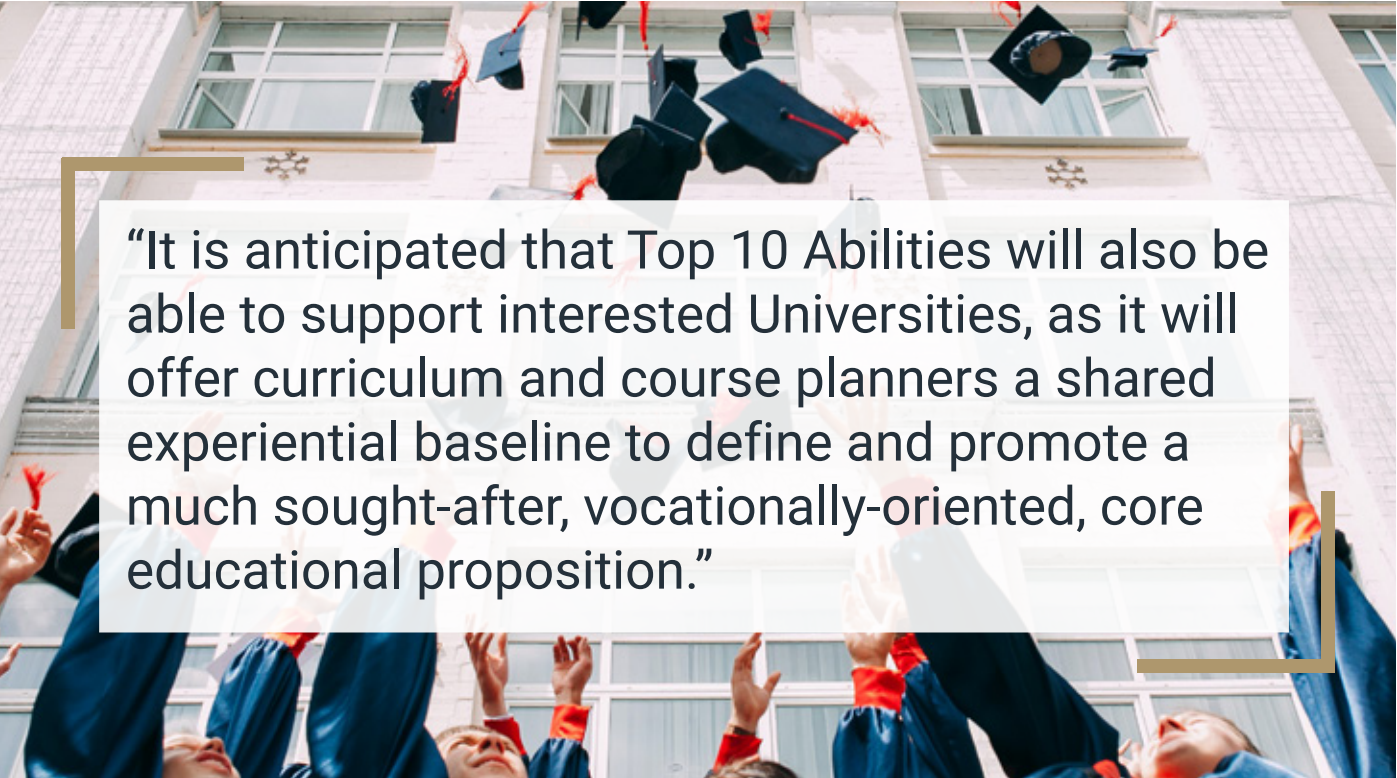


The following activities are targeted in the Top 10 Abilities initiative:

- engagement with ECSO members and the wider community of security professionals, employers, HR professionals etc. to identify top 10 abilities for each job role, 10 being a practitioner-defined number for now. A wide consultation is being developed in this respect.
- engagement with ECSO members, including cyber range and training providers, for the definition and creation of real-life experiential scenarios and resulting exercises that can be used to assess the proposed top 10 abilities. However, there is no click-and-run type of cyber exercise, and there is no click-and-run type of assessment that will just observe the actions and responses of the people participating in the cyber exercise and return the organisation's scorecard. Automation means lower costs, greater speed of execution

and increased realism. Most tools and technologies used in cyber exercises today lack automation and are heavily dependent on security professionals and facilitators to run the show on stage and at the back. Setting up and maintaining simulation environments is still expensive. With some notable exceptions.

- it is anticipated that Top 10 Abilities will also be able to support interested Universities, as it will offer curriculum and course planners a shared experiential baseline to define and promote a much sought-after, vocationally-oriented, core educational proposition. This to be synergic with the work being carried out within ECSO SWG5.2 on the Minimum Reference Curriculum which will soon be released for wider consultation. This would also foster the ambitions for a "Cybersecurity Education Made in Europe" programme.



**"It is anticipated that Top 10 Abilities will also be able to support interested Universities, as it will offer curriculum and course planners a shared experiential baseline to define and promote a much sought-after, vocationally-oriented, core educational proposition."**

## Conclusions

The design of comprehensive cybersecurity workforce development strategies that go beyond policies, targeting only the education and training system, needs to factor in and involve employers in developing a regional cybersecurity workforce.

Some ingenuity is required to create and catalyse a virtuous cycle that guarantees a good match between the supply of workers and the requirements of jobs, taking into account the primary role that employers should have in sustaining the cybersecurity workforce.

ECSO's Top 10 Abilities project aims to offer expert contributions towards such ingenuity. For more information and to get involved in Top 10 Abilities, please refer to: <https://top10abilities.org/>

## About the Authors

**Nina Olesen**  
Senior Policy Manager, ECSO

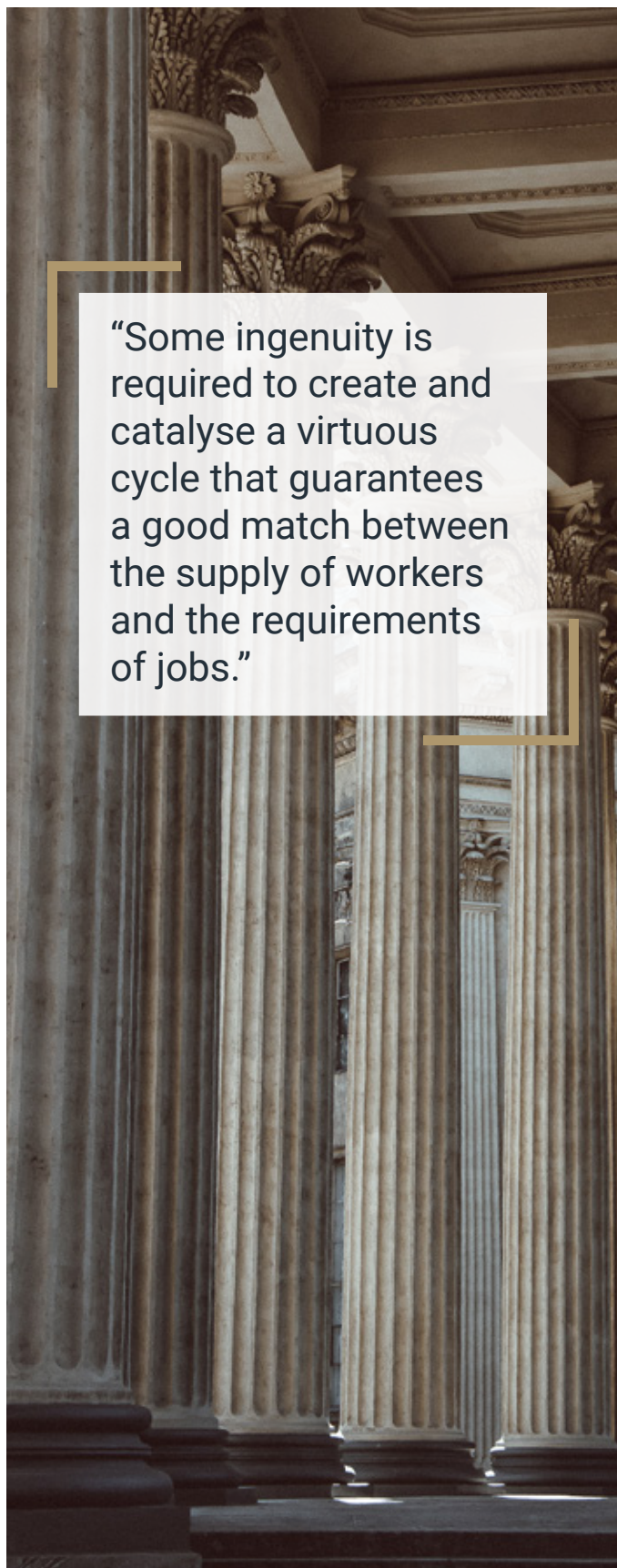
Nina is responsible for managing the European Cyber Security Organisation's WG3 on 'Cyber Resilience of Economy, Infrastructure, and Services' and WG5 on 'Education, Training, Cyber Ranges, and Human Aspects'. Nina also oversees ECSO's Women4Cyber and Youth4Cyber initiatives.

**Dr. Almerindo Graziano**  
CEO Silensec | CYBER RANGES

Al co-chairs the European Cyber Security Organisation's ECSO WG5 on cyber ranges, cyber exercises and training.

**Marcello Hinxman-Allegri, CMktr SCIP**  
Head of Marketing Silensec | CYBER RANGES

Marcello co-chairs the European Cyber Security Organization's SWG 5.2 on education and training.



**"Some ingenuity is required to create and catalyse a virtuous cycle that guarantees a good match between the supply of workers and the requirements of jobs."**