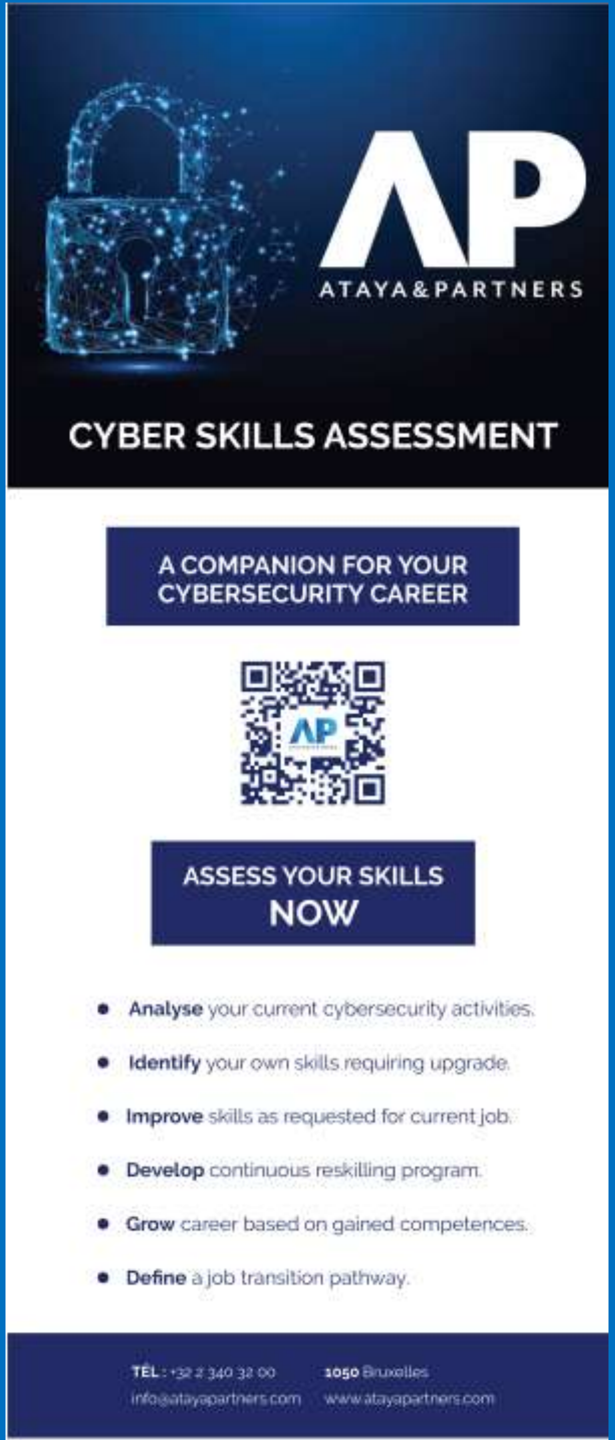


AP

ATAYA&PARTNERS

CYBER SKILLS ASSESSMENT

A COMPANION FOR YOUR CYBERSECURITY CAREER

ASSESS YOUR SKILLS NOW

- **Analyse** your current cybersecurity activities.
- **Identify** your own skills requiring upgrade.
- **Improve** skills as requested for current job.
- **Develop** continuous reskilling program.
- **Grow** career based on gained competences.
- **Define** a job transition pathway.

TÉL : +32 2 340 32 00
info@atayapartners.com

1050 Bruxelles
www.atayapartners.com

Security Forum

24 octobre 2019

Cyber skills Assessment

What skills do you miss in your current and future jobs?

Prof. Georges Ataya

High demand for Cybersecurity professionals

.AGORIA

% OF LABOUR DEMAND THAT WILL REMAIN UNFILLED IN 2030: TOP 3 SECTORS

18%
Healthcare

18%
ICT

13%
Education

4.5 million
WORKING PEOPLE NEED TO UPSKILL

584,000
UNFILLED VACANCIES IN BELGIUM IN 2030

310,000
WORKERS AND UNEMPLOYED PEOPLE IN RETRAINING

95 billion euros of GDP
AT STAKE IN 2030 ALONE

Source: “Digitalisation and the Belgian labour market” from Agoria

Cumulative impact

We do not have enough people

They do not have the right skills

They do not get the right training

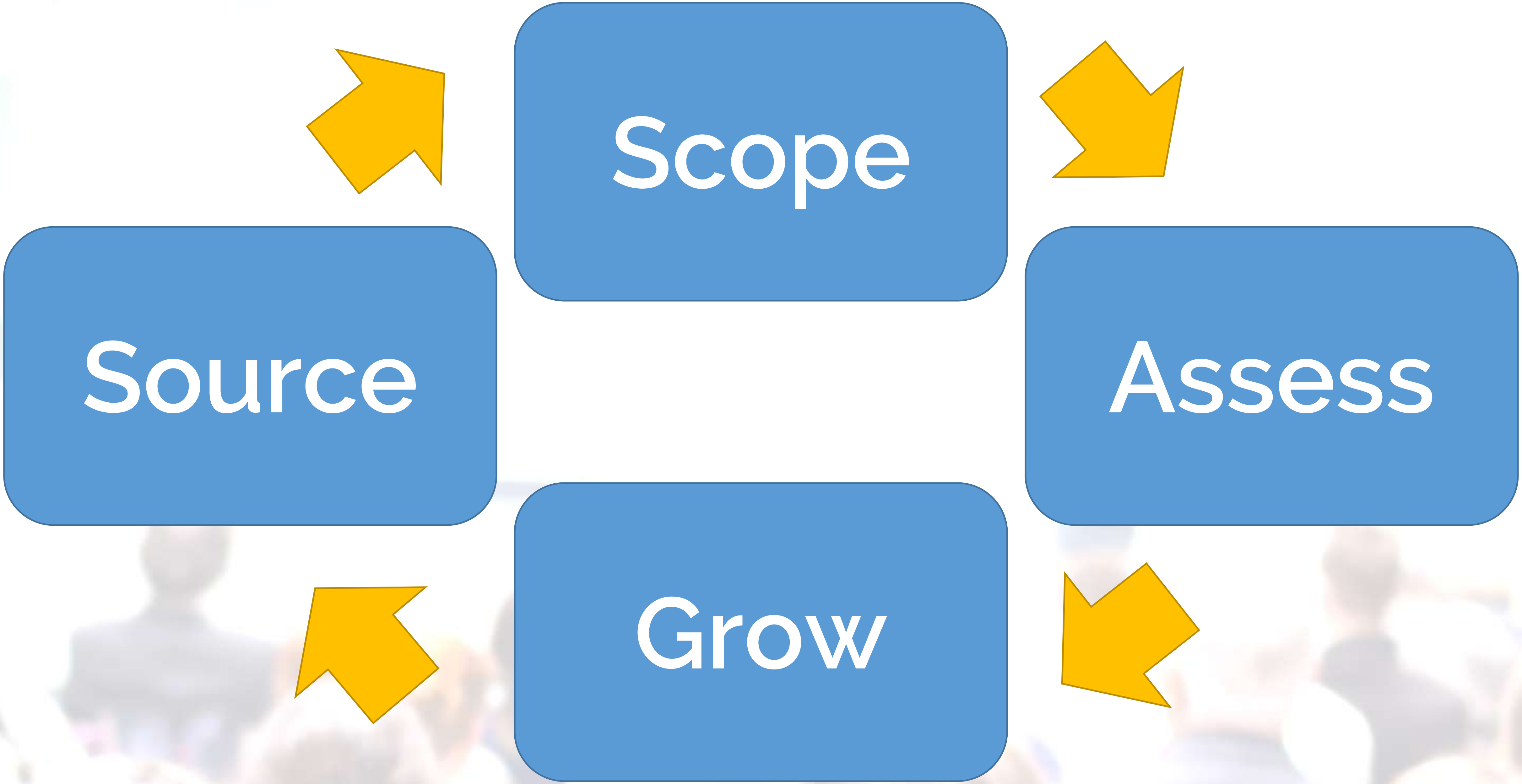
Training and education for an optimal preservation of Skills

Multiple sources for skills upgrade

The cybersecurity workforce gap to reach up to 350.000 positions in Europe by 2022

2017 Global Information Security Workforce Study.

sources for skills upgrade



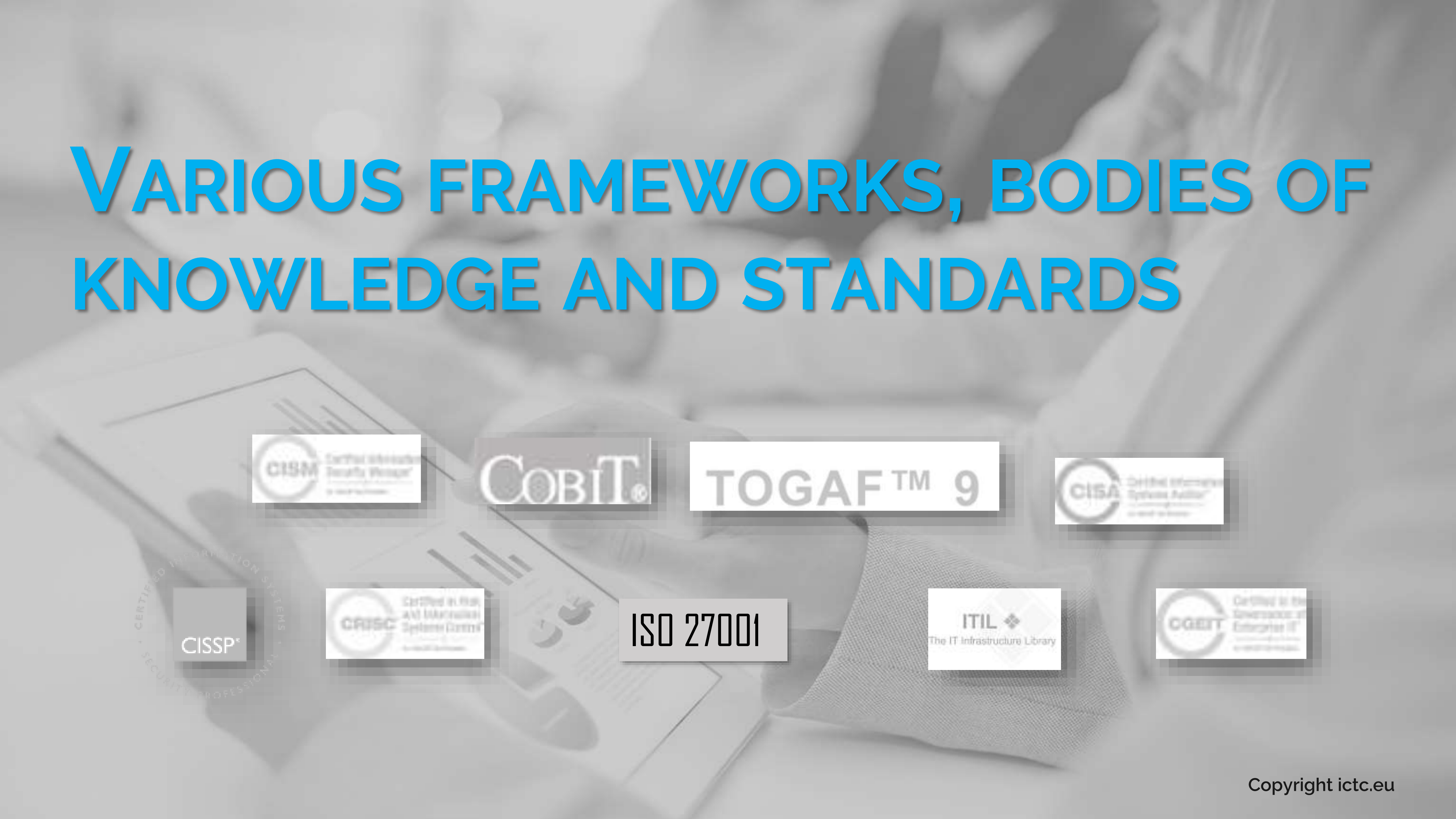
Scope

Assess

Grow

Source

Various frameworks, bodies of knowledge and standards



CISM Certified Information Security Manager

COBIT

TOGAF ™ 9

CISA Certified Information Systems Auditor

CISSP

CRISC Certified in Risk and Information Systems Control

ISO 27001

ITIL The IT Infrastructure Library

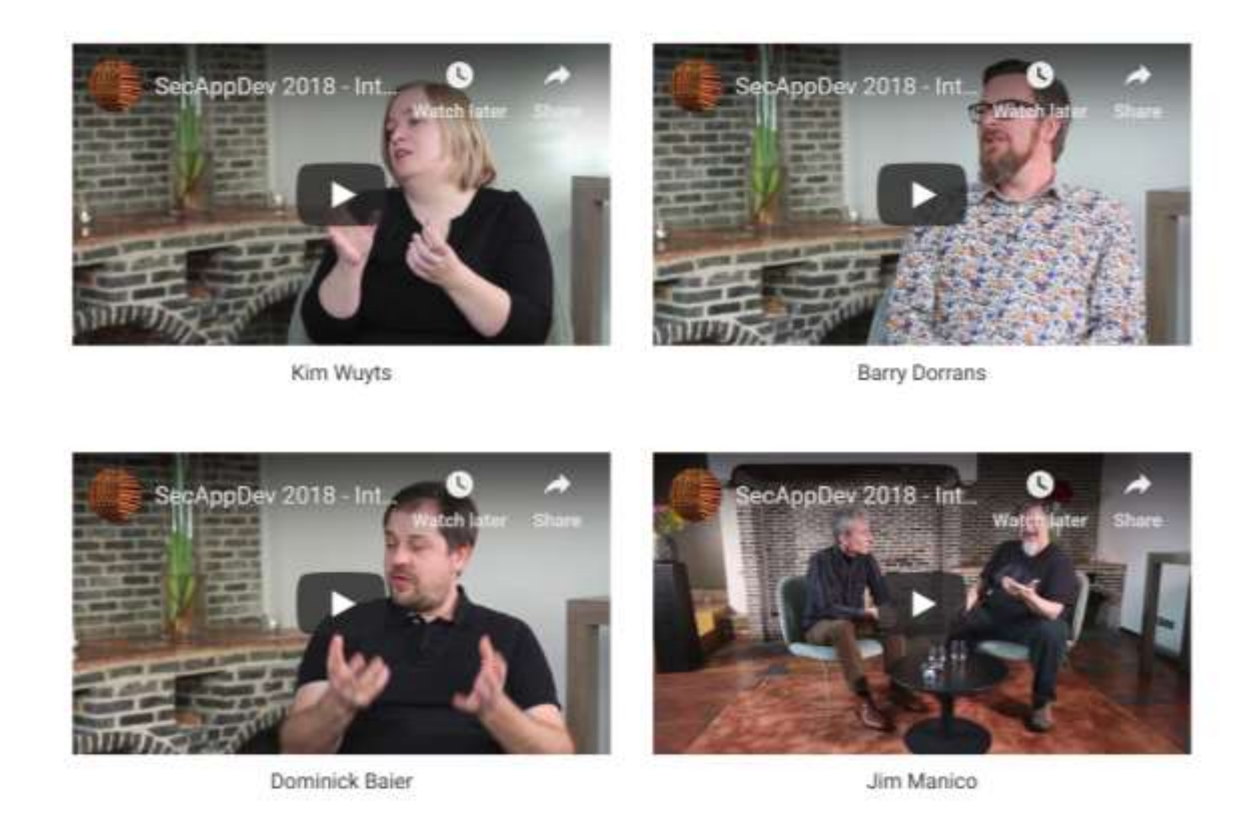
CGEIT Certified in the Governance of Enterprise IT

SECURE APPLICATION DEVELOPMENT

Brussels then L*euven*

secappdev.org

Co-founded, with Johan Peeters, the World-exclusive Secure Application Development week running since 2005. Speaks on Application security. International keynote speakers.



Kim Wuyts

Barry Dorrans

Dominick Baier

Jim Manico

Four major transformation were overall conducted:

Solvay Business School
Postgraduate Degree in ICT Audit & Security
IT Governance
IT MANAGEMENT EDUCATION
INFORMATION SECURITY MANAGEMENT EDUCATION

2001 – “Master in IT Audit”

2003 – “Postgraduate in IT Audit and Security”

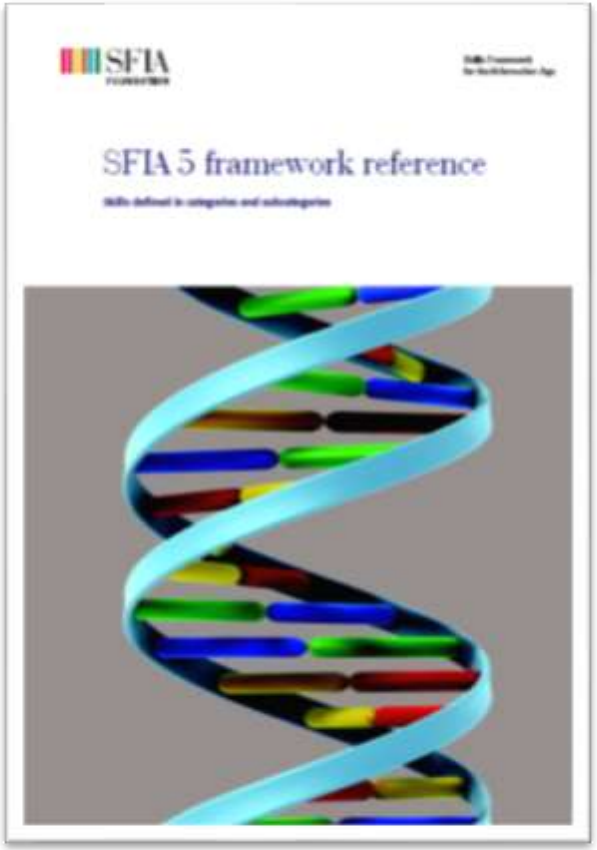
2009 – “Executive Master in IT Management”

2005 - 2012 – Executive Master and Executive Program in IT Governance were delivered in Brussels and in Dubai (UAE).

2015 – ”Executive Master in IT Management” and “Executive Master in Information Security” as well as ten derived Executive programs.

Information security management education

S – track Info Security	G – track IT Governance	M – track IT Management	B – track Business Agility	A – track Activating skills
S1 – Inform Secu Manag ISO 27001 CISM	G1 – The CIO Founda CGEIT	M1 – IT Service and Run Manag ITIL	B1 – Enterprise TOGAF™ 9	A1 – IT Finance and Portfolio Management
S2 – IT Security Practices CISSP	G2 – IT Governance Work COBIT®	M2 – Applications Build and Management	B2 – Business Transformation	A2 – Soft Skills for IT professionals
S3 – Cybersecurity Workshop	G3 – IT Risk and Legal cor CRISC	M3 – IT Sourcing Management	B3 – Digital Agility and Innovation	A3 – Building Expert Opi CISA



SFIA FOUNDATION

Skills Framework for the Information Age

SFIA 5 framework reference

Skills defined in categories and subcategories

SFIA FOUNDATION

Strategy and architecture

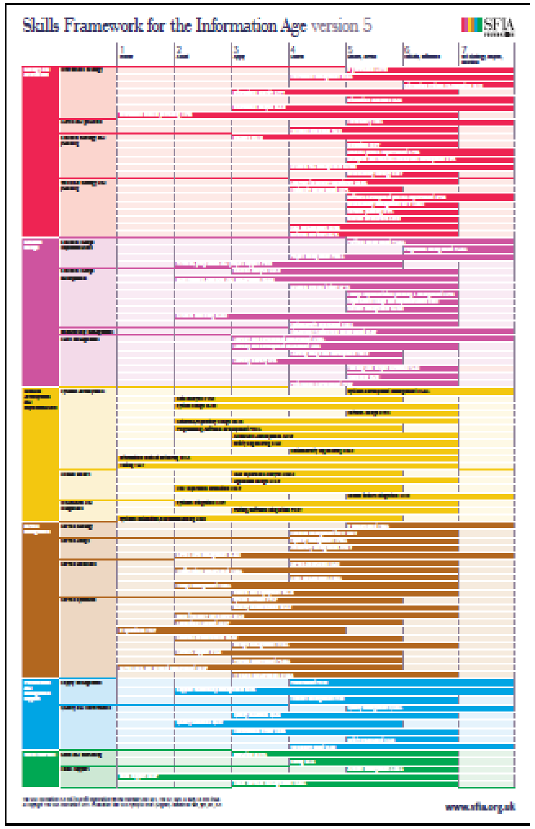
Business change

Solution development and implementation

Service management

Procurement and Management

Client interface



Skills Framework for the Information Age version 5

www.sfia.org.uk

Skills requirements for Cyber Security domains

Technical

1. Malicious Code and Activity
2. Networks and Communications
3. PKI and Cryptography
4. Forensics and Investigation
5. Evolving technology: Clouds, IOT, Big Data
6. Web security
7. Payment systems Security
8. Mobile and wireless Security
9. Physical Environmental

Generic

1. Information Security Architecture
2. Privacy
3. Access Control (IAM)
4. Standards, Policies
5. Detection, Monitoring and Analysis (IDP)
6. Legal, compliance and regulatory
7. Incident and Crisis Response
8. Recovery activities
9. Business process controls
10. Data Loss Management

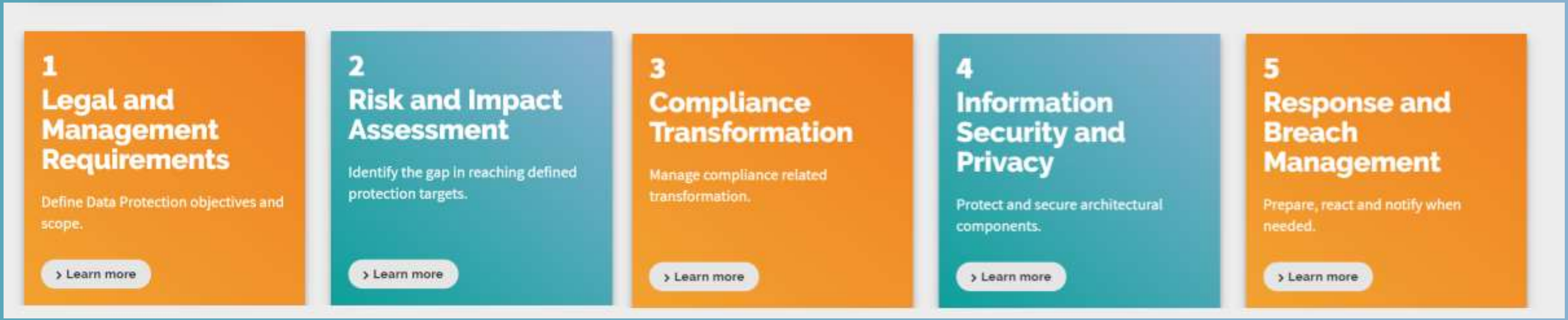
Management

1. Organization, planning and frameworks
2. Risk analysis and mitigation
3. Security Operations and Administration
4. Awareness campaigns and communication
5. Disaster planning and Recovery
6. Skills, sourcing and third party

Source: Georges Ataya

Leading to certified DPO

PROGRAMME IN EUROPEAN DATA PROTECTION



1 Legal and Management Requirements

Define Data Protection objectives and scope.

2 Risk and Impact Assessment

Identify the gap in reaching defined protection targets.

3 Compliance Transformation

Manage compliance related transformation.

4 Information Security and Privacy

Protect and secure architectural components.

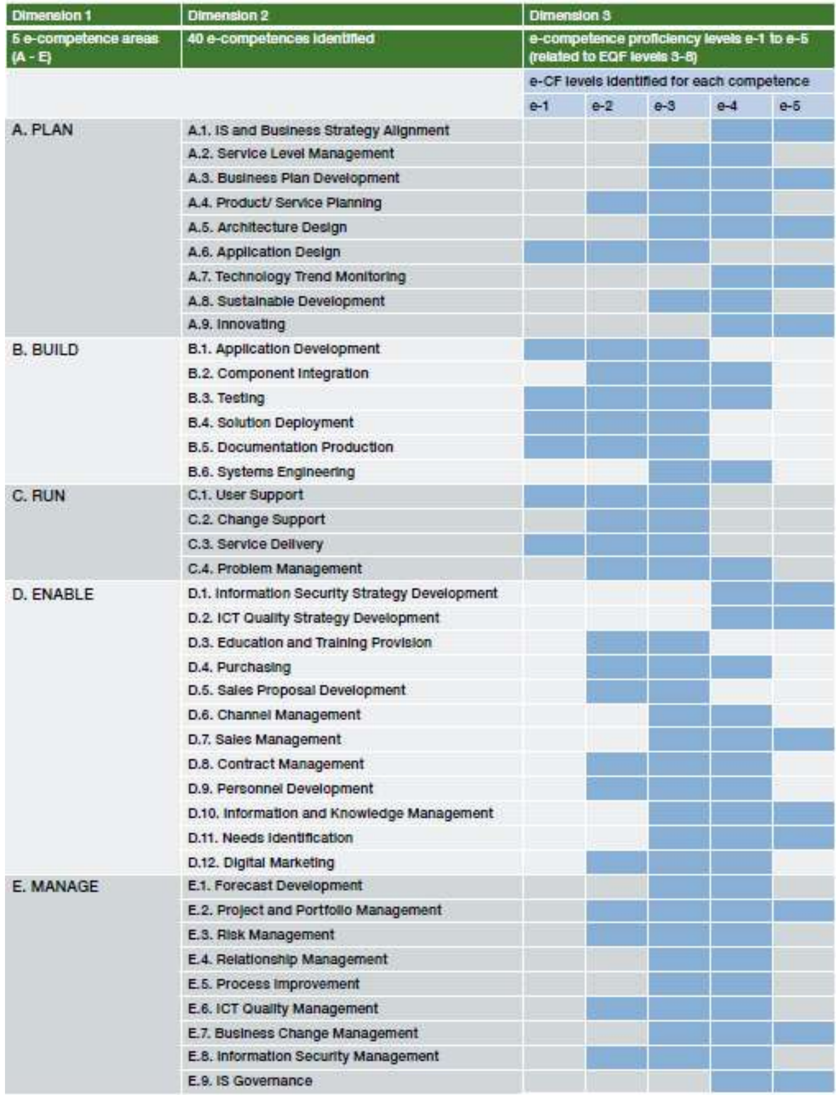
5 Response and Breach Management

Prepare, react and notify when needed.

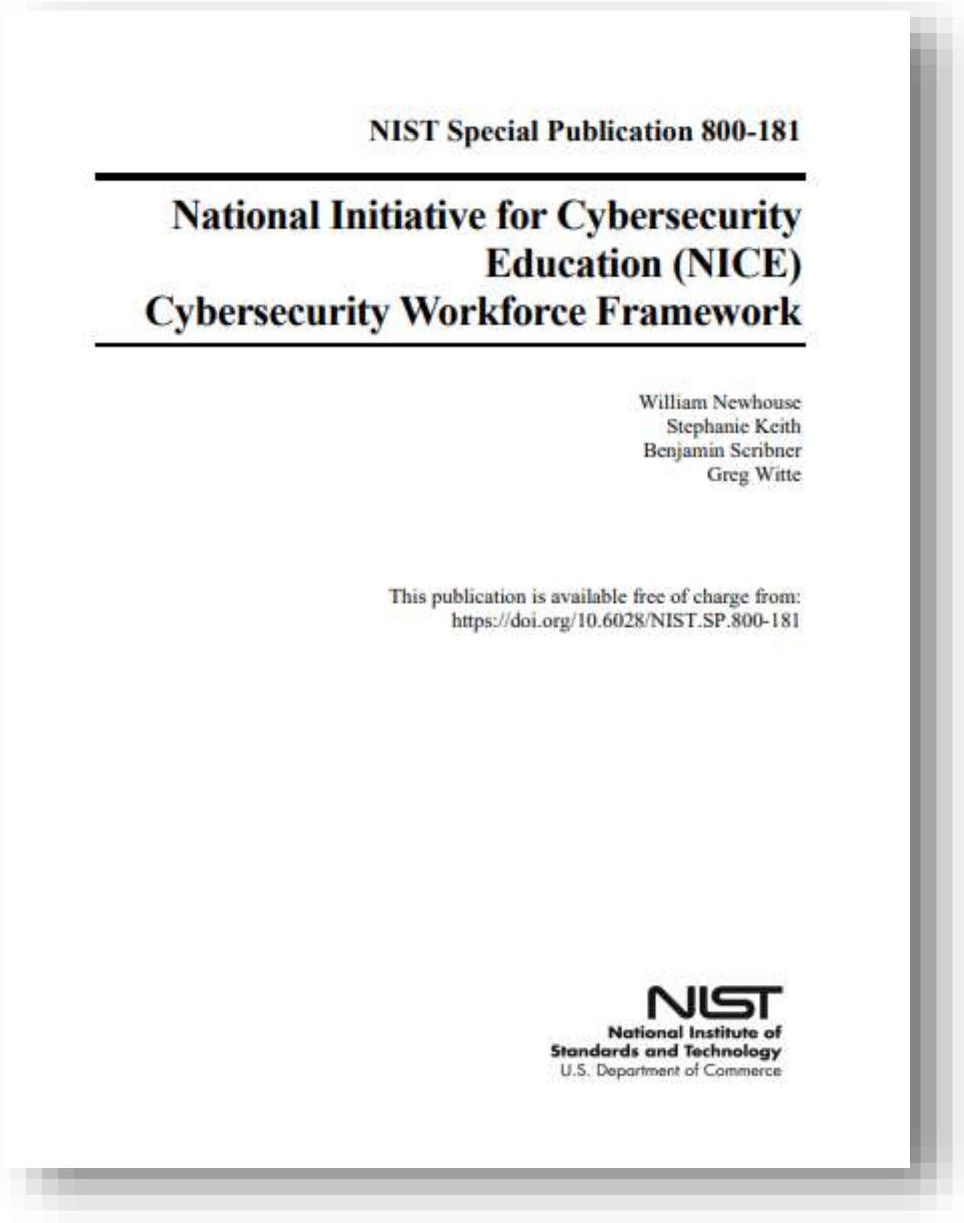
ULB Solvay Brussels School Executive Education

European e-Competence Framework 3.0

A common European framework for ICT Professionals in all industry sectors



Dimension 1	Dimension 2	Dimension 3				
5 e-competence areas (A - E)	40 e-competences identified	e-competence proficiency levels e-1 to e-5 (related to EQF levels 3-8)				
		e-CF levels identified for each competence				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. IS and Business Strategy Alignment				🟦	🟦
	A.2. Service Level Management			🟦	🟦	
	A.3. Business Plan Development			🟦	🟦	🟦
	A.4. Product/ Service Planning		🟦	🟦	🟦	
	A.5. Architecture Design			🟦	🟦	🟦
	A.6. Application Design	🟦	🟦	🟦		
	A.7. Technology Trend Monitoring				🟦	🟦
	A.8. Sustainable Development			🟦	🟦	
	A.9. Innovating				🟦	🟦
B. BUILD	B.1. Application Development	🟦	🟦	🟦		
	B.2. Component Integration		🟦	🟦	🟦	
	B.3. Testing	🟦	🟦	🟦	🟦	
	B.4. Solution Deployment	🟦	🟦	🟦		
	B.5. Documentation Production	🟦	🟦	🟦		
	B.6. Systems Engineering			🟦	🟦	
C. RUN	C.1. User Support	🟦	🟦	🟦		
	C.2. Change Support		🟦	🟦		
	C.3. Service Delivery	🟦	🟦	🟦		
	C.4. Problem Management		🟦	🟦	🟦	
D. ENABLE	D.1. Information Security Strategy Development				🟦	🟦
	D.2. ICT Quality Strategy Development				🟦	🟦
	D.3. Education and Training Provision		🟦	🟦		
	D.4. Purchasing		🟦	🟦	🟦	
	D.5. Sales Proposal Development		🟦	🟦		
	D.6. Channel Management			🟦	🟦	
	D.7. Sales Management			🟦	🟦	🟦
	D.8. Contract Management		🟦	🟦	🟦	
	D.9. Personnel Development		🟦	🟦	🟦	
	D.10. Information and Knowledge Management			🟦	🟦	🟦
	D.11. Needs Identification			🟦	🟦	🟦
	D.12. Digital Marketing		🟦	🟦	🟦	
E. MANAGE	E.1. Forecast Development			🟦	🟦	
	E.2. Project and Portfolio Management		🟦	🟦	🟦	🟦
	E.3. Risk Management		🟦	🟦	🟦	
	E.4. Relationship Management			🟦	🟦	
	E.5. Process Improvement			🟦	🟦	
	E.6. ICT Quality Management		🟦	🟦	🟦	
	E.7. Business Change Management			🟦	🟦	🟦
	E.8. Information Security Management		🟦	🟦	🟦	
	E.9. IS Governance				🟦	🟦



NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-181

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

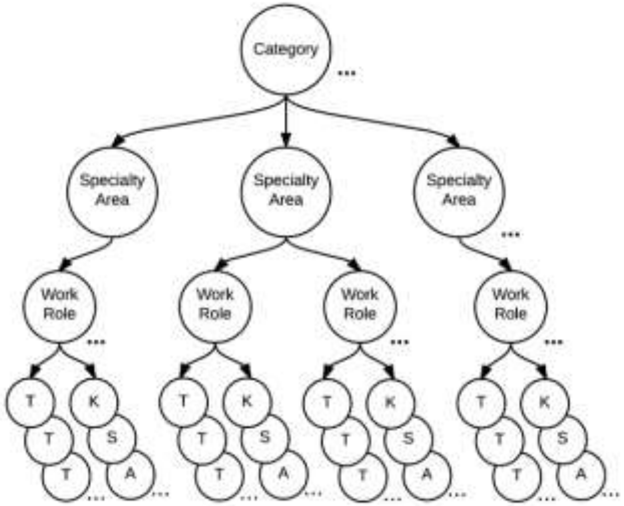
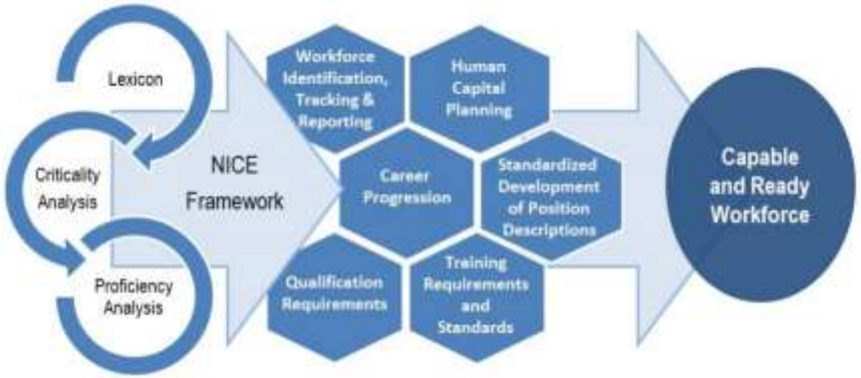


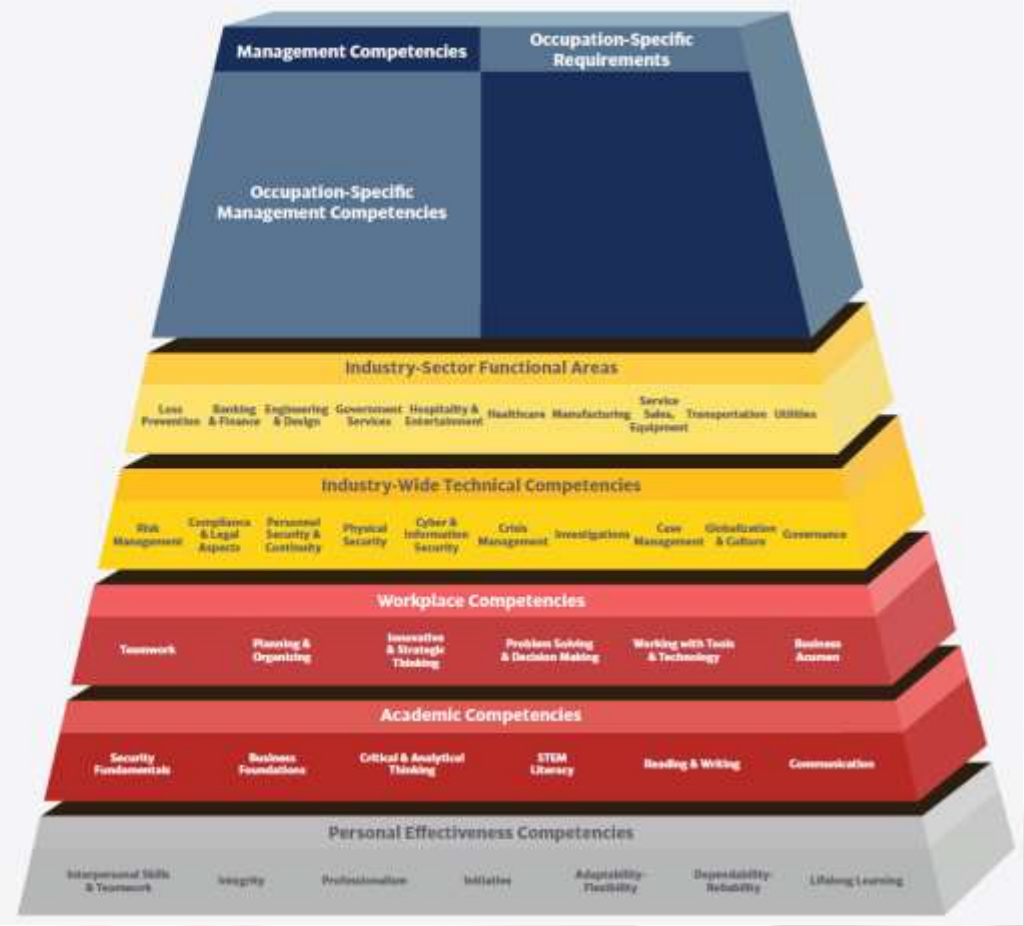
Figure 1 - Relationships among NICE Framework Components



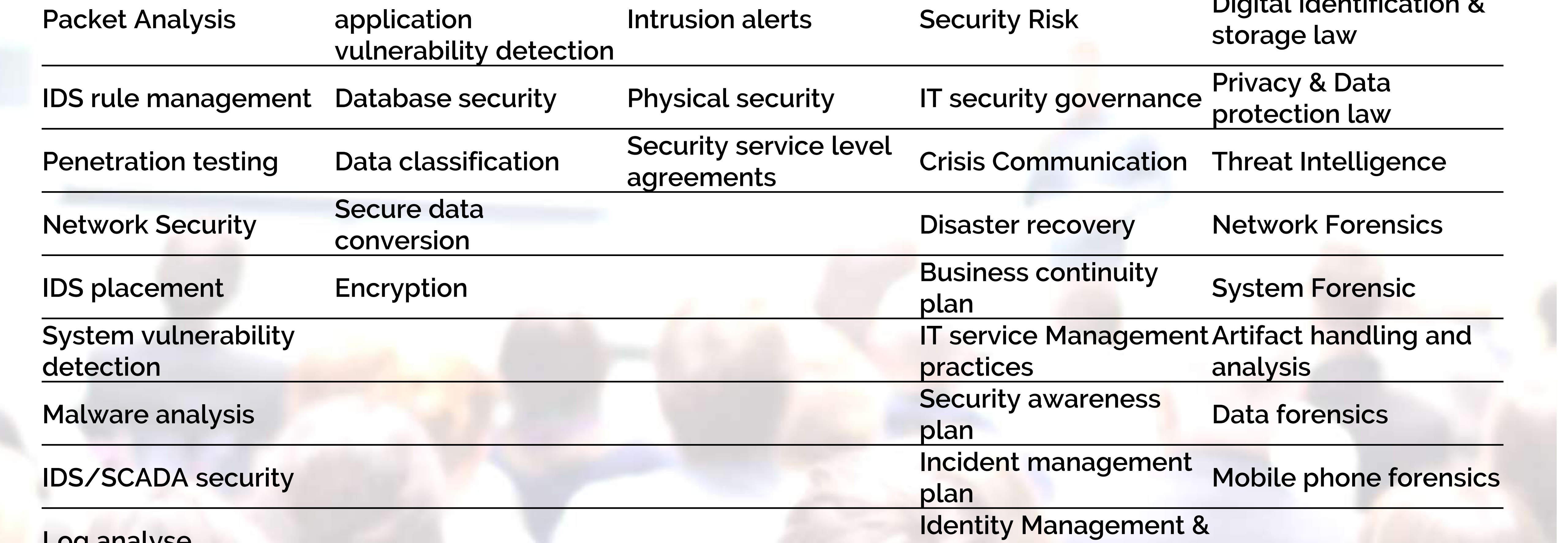
Lexicon
Criticality Analysis
Proficiency Analysis
NICE Framework
Workforce Identification, Tracking & Reporting
Human Capital Planning
Career Progression
Standardized Development of Position Descriptions
Qualification Requirements
Training Requirements and Standards
Capable and Ready Workforce

| Cybersecurity Competency Model

- Occupation-Related Competencies
  - Tier 9 – Management Competencies
  - Tier 8 – Occupation-Specific Requirements
  - Tier 7 – Occupation-Specific Technical Competencies
  - Tier 6 – Occupation-Specific Knowledge Competencies
- Industry-Related Competencies
  - Tier 5 – Industry-Sector Technical Competencies
  - Tier 4 – Industry-Wide Technical Competencies
- Foundational Competencies
  - Tier 3 – Workplace Competencies
  - Tier 2 – Academic Competencies
  - Tier 1 – Personal Effectiveness

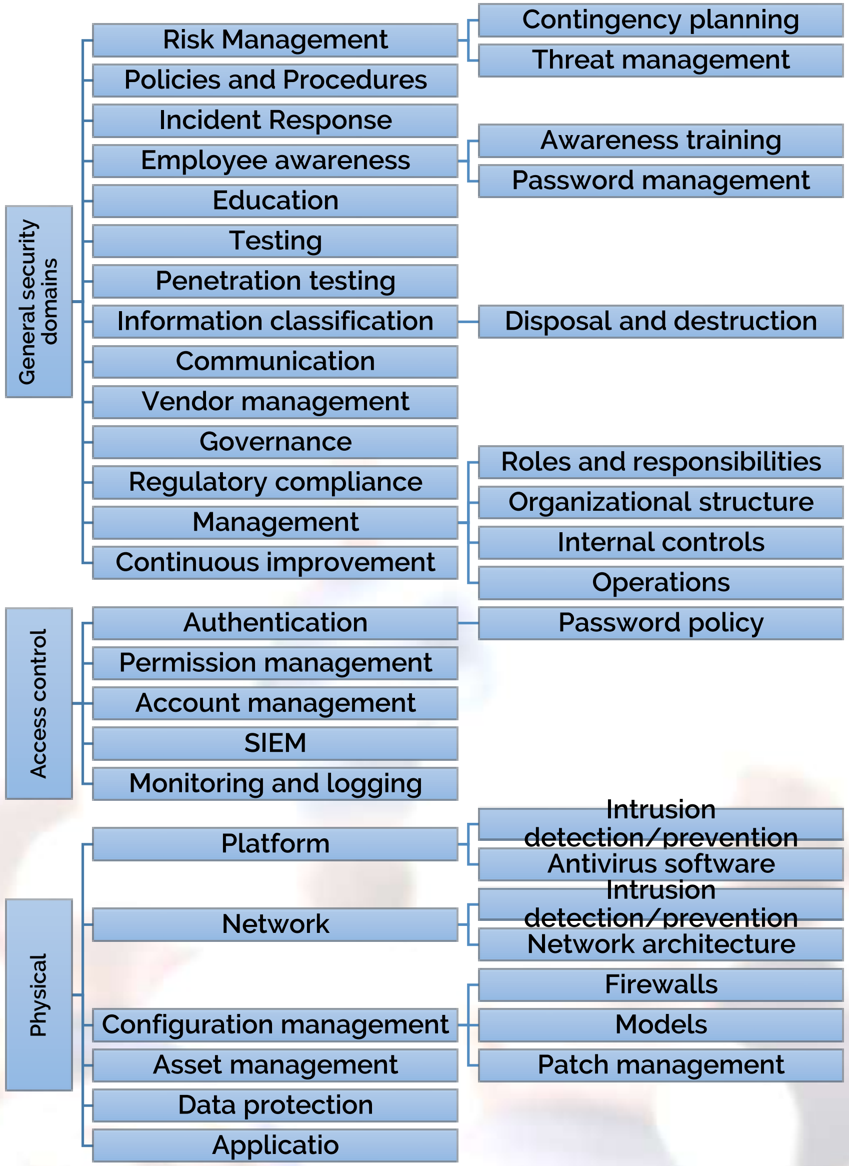


Industry-wide technical competences

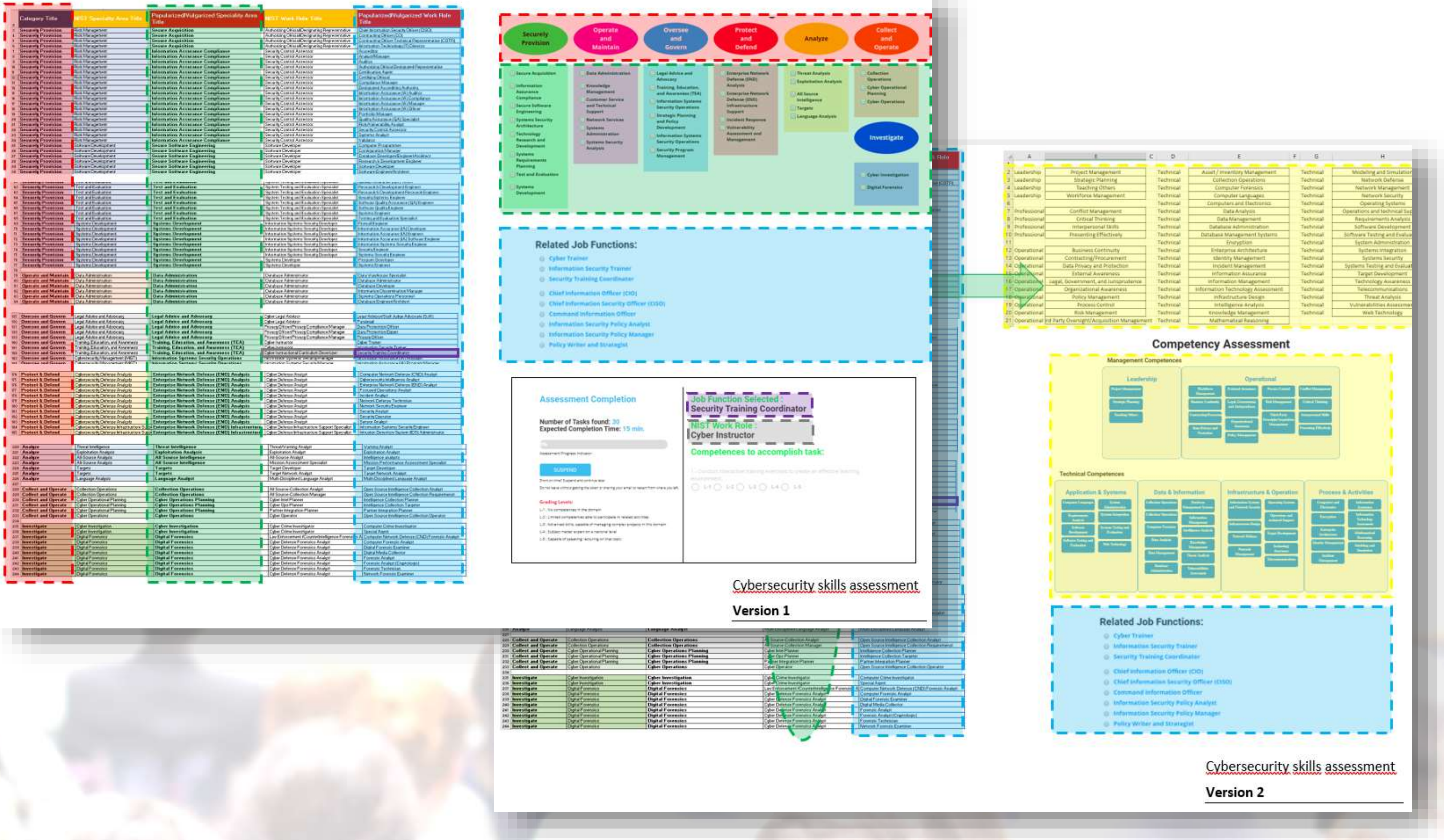


Network Security and Platform Security	Database and Application Security	Service Layer Security	Incident and Security Management	Forensics and Legal
Network vulnerability detection	Secure coding	Server security	Security Standards	Security of network and information systems law (NIS)
Authentication	Data validation	Cryptography	Incident handling	Cybercrime law
Packet Analysis	Webserver & application vulnerability detection	Intrusion alerts	Security Risk	Digital identification & storage law
IDS rule management	Database security	Physical security	IT security governance	Privacy & Data protection law
Penetration testing	Data classification	Security service level agreements	Crisis Communication	Threat Intelligence
Network Security	Secure data conversion		Disaster recovery	Network Forensics
IDS placement	Encryption		Business continuity plan	System Forensic
System vulnerability detection			IT service Management practices	Artifact handling and analysis
Malware analysis			Security awareness plan	Data forensics
IDS/SCADA security			Incident management plan	Mobile phone forensics
Log analyse			Identity Management &	

IT security domains



- General security domains
  - Risk Management
    - Contingency planning
    - Threat management
  - Policies and Procedures
  - Incident Response
  - Employee awareness
    - Awareness training
    - Password management
  - Education
  - Testing
  - Penetration testing
  - Information classification
    - Disposal and destruction
  - Communication
  - Vendor management
  - Governance
  - Regulatory compliance
  - Management
    - Roles and responsibilities
    - Organizational structure
    - Internal controls
    - Operations
  - Continuous improvement
- Access control
  - Authentication
    - Password policy
  - Permission management
  - Account management
  - SIEM
  - Monitoring and logging
- Physical
  - Platform
    - Intrusion detection/prevention
    - Antivirus software
  - Network
    - Intrusion detection/prevention
    - Network architecture
  - Configuration management
    - Firewalls
    - Models
    - Patch management
  - Asset management
  - Data protection
  - Applicatio



Category Title
NIST Specialty Area Title
Popularized/Vulgarized Specialty Area Title
NIST Work Role Title
Popularized/Vulgarized Work Role Title
Securely Provision
Operate and Maintain
Oversee and Govern
Protect and Defend
Analyze
Collect and Operate
Investigate
Secure Acquisition
Information Assurance Compliance
Secure Software Engineering
Systems Security Architecture
Technology Research and Development
Systems Requirements Planning
Test and Evaluation
Systems Development
Data Administration
Knowledge Management
Customer Service and Technical Support
Network Services
Systems Administration
Systems Security Analysis
Legal Advice and Advocacy
Training, Education, and Awareness (TEA)
Information Systems Security Operations
Strategic Planning and Policy Development
Information Systems Security Operations
Security Program Management
Enterprise Network Defense (END) Analysis
Enterprise Network Defense (END) Infrastructure Support
Incident Response
Vulnerability Assessment and Management
Threat Analysis
Exploitation Analysis
All Source Intelligence
Targets
Language Analysis
Collection Operations
Cyber Operational Planning
Cyber Operations
Cyber Investigation
Digital Forensics

Related Job Functions:

- Cyber Trainer
- Information Security Trainer
- Security Training Coordinator
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Command Information Officer
- Information Security Policy Analyst
- Information Security Policy Manager
- Policy Writer and Strategist

Assessment Completion

Number of Tasks found: 30
Expected Completion Time: 15 min.

Job Function Selected :
Security Training Coordinator

NIST Work Role :
Cyber Instructor

Competences to accomplish task:

○ L-1 ○ L-2 ○ L-3 ○ L-4 ○ L-5

	A	B	C	D	E	F	G	H
2	Leadership	Project Management		Technical	Asset / Inventory Management		Technical	Modeling and Simulation
3	Leadership	Strategic Planning		Technical	Collection Operations		Technical	Network Defense
4	Leadership	Teaching Others		Technical	Computer Forensics		Technical	Network Management
5	Leadership	Workforce Management		Technical	Computer Languages		Technical	Network Security
6				Technical	Computers and Electronics		Technical	Operating Systems
7	Professional	Conflict Management		Technical	Data Analysis		Technical	Operations and Technical Sup
8	Professional	Critical Thinking		Technical	Data Management		Technical	Requirements Analysis
9	Professional	Interpersonal Skills		Technical	Database Administration		Technical	Software Development
10	Professional	Presenting Effectively		Technical	Database Management Systems		Technical	Software Testing and Evalua
11				Technical	Encryption		Technical	System Administration
12	Operational	Business Continuity		Technical	Enterprise Architecture		Technical	Systems Integration
13	Operational	Contracting/Procurement		Technical	Identity Management		Technical	Systems Security
14	Operational	Data Privacy and Protection		Technical	Incident Management		Technical	Systems Testing and Evaluat
15	Operational	External Awareness		Technical	Information Assurance		Technical	Target Development
16	Operational	Legal, Government, and Jurisprudence		Technical	Information Management		Technical	Technology Awareness
17	Operational	Organizational Awareness		Technical	Information Technology Assessment		Technical	Telecommunications
18	Operational	Policy Management		Technical	Infrastructure Design		Technical	Threat Analysis
19	Operational	Process Control		Technical	Intelligence Analysis		Technical	Vulnerabilities Assessmen
20	Operational	Risk Management		Technical	Knowledge Management		Technical	Web Technology
21	Operational	rd Party Oversight/Acquisition Management		Technical	Mathematical Reasoning			

Competency Assessment

Related Job Functions:

- Cyber Trainer
- Information Security Trainer
- Security Training Coordinator
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Command Information Officer
- Information Security Policy Analyst
- Information Security Policy Manager
- Policy Writer and Strategist

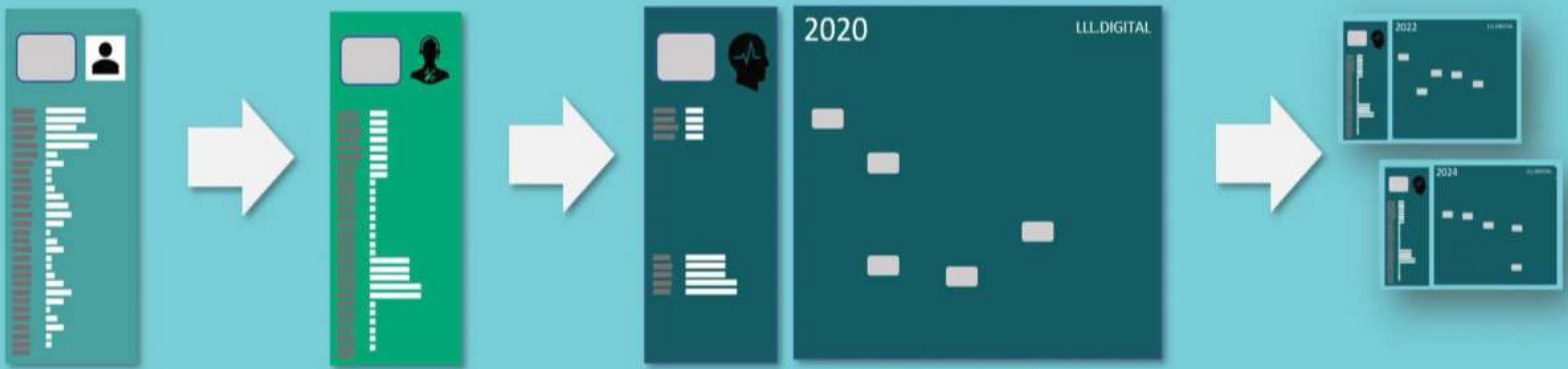
Cybersecurity skills assessment

Version 1

Cybersecurity skills assessment

Version 2

Life-Long Learning Concept



Assess your competences

Compare to your career target and current activity needs

Develop your life-long learning plan

Periodically Review and update your plan

Life-Long Learning Concept

Assess your competences

Digital Competences

AP Cybersecurity Competence Framework
SFIA
European e-Competence Framework

Managerial Competences

IT MANAGEMENT EDUCATION
INFORMATION SECURITY MANAGEMENT EDUCATION
PROGRAMME IN EUROPEAN DATA PROTECTION

Soft skills

Develop your life-long learning plan

Academic Education

Professional Certification

CEH CASP CISSP CAP
Security+ CISA CISM
cisco CompTIA vmware
ITIL PRINCE2 (ISC)² iseb
PMI Scrum ISACA ISTQB

Conferences

BELGIAN CYBER SECURITY CONVENTION

ICT Infrastructure

DIGITAL TRANSFORMATION CONFERENCE

INTERNET OF THINGS CONVENTION 2018

infosecurity BELGIUM

Self study

Udemy coursera

CSX CYBERSECURITY NEXUS PECB

Professional associations

CYBER SECURITY COALITION ECS

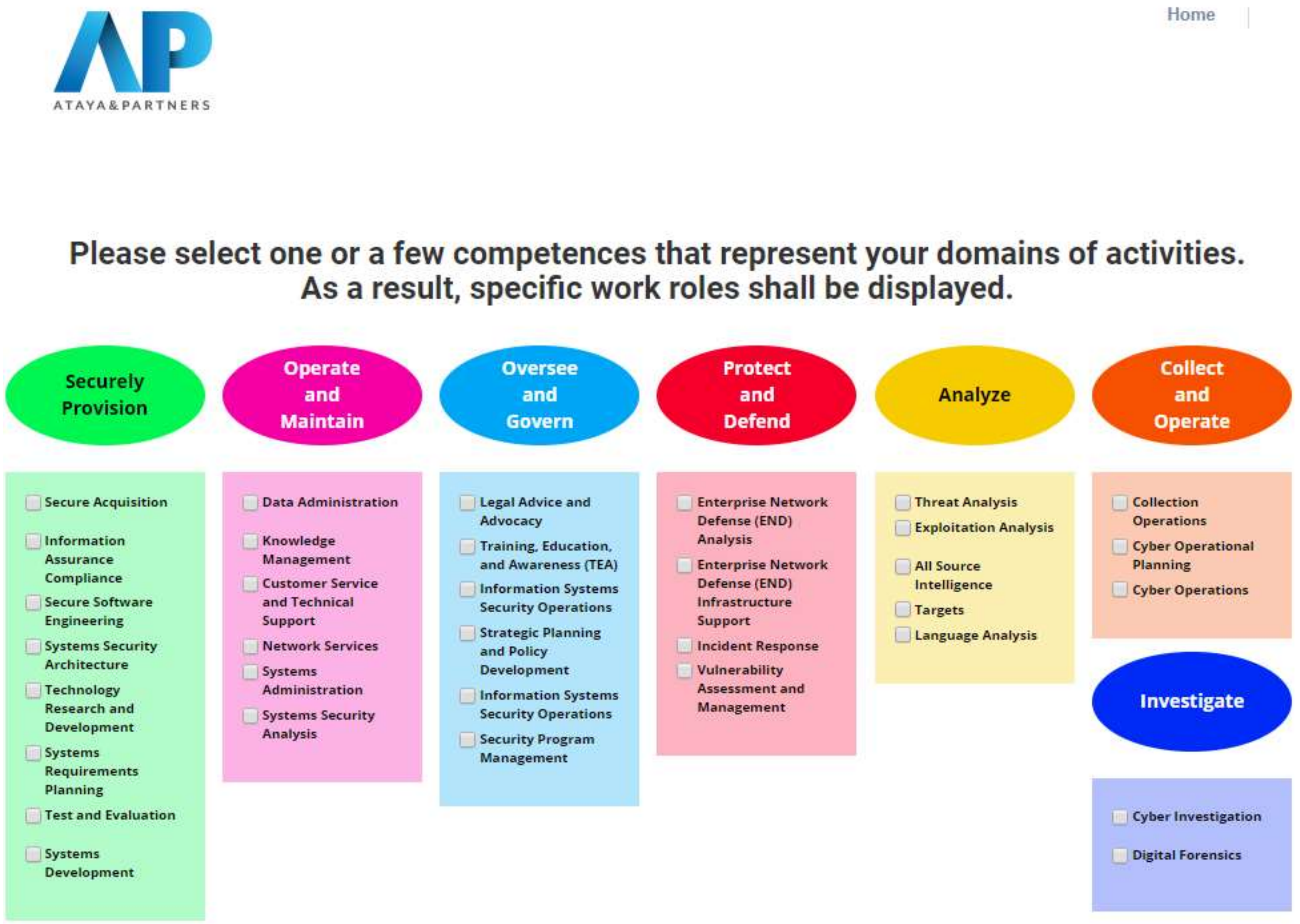
CIONET ISACA Belgium Chapter

A COMPANION FOR YOUR CYBERSECURITY CAREER

AP
ATAYA&PARTNERS

BETA VERSION

ASSESS YOUR SKILLS NOW



ATAYA&PARTNERS

Home

Please select one or a few competences that represent your domains of activities. As a result, specific work roles shall be displayed.

Securely Provision

- □ Secure Acquisition
- □ Information Assurance Compliance
- □ Secure Software Engineering
- □ Systems Security Architecture
- □ Technology Research and Development
- □ Systems Requirements Planning
- □ Test and Evaluation
- □ Systems Development

Operate and Maintain

- □ Data Administration
- □ Knowledge Management
- □ Customer Service and Technical Support
- □ Network Services
- □ Systems Administration
- □ Systems Security Analysis

Oversee and Govern

- □ Legal Advice and Advocacy
- □ Training, Education, and Awareness (TEA)
- □ Information Systems Security Operations
- □ Strategic Planning and Policy Development
- □ Information Systems Security Operations
- □ Security Program Management

Protect and Defend

- □ Enterprise Network Defense (END) Analysis
- □ Enterprise Network Defense (END) Infrastructure Support
- □ Incident Response
- □ Vulnerability Assessment and Management

Analyze

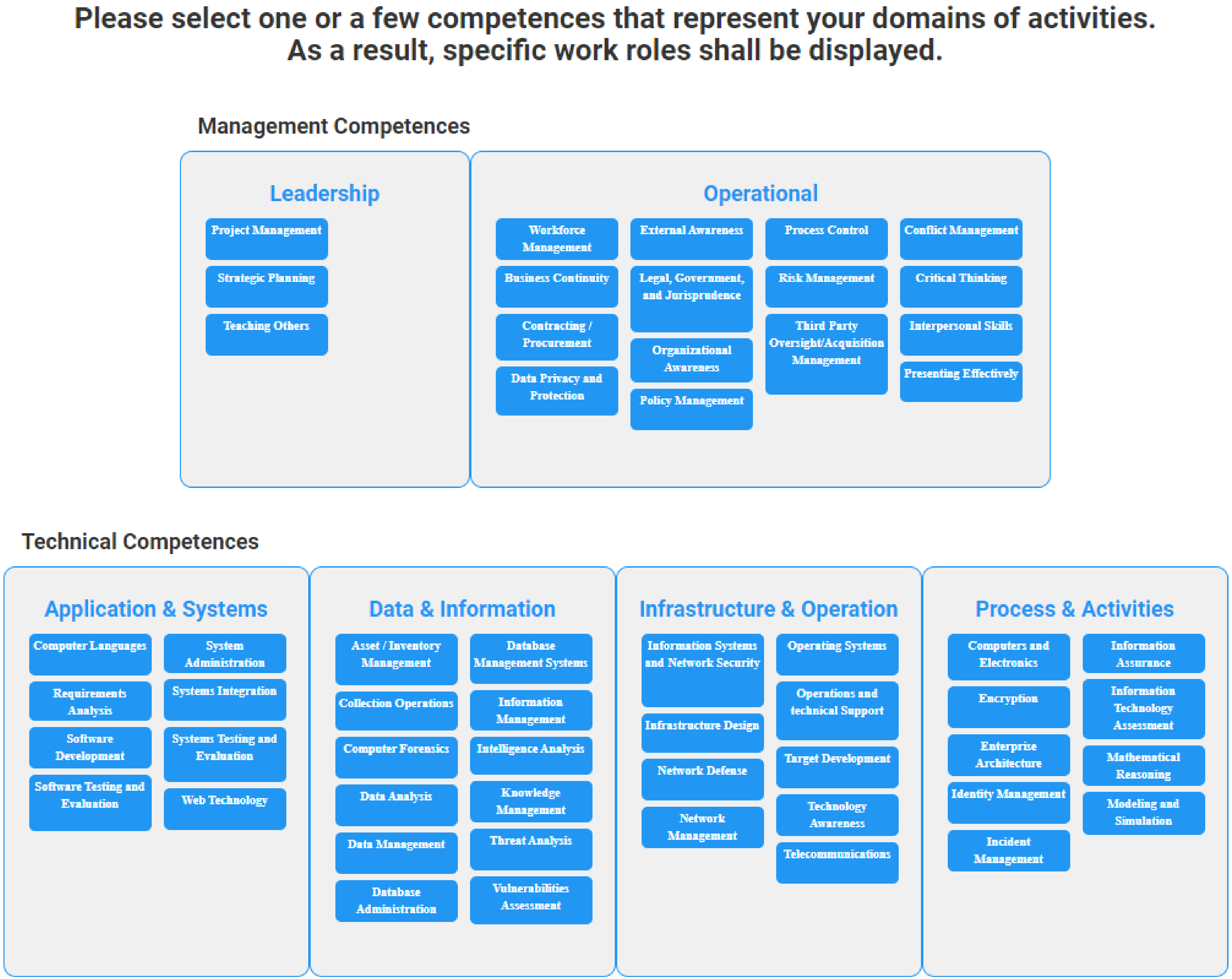
- □ Threat Analysis
- □ Exploitation Analysis
- □ All Source Intelligence
- □ Targets
- □ Language Analysis

Collect and Operate

- □ Collection Operations
- □ Cyber Operational Planning
- □ Cyber Operations

Investigate

- □ Cyber Investigation
- □ Digital Forensics



Please select one or a few competences that represent your domains of activities.
As a result, specific work roles shall be displayed.

Management Competences

Leadership

- Project Management
- Strategic Planning
- Teaching Others

Operational

- Workforce Management
- Business Continuity
- Contracting / Procurement
- Data Privacy and Protection
- External Awareness
- Legal, Government, and Jurisprudence
- Organizational Awareness
- Policy Management
- Process Control
- Risk Management
- Third Party Oversight/Acquisition Management
- Conflict Management
- Critical Thinking
- Interpersonal Skills
- Presenting Effectively

Technical Competences

Application & Systems

- Computer Languages
- Requirements Analysis
- Software Development
- Software Testing and Evaluation
- System Administration
- Systems Integration
- Systems Testing and Evaluation
- Web Technology

Data & Information

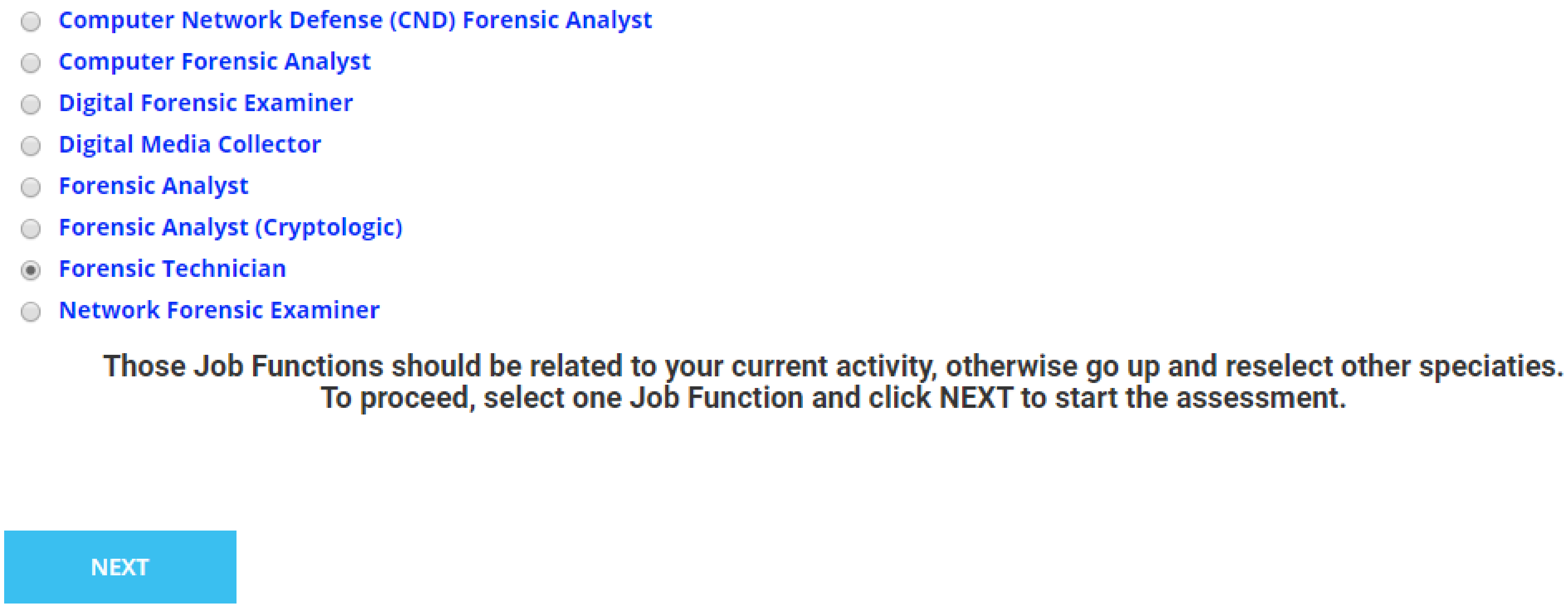
- Asset / Inventory Management
- Collection Operations
- Computer Forensics
- Data Analysis
- Data Management
- Database Administration
- Database Management Systems
- Information Management
- Intelligence Analysis
- Knowledge Management
- Threat Analysis
- Vulnerabilities Assessment

Infrastructure & Operation

- Information Systems and Network Security
- Infrastructure Design
- Network Defense
- Network Management
- Operating Systems
- Operations and technical Support
- Target Development
- Technology Awareness
- Telecommunications

Process & Activities

- Computers and Electronics
- Encryption
- Enterprise Architecture
- Identity Management
- Incident Management
- Information Assurance
- Information Technology Assessment
- Mathematical Reasoning
- Modeling and Simulation



○ Computer Network Defense (CND) Forensic Analyst

○ Computer Forensic Analyst

○ Digital Forensic Examiner

○ Digital Media Collector

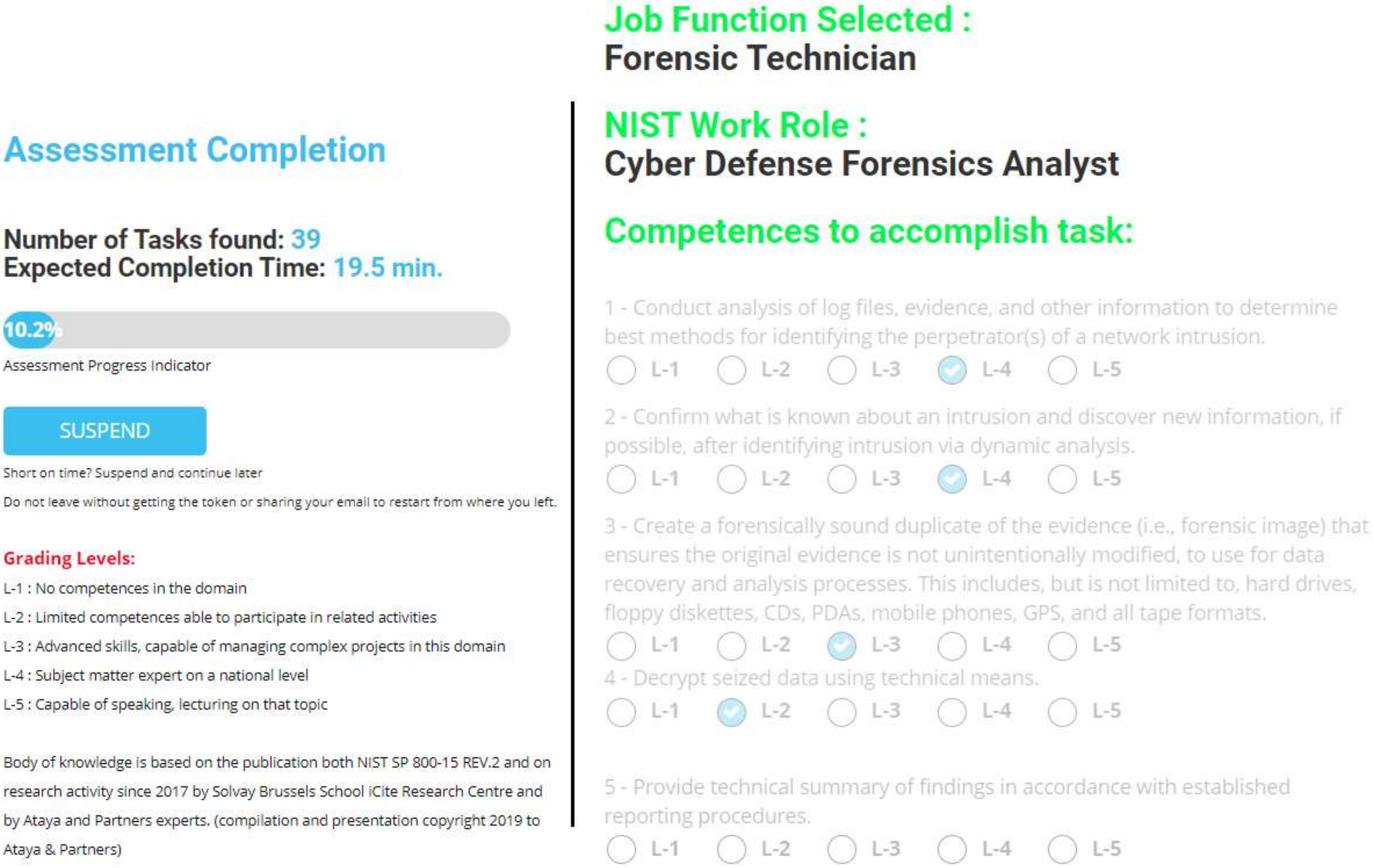
○ Forensic Analyst

○ Forensic Analyst (Cryptologic)

● Forensic Technician

○ Network Forensic Examiner

Those Job Functions should be related to your current activity, otherwise go up and reselect other speciaties.
To proceed, select one Job Function and click NEXT to start the assessment.



Assessment Completion

Number of Tasks found: 39
Expected Completion Time: 19.5 min.

Assessment Progress Indicator

Short on time? Suspend and continue later

Do not leave without getting the token or sharing your email to restart from where you left.

Grading Levels:

L-1 : No competences in the domain

L-2 : Limited competences able to participate in related activities

L-3 : Advanced skills, capable of managing complex projects in this domain

L-4 : Subject matter expert on a national level

L-5 : Capable of speaking, lecturing on that topic

Body of knowledge is based on the publication both NIST SP 800-15 REV.2 and on research activity since 2017 by Solvay Brussels School iCite Research Centre and by Ataya and Partners experts. (compilation and presentation copyright 2019 to Ataya & Partners)

Job Function Selected :
Forensic Technician

NIST Work Role :
Cyber Defense Forensics Analyst

Competences to accomplish task:

1 - Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.

○ L-1 ○ L-2 ○ L-3 ● L-4 ○ L-5

2 - Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.

○ L-1 ○ L-2 ○ L-3 ● L-4 ○ L-5

3 - Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.

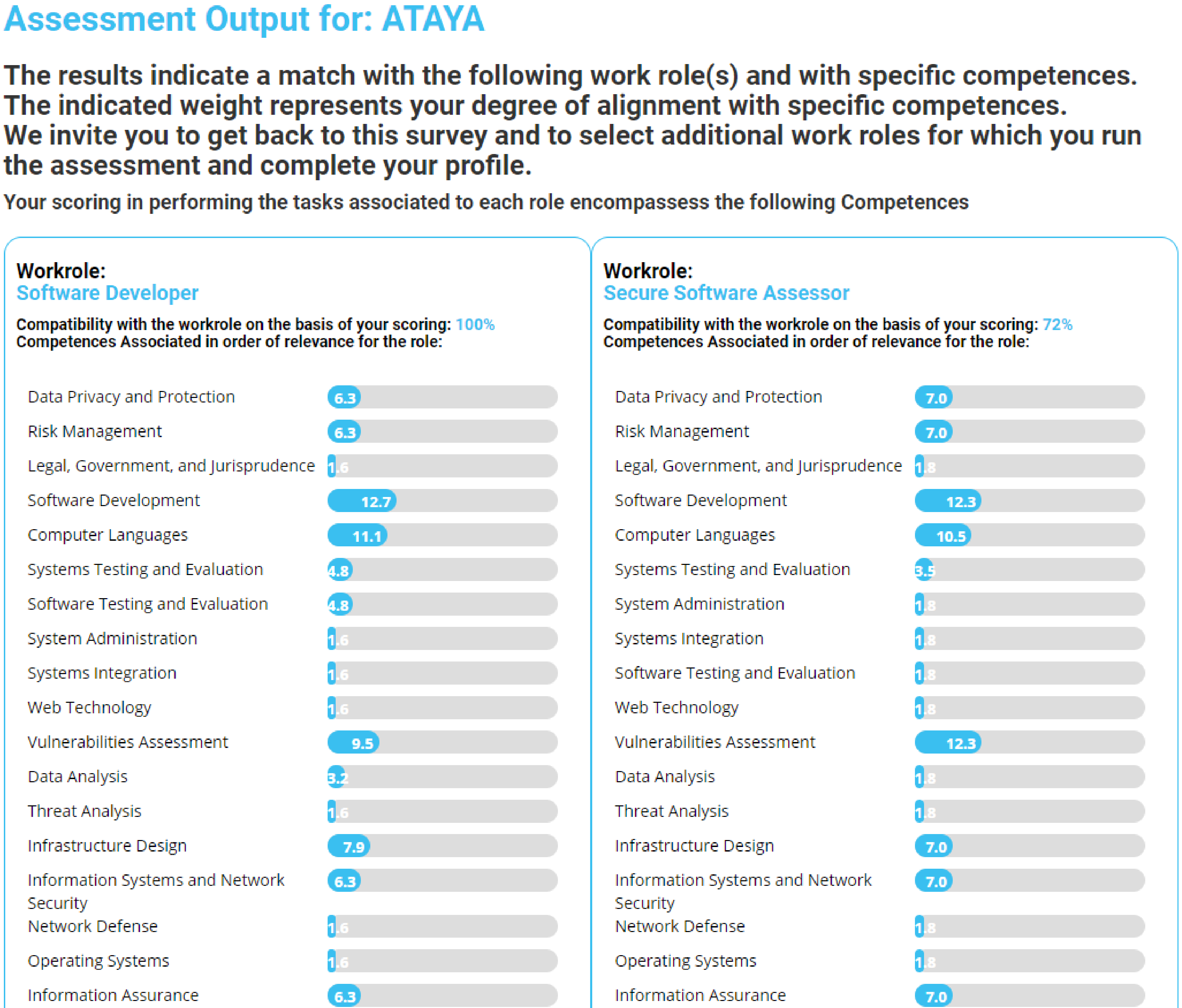
○ L-1 ○ L-2 ● L-3 ○ L-4 ○ L-5

4 - Decrypt seized data using technical means.

○ L-1 ● L-2 ○ L-3 ○ L-4 ○ L-5

5 - Provide technical summary of findings in accordance with established reporting procedures.

○ L-1 ○ L-2 ○ L-3 ○ L-4 ○ L-5



Assessment Output for: ATAYA

The results indicate a match with the following work role(s) and with specific competences.
The indicated weight represents your degree of alignment with specific competences.
We invite you to get back to this survey and to select additional work roles for which you run the assessment and complete your profile.

Your scoring in performing the tasks associated to each role encompassess the following Competences

Workrole:
Software Developer

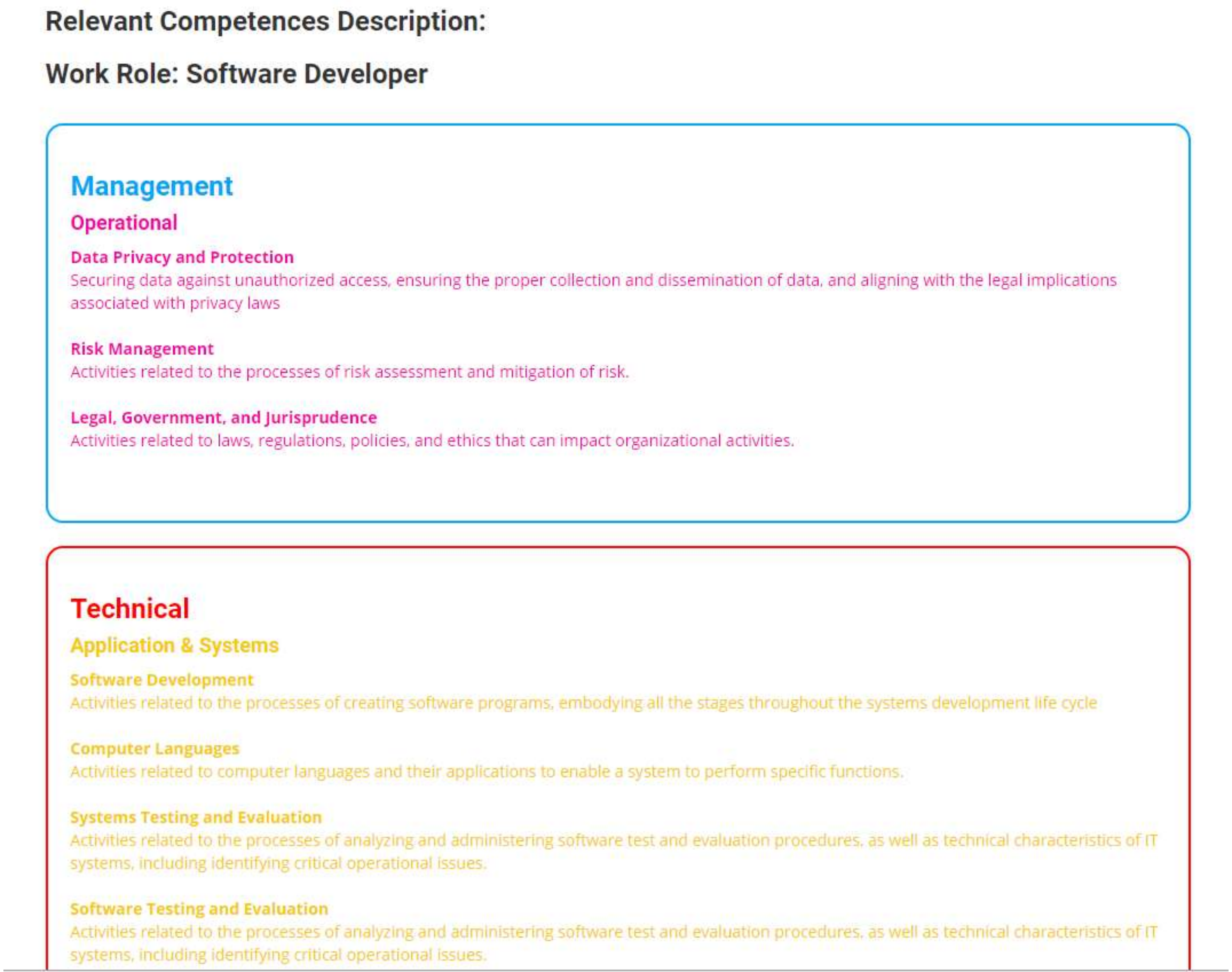
Compatibility with the workrole on the basis of your scoring: 100%
Competences Associated in order of relevance for the role:

Data Privacy and Protection	6.3
Risk Management	6.3
Legal, Government, and Jurisprudence	1.6
Software Development	12.7
Computer Languages	11.1
Systems Testing and Evaluation	4.8
Software Testing and Evaluation	4.8
System Administration	1.6
Systems Integration	1.6
Web Technology	1.6
Vulnerabilities Assessment	9.5
Data Analysis	3.2
Threat Analysis	1.6
Infrastructure Design	7.9
Information Systems and Network Security	6.3
Network Defense	1.6
Operating Systems	1.6
Information Assurance	6.3

Workrole:
Secure Software Assessor

Compatibility with the workrole on the basis of your scoring: 72%
Competences Associated in order of relevance for the role:

Data Privacy and Protection	7.0
Risk Management	7.0
Legal, Government, and Jurisprudence	1.8
Software Development	12.3
Computer Languages	10.5
Systems Testing and Evaluation	3.5
System Administration	1.8
Systems Integration	1.8
Software Testing and Evaluation	1.8
Web Technology	1.8
Vulnerabilities Assessment	12.3
Data Analysis	1.8
Threat Analysis	1.8
Infrastructure Design	7.0
Information Systems and Network Security	7.0
Network Defense	1.8
Operating Systems	1.8
Information Assurance	7.0



Relevant Competences Description:

Work Role: Software Developer

Management

Operational

Data Privacy and Protection
Securing data against unauthorized access, ensuring the proper collection and dissemination of data, and aligning with the legal implications associated with privacy laws

Risk Management
Activities related to the processes of risk assessment and mitigation of risk.

Legal, Government, and Jurisprudence
Activities related to laws, regulations, policies, and ethics that can impact organizational activities.

Technical

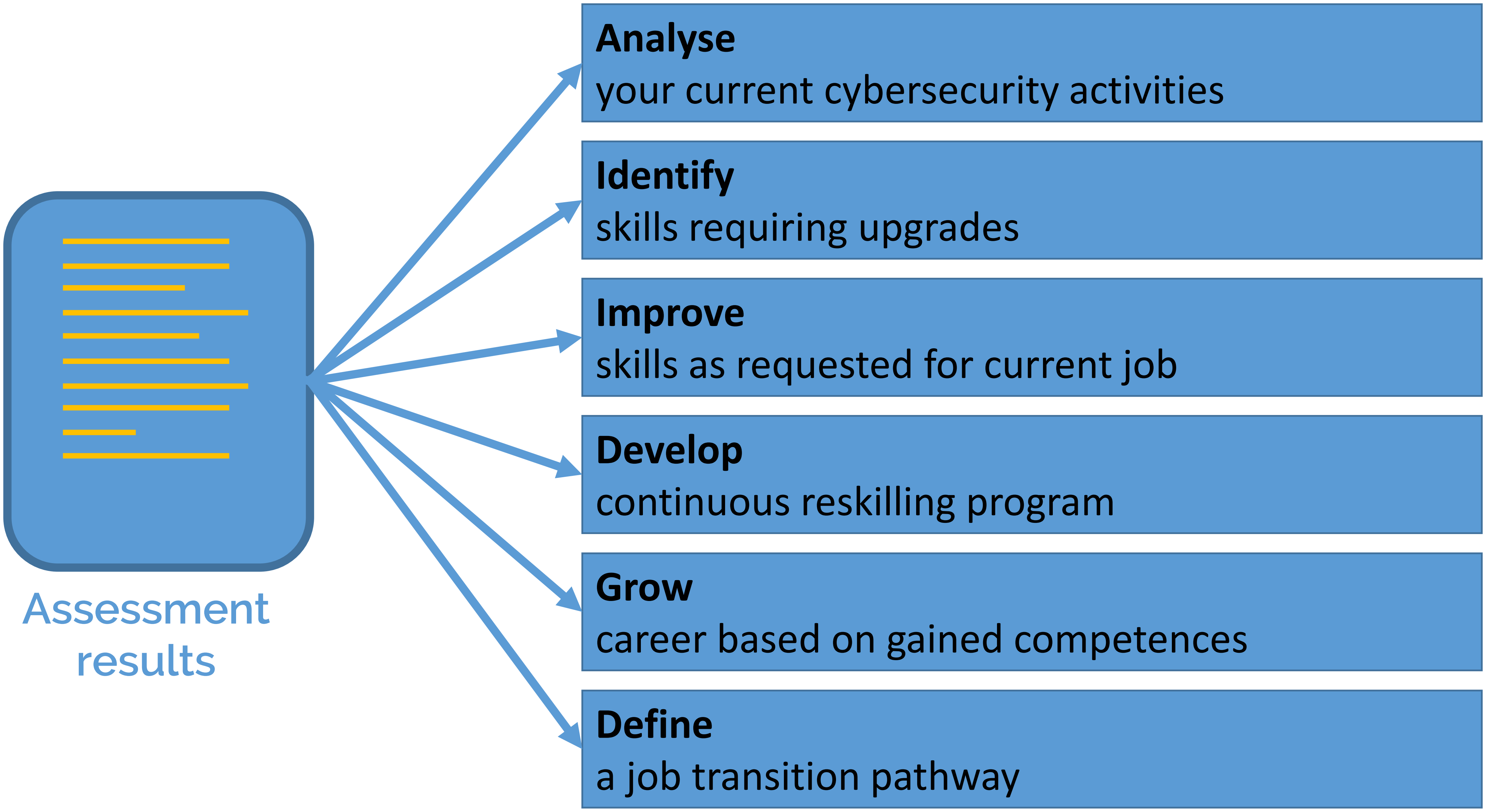
Application & Systems

Software Development
Activities related to the processes of creating software programs, embodying all the stages throughout the systems development life cycle

Computer Languages
Activities related to computer languages and their applications to enable a system to perform specific functions.

Systems Testing and Evaluation
Activities related to the processes of analyzing and administering software test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.

Software Testing and Evaluation
Activities related to the processes of analyzing and administering software test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.



Assessment results

Analyse
your current cybersecurity activities

Identify
skills requiring upgrades

Improve
skills as requested for current job

Develop
continuous reskilling program

Grow
career based on gained competences

Define
a job transition pathway

Professor, founder and Academic Director of Digital and information security management at SBS-EM
Co-founder of the Belgian Cybersecurity Coalition
Co-founder DPO Circle
Member of the Advisory Board: Agoria, BECI, CIONET, ISACA, belgian Cybersecurity Coalition
Founder at Ataya & Partners
Past International Vice President at ISACA
Past Partner Ernst & Young
Past Deputy International CIO ITT World Directories

gsm: +32 475 705709 -
solvay.edu/IT solvay.edu/gdpr

Solvay Brussels School
Economics & Management

Personal page: www.ataya.info - Skype: atayageorges -
twitter: gataya - Linked-in: ataya

ATAYA & PARTNERS