Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

Training module title:

The European Digital Competence Framework: DigComp 2.1

By IHF asbl

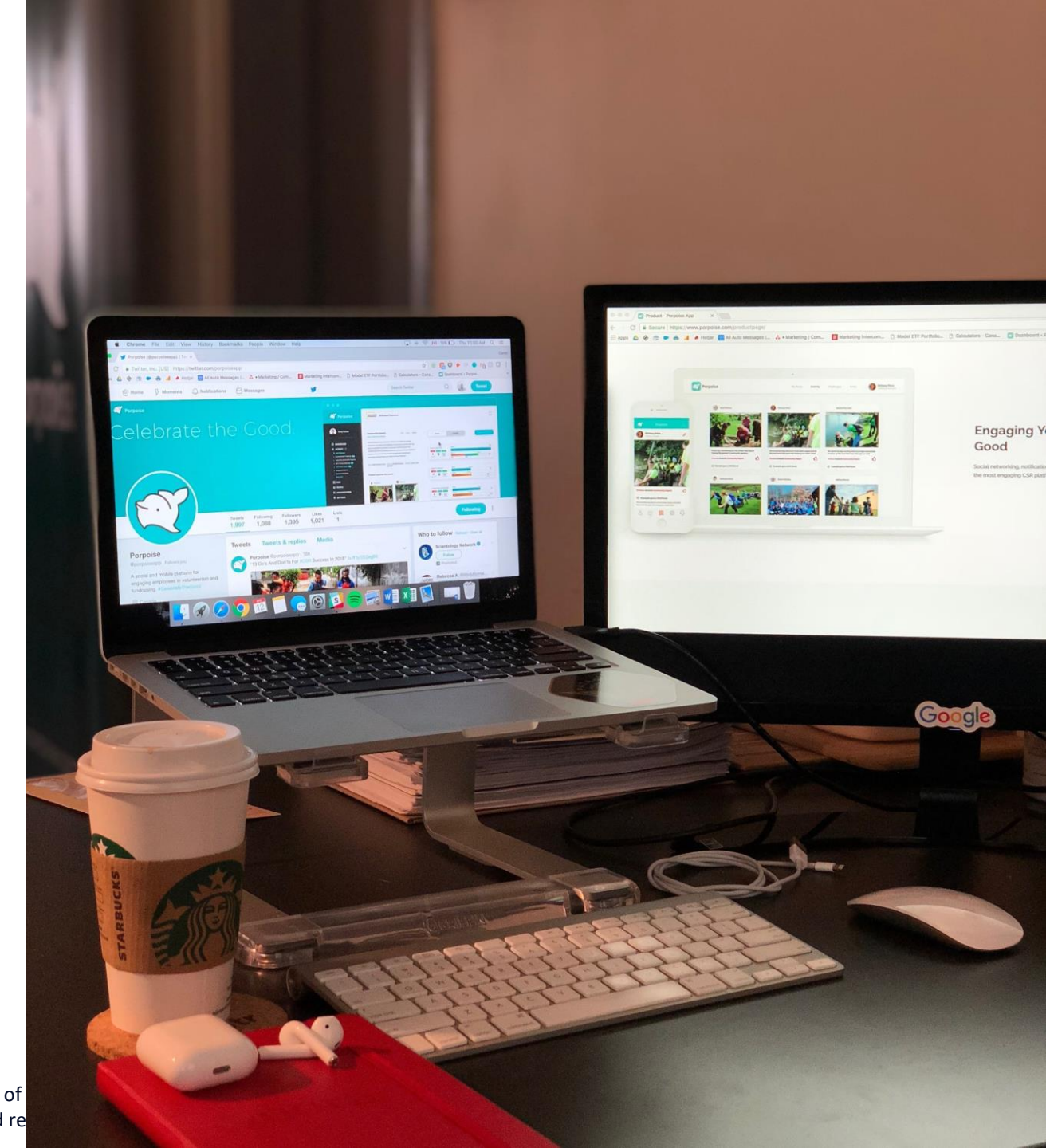
Erasmus+

Objectives and Goals:

In the context of this module, you will have the opportunity to familiarize with the DigComp Framework – the official EU framework for the education and training of digital skills.

DigComp establishes a common reference model for what the European Commission envisions as the key competences and skills in the domain of IT literacy and digital proficiency.

In this module you will see in which way the DigComp frames cybersecurity and the competences associated to it.



Erasmus+

The European Commission's support for the production of
only of the authors, and the Commission cannot be held re

Index

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

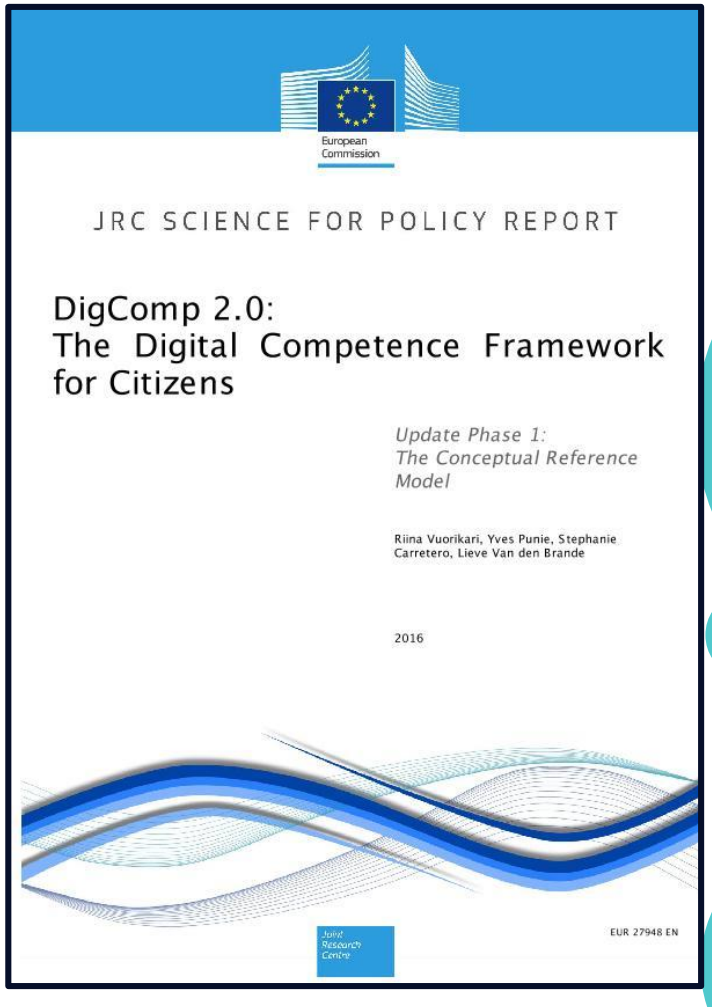
Unit 1: A comprehensive introduction to DigComp 2.1

Section 1.1: Background

In 2013, the Joint Research Centre of the European Commission published what became the theoretical framework for many projects carried out at both national and cross-national level aimed at empowering citizens' digital skills and ICT proficiency.

DigComp is among one of the largest EU's initiatives in the domain of education and training.

The main objective is to provide for a standard model through which Europeans access digital education and capacity building opportunities of IT skills.



Erasmus+

Unit 1: A comprehensive introduction to DigComp 2.1

Section 1.1: DigComp's 2013 version

In its initial version, the DigComp included 21 competences clustered into five areas of interest:

1. Information and data literacy	2. Communication and collaboration	3. Digital content creation	4. Safety	5. Problem Solving
• 1.1 Browsing, searching and filtering data, information and digital content • 1.2 Evaluating data, information and digital content • 1.3 Managing data, information and digital content	• 2.1 Interacting through digital technologies • 2.2 Sharing through digital technologies • 2.3 Engaging in citizenship through digital technologies • 2.4 Collaborating through digital technologies • 2.5 Netiquette • 2.6 Managing digital identity	• 3.1 Developing digital content • 3.2 Integrating and re-elaborating digital content • 3.3 Copyright and licences • 3.4 Programming	• 4.1 Protecting devices • 4.2 Protecting personal data and privacy • 4.3 Protecting health and well-being • 4.4 Protecting the environment	• 5.1 Solving technical problems • 5.2 Identifying needs and technological responses • 5.3 Creatively using digital technologies • 5.4 Identifying digital competence gaps

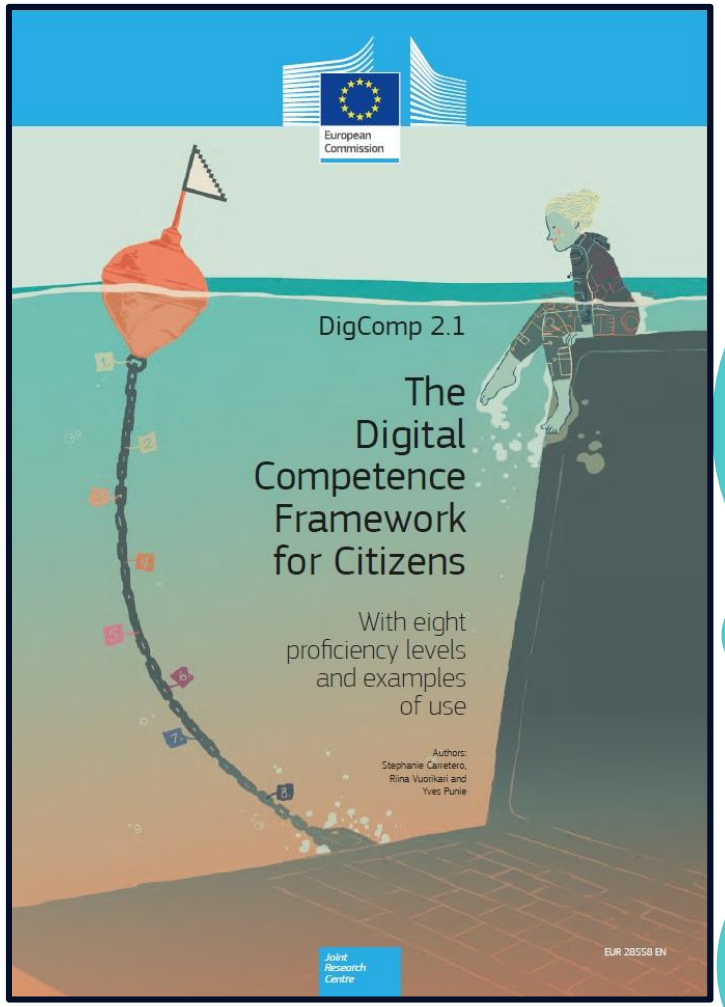
Erasmus+

Unit 1: A comprehensive introduction to DigComp 2.1

Section 1.2: DigComp 2.1 – what's new?

In 2017, the JRC published the official updated version of DigComp: DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use.

Compared to the previous version, the "new" DigComp includes eight proficiency level for each of the 21 competences that users can rely on to evaluate and assess their own expertise and competences with that given skill.



Erasmus+

Unit 1: A comprehensive introduction to DigComp 2.1

Section 1.3: DigComp 2.1 – the official follow-up

The JRC of the European Commission has been responsible also for the ultimate consolidation of two very important reports that summed up official exploitation of the DigComp in both educational/training settings (DigComp into Action, 2018) and employability/employment (DigComp at Work, 2020).

Both documents list a very comprehensive and detailed list of case studies (nearly 40 in total) that the European Commission elected as “best practices” for DigComp’s implementation.

Users can familiarise on how the DigComp can be applied within their operational context taking inspiration from consolidated and reliable lessons-learned.

Unit 1: A comprehensive introduction to DigComp 2.1

Section 1.4: DigComp into Action

DigComp into Action lists a series of best practices in the implementation of the DigComp 2.1 at transnational and national level.

The cohort of targets is very wide and diverse, testimonial of the great flexibility of the tool.

Entrepreneurs may find interesting case studies from which extrapolate source of inspiration for the training, capacity building and upskilling of their employees on digital skills and IT proficiency.

Unit 1: A comprehensive introduction to DigComp 2.1

Section 1.5: DigComp at Work

Similar to DigComp into Action, the DigComp at Work supports STKHs and groups of interest in the implementation of the DigComp 2.1 in employability and employment settings.

Readers can find robust case studies and best practices from private sector's representatives relying on DigComp for education and training on digital skills of their workforce.

Cybersecurity is area of interest of these initiatives and it is typically included as stand-alone training area of wider training curricula encompassing the broad spectrum of IT skills.

Erasmus+

Unit 2: DigComp 2.1 for Cyber awareness

Introduction: Why the DigComp for cybersecurity?

The DigComp 2.1 looks into IT skills and digital competences in high-demand not only in the labour market, but also in all domains of civil society and active citizenship.

With that said, users can work on the DigComp as a reference and support tool to reignite and foster their understanding and overall proficiency with the aforementioned 21 competences (with particular reference to those strictly pertaining to cybersecurity) while self-assessing their progress and the ones achieved by their employees/workers.

DigComp encourages users to take action in tackling and gaps and skills-lag while providing for a robust and reliable performance-monitoring model.

Erasmus+

Unit 2: DigComp 2.1 for Cyber awareness

Section 2.1: Analysing the Safety's pillar

As we already mentioned, DigComp 2.1 includes 21 key competences for digital literacy and IT proficiency that are grouped among five "pillars" (i.e., training areas) and progress through an 8-level proficiency model.

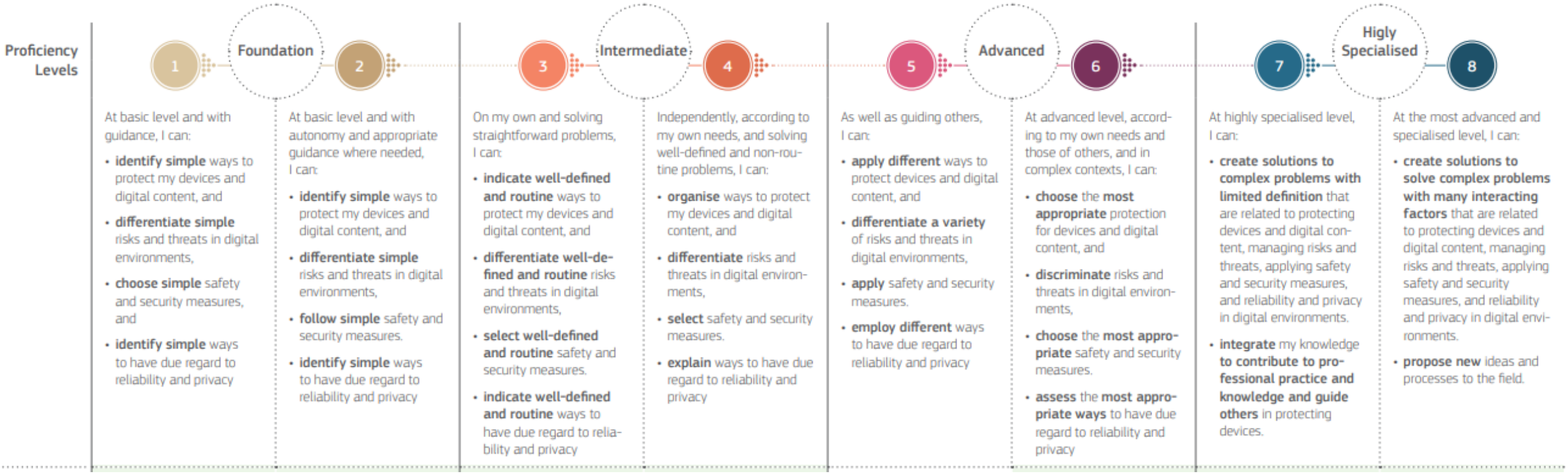
In the context of this training programme, it might be of particular interest for readers familiarising with the fourth pillar (i.e., Safety) – with specific reference to competence 4.1 and 4.2 (**Protecting devices** and **Protecting personal data and privacy**)

For each of the two competences, you can rely on the framework and the 8-level self-assessment model to evaluate your compliance with the highest standard of performance (i.e., Advanced and High-specialised levels)

Erasmus+

Unit 2: DigComp 2.1 for Cyber awareness

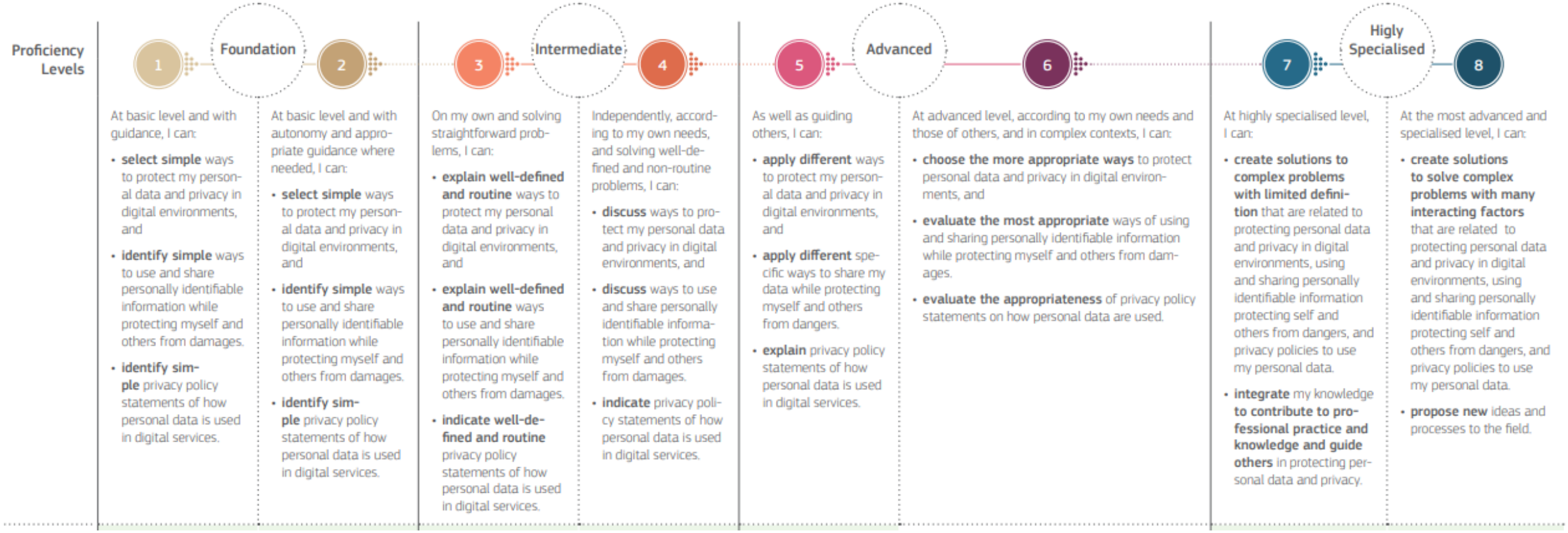
Section 2.2: 8 proficiency levels for 4.1 protecting devices



Source: DigComp 2.1, pp. 36

Unit 2: DigComp 2.1 for Cyber awareness

Section 2.3: 8 proficiency levels for 4.2 protecting privacy and data



Source: DigComp 2.1, pp. 37

Unit 2: DigComp 2.1 for Cyber awareness

Section 2.4: Competence no. 4.1 and no. 4.2

When it comes to cybersecurity and IT-hygiene, the DigComp can be relied on as a very robust tool to perform internal quality assurance processes while monitoring one's compliance with the highest safety standards.

Protecting devices and Protecting personal data and privacy are among the very essentials of cybersecurity for micro- and small/medium organisations.

Competence levels 7 and 8 indicate the long-term impact of embracing simple action as such into formalised and structured routines.

The training material developed by other Cyber-MSME partners indicates practical "tips and tricks", recommendations and tools to achieve the cyber-hygiene of devices and data.

Erasmus+

Unit 2: DigComp 2.1 for Cyber awareness

Section 2.5: Contributions from the fifth pillar

All fifth pillar's competences (5.1 Solving technical problems, 5.2 Identifying needs and technological responses, 5.3 Creatively using digital technologies, 5.4 Identifying digital competence gaps) should be considered as well as drivers of a cyber-aware mindset.

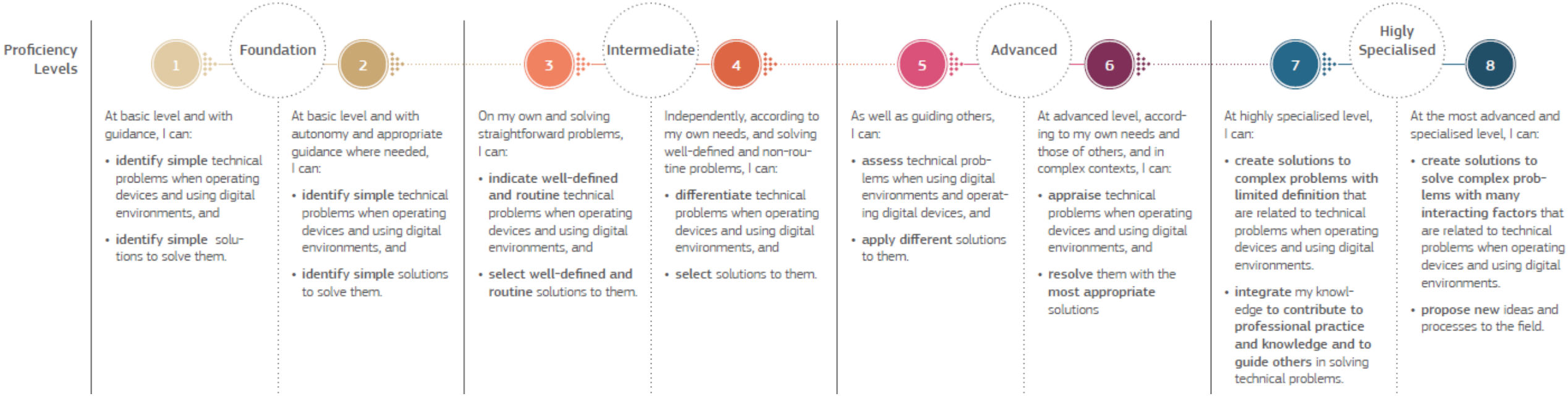
Problem solving for cybersecurity response essentially to the need of an operative framework for:

- Risk identification
- Risk analysis
- Risk evaluation
- Assessment, testing and validation of countermeasures

Problem solving embraces cybersecurity at large, including both new ways to approach to cybersecurity, and creative cost-effective solutions for cyber-resilience.

Unit 2: DigComp 2.1 for Cyber awareness

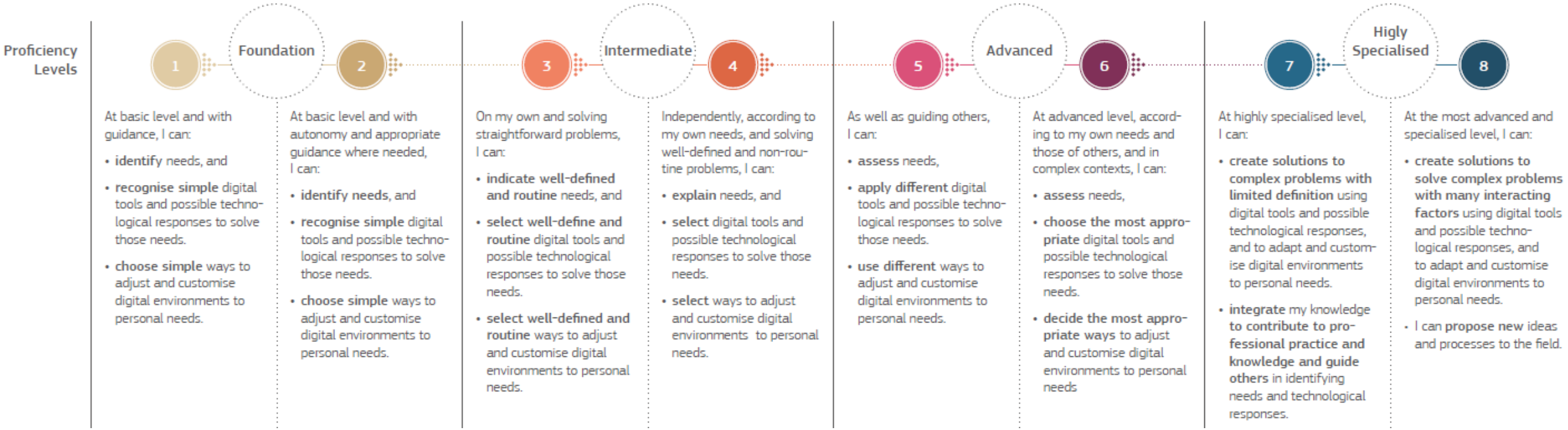
Section 2.6: 8 proficiency levels for 5.1 solving technical problems



Source: DigComp 2.1, pp. 40

Unit 2: DigComp 2.1 for Cyber awareness

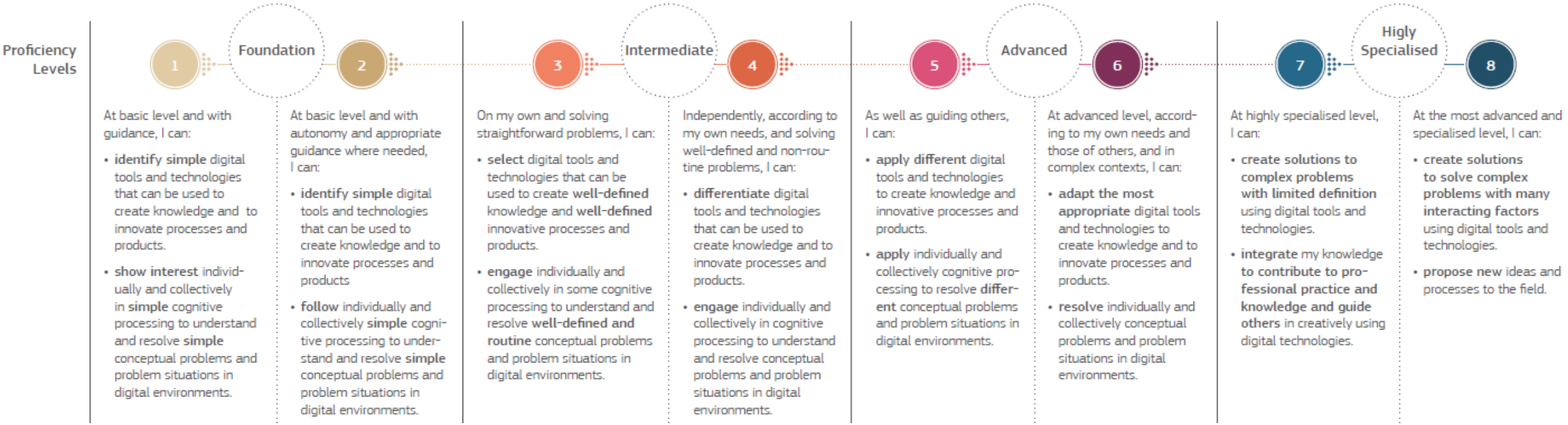
Section 2.7: 8 proficiency levels for 5.2 identifying needs and IT responses



Source: DigComp 2.1, pp. 41

Unit 2: DigComp 2.1 for Cyber awareness

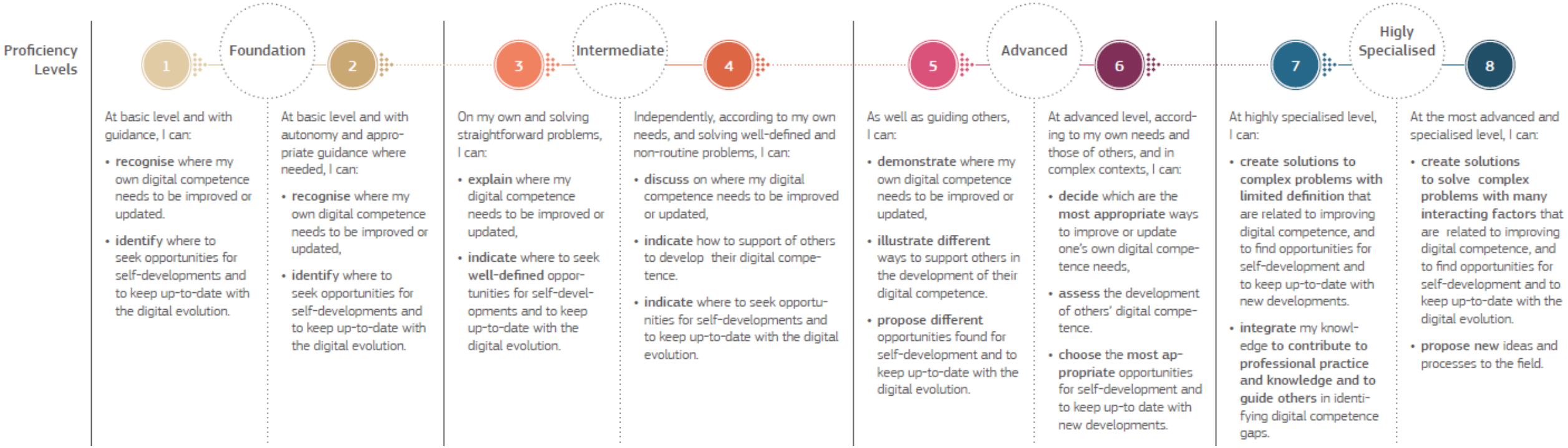
Section 2.8: 8 proficiency levels for 5.3 creative use of digital technologies



Source: DigComp 2.1, pp. 42

Unit 2: DigComp 2.1 for Cyber awareness

Section 2.9: 8 proficiency levels for 5.4 identifying digital competence gaps



Source: DigComp 2.1, pp. 43

Summing up

Key takeaways

- DigComp 2.1 – the EU framework for education and training on digital skills
- 5 training areas (i.e., pillars) for a total of 21 competences
- IT security and cyber-hygiene: pillar no.2
- 4.1 Protecting devices: 8-level progression model
- 4.2 Protecting personal data and privacy: 8-level progression model
- Problem Solving: Identification → Analysis → Evaluation

Erasmus+

Thank you

for your attention!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.