



CONCORDIA Feasibility study on Certifications schemes and the Skills Certification Framework

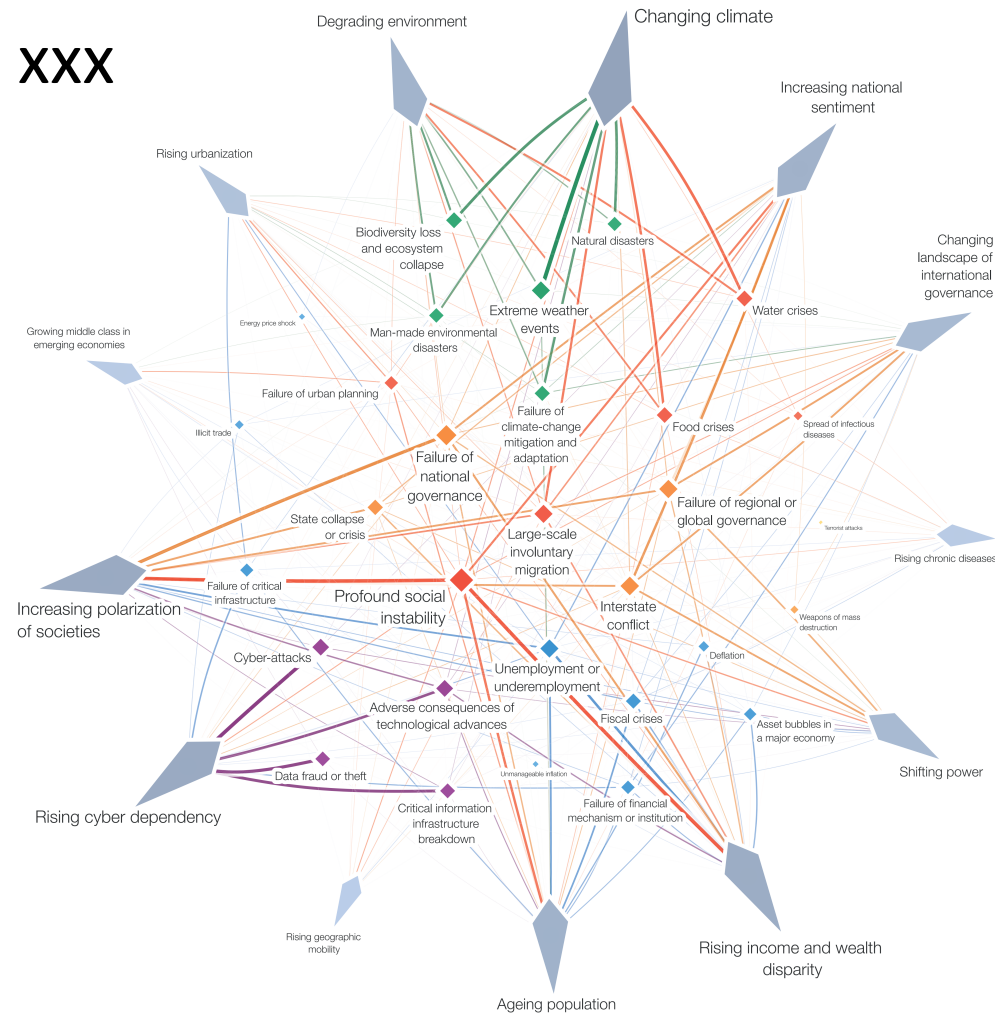
Presented by Chatzopoulou Argyro
TÜV TRUST IT GmbH

CONCORDIA Feasibility study on Certifications schemes



The Need for Cybersecurity Professionals

- XXX



Threats relating to Cybersecurity are identified as an emerging and persistent issue

Executive Perspectives on Top Risks 2019 and 2020, Protiviti (Protiviti, 2019)

The Global Risks Report 2019, World Economic Forum (World Economic Forum, 2019)

Ninth Annual Cost of Cybercrime Study, Accenture (Accenture, 2019)

Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 cybersecurity workforce study, 2019, (ISC)2, ((ISC)2, 2019)

State of Cybersecurity 2019 & 2020, ISACA (ISACA, 2020)

Is there a Cybersecurity Skills Gap?

- Enterprises are still short-staffed in cybersecurity, struggle to find sufficient talent for open positions and expect their cybersecurity budgets to grow. Efforts to increase the number of women in cybersecurity roles progressed slightly, and more enterprises established gender diversity programs.
- A shortage in the global cybersecurity workforce continues to be a problem for companies in all industries and of all sizes. In fact, this shortage remains the number one job concern for those working in the field. That's not surprising given that 2018 was "the year of the megabreach."

Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 cybersecurity workforce study, 2019, (ISC)2, ((ISC)2, 2019)

(ISC)2 Cybersecurity Workforce Study in 2018, (ISC)2 ((ISC)2, 2018)

State of Cybersecurity 2019 & 2020, ISACA (ISACA, 2020)

2017 Global Information Security Workforce Study, Benchmarking Workforce Capacity and Response to Cyber Risk, Frost & Sullivan, Centre for Cybersecurity Studies, 2017 (Frost & Sullivan, 2017).

Cloud Computing, Cyber Security and Green IT. The impact on e-Skills requirements" Final Report (Danish Technological Institute and Fraunhofer, 2012).

Skills Panorama (CEDEFOP, 2018)

ICT professionals: skills opportunities and challenges (2019 update) (CEDEFOP, 2019)

WG5 ANALYSIS Information and Cyber Security Professional Certification Task Force (EHR4CYBER), ECSO (ECSO, 2020)

The European e-Competence Framework (e-CF)

The European Norm (EN) 16234-1 European e-Competence Framework (e-CF) provides a reference of 41 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.

Dimension 1 5 e-CF areas (A – E)	Dimension 2 40 e-Competences identified	Dimension 3 e-Competence proficiency levels e-1 to e-5, related to EQF levels 3–8				
		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					



European ICT Professional Role Profiles



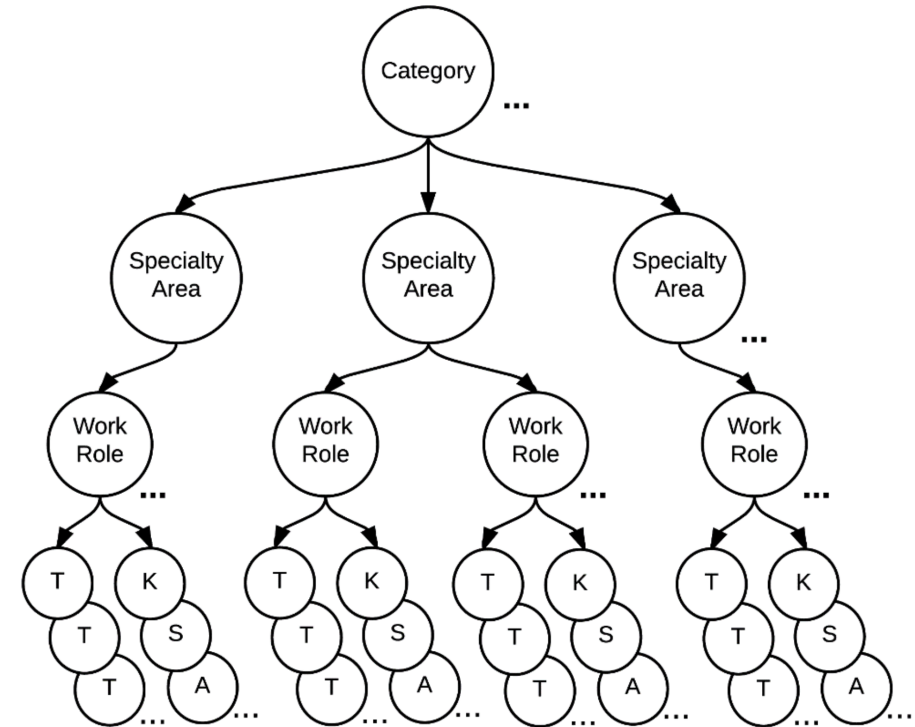
ESCO (European Skills, Competences, Qualifications and Occupations)

is the European multilingual classification of Skills, Competences, Qualifications and Occupations.

ESCO provides descriptions of 2942 occupations and 13.485 skills linked to these occupations.

- ICT security administrator
- ICT security consultant
- Chief ICT security officer
- ICT security manager
- Director of compliance and information security in gambling
- ICT security technician

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) (NIST, 2017) , published by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-181, is a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed .





Profile title	INFORMATION SECURITY MANAGER ROLE (11)		
Summary statement	Leads and manages the organisation information security policy.		
Mission	Defines the information security strategy and manages implementation across the organisation. Embeds proactive information security protection by assessing, informing, alerting and educating the entire organisation.		
Deliverables	Accountable	Responsible	Contributor
	<ul style="list-style-type: none">Information Security Policy	<ul style="list-style-type: none">Knowledge or Information BaseInformation Security Strategy	<ul style="list-style-type: none">Risk Management PolicyNew Solution and Critical Business Integration Proposal
Main task/s	<ul style="list-style-type: none">Define the information security strategy and standardsContribute to the development of the organisation’s security policyManages security auditsEvaluate risks, threats and consequencesEstablish and manage prevention, detection, correction and remediation plansInform and raise awareness among general management and across all IT users and professionalsConduct information security operations		
e-Competences (from e-CF)	A.7. Technology Trend Monitoring	Level 4	
	D.1. Information Security Strategy Development	Level 5	
	E.3. Risk Management	Level 4	
	E.8. Information Security Management	Level 4	
	E.9. IS Governance	Level 5	
KPI area	Security policy effectiveness		

EU
ICT

Chief ICT security officer

Description

Chief ICT security officers protect company and employee information against unauthorized access. They also define the Information System security policy, manage security deployment across all Information Systems and ensure the provision of information availability.

Essential skills and competences

- ensure adherence to organisational ICT standards
- ensure compliance with legal requirements
- ensure information privacy
- implement ICT risk management
- implement corporate governance
- lead disaster recovery exercises
- maintain plan for continuity of operations
- manage IT security compliances
- manage disaster recovery plans
- monitor technology trends
- utilise decision support system

Essential Knowledge

- ICT network security risks
- ICT security legislation
- ICT security standards
- audit techniques
- cyber security
- decision support systems
- information security strategy
- organisational resilience

Optional skills and competences

- coordinate technological activities
- create solutions to problems
- manage staff
- optimise choice of ICT solution
- train employees
- use different communication channels

ESCO



Work Role Name	Information Systems Security Manager	
Work Role ID	OV-MGT-001	
Specialty Area	Cybersecurity Management (MGT)	
Category	Oversee and Govern (OV)	
Work Role Description	Responsible for the cybersecurity of a program, organization, system, or enclave.	
Tasks	T0001, T0002, T0003, T0004, T0005, T0024, T0025, T0044, T0089, T0091, T0092, T0093, T0095, T0097, T0099, T0106, T0115, T0130, T0132, T0133, T0134, T0135, T0147, T0148, T0149, T0151, T0157, T0158, T0159, T0192, T0199, T0206, T0211, T0213, T0215, T0219, T0227, T0229, T0234, T0239, T0248, T0254, T0255, T0256, T0263, T0264, T0265, T0275, T0276, T0277, T0280, T0281, T0282	
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0018, K0021, K0026, K0033, K0038, K0040, K0042, K0043, K0046, K0048, K0053, K0054, K0058, K0059, K0061, K0070, K0072, K0076, K0077, K0087, K0090, K0092, K0101, K0106, K0121, K0126, K0149, K0150, K0151, K0163, K0167, K0168, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0267, K0287, K0332, K0342, K0622, K0624	
Skills	S0018, S0027, S0086	NICE: 1191 Knowledge, Skills and Abilities and 1006 Tasks
Abilities	A0128, A0161, A0170	



Analysis of the existing Cybersecurity Skills Certification Schemes.



Current gaps in Cybersecurity Skills Certification

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CERTIFIED INFORMATION SECURITY MANAGER	■						■	■	■					■						
CERTIFIED INFORMATION SYSTEMS AUDITOR														■						
CSX(F)																				
CSX(P)				■						■										
CYBERSECURITY AUDIT																				
CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL									■					■						
CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT									■											
CERTIFIED ETHICAL HACKER													■							
COMPUTER HACKING FORENSICS INVESTIGATOR																				
COMPTIA CYBERSECURITY ANALYST														■						
COMPTIA ADVANCED SECURITY PRACTITIONER				■	■				■	■	■				■					
COMPTIA SECURITY+	■			■	■		■	■	■	■										
COMPTIA PENTEST+				■	■															
COMPTIA NETWORK+		■	■	■	■				■											
OFFENSIVE SECURITY CERTIFIED PROFESSIONAL				■					■											
OFFENSIVE SECURITY WIRELESS PROFESSIONAL				■					■											
OFFENSIVE SECURITY CERTIFIED EXPERT				■	■				■											
OFFENSIVE SECURITY EXPLOIT EXPERT																				
OFFENSIVE SECURITY WEB EXPERT																				
CERTIFIED CLOUD SECURITY PROFESSIONAL			■																	
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL	■		■	■	■		■	■	■	■	■			■	■		■	■		
SYSTEMS SECURITY CERTIFIED PRACTITIONER	■			■	■		■	■	■	■										
CERTIFIED AUTHORIZATION PROFESSIONAL																				
CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL																				
HEALTHCARE INFORMATION SECURITY AND PRIVACY PRACTITIONER																				
EITCA/IS																				
CESG CERTIFIED PROFESSIONAL (CCP) SCHEME				■						■										

ICT SECURITY CONSULTANT






ALL SOURCE-COLLECTION REQUIREMENTS MANAGER
 CYBER CRIME INVESTIGATOR
 CYBER INSTRUCTIONAL CURRICULUM DEVELOPER
 CYBER INTEL PLANNER
 CYBER OPERATOR
 CYBER OPS PLANNER
 DATA ANALYST
 INFORMATION SYSTEMS SECURITY DEVELOPER
 LAW ENFORCEMENT /COUNTERINTELLIGENCE
 FORENSICS ANALYST
 MULTI-DISCIPLINED LANGUAGE ANALYST
 PARTNER INTEGRATION PLANNER
 PRODUCT SUPPORT MANAGER
 SECURITY ARCHITECT
 SOFTWARE DEVELOPER
 SYSTEMS DEVELOPER
 TARGET DEVELOPER
 TARGET NETWORK ANALYST
 THREAT/WARNING ANALYST

CONCORDIA Skills Certification Framework

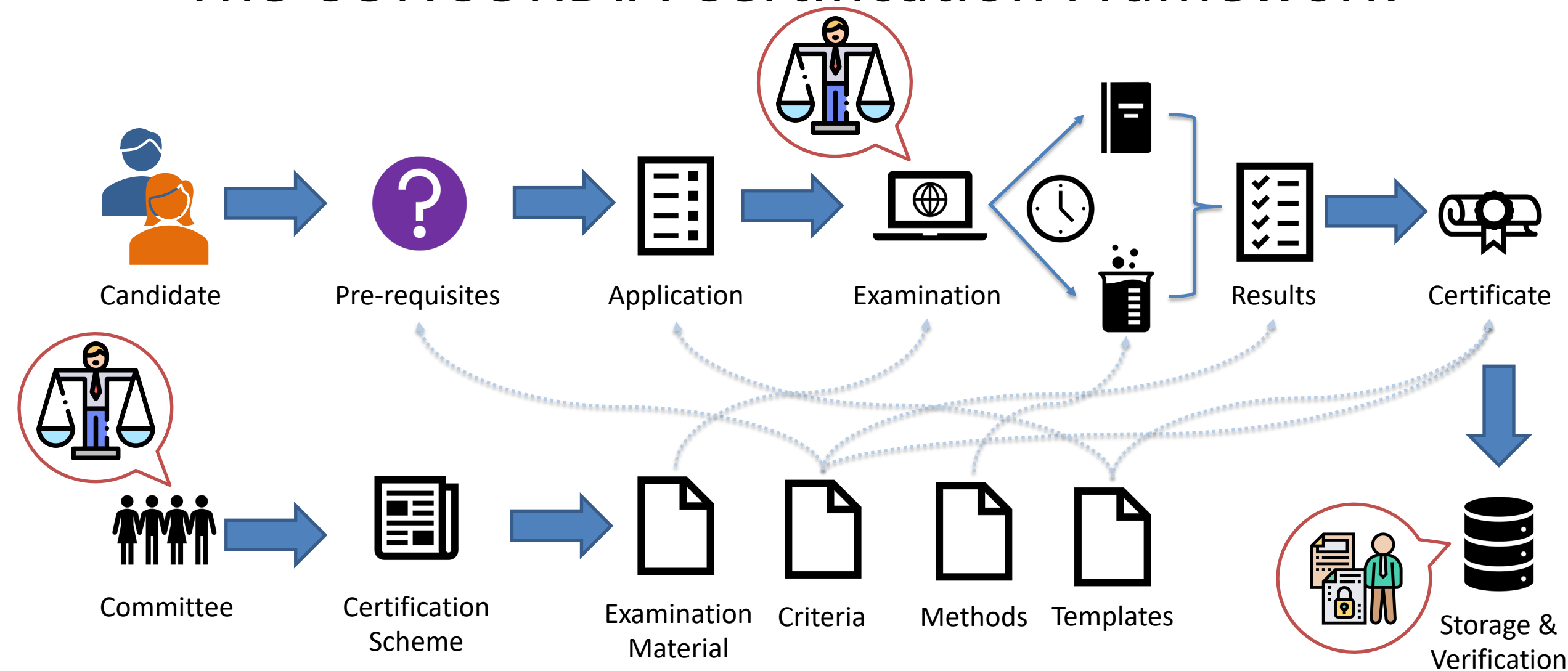
Principles

The overall purpose of certification of persons is to recognize an individual's competence to perform a task or job. It is the responsibility of the granting authority to ensure that only individuals who have demonstrated the relevant competence are awarded a certificate.

To provide the optimum value of certification the principles that need to be adhered are:

	<p>Impartiality</p>		<p>Competence</p>
	<p>Confidentiality and openness</p>		<p>Responsibility</p>
 <p>Responsiveness to complaints and appeals</p>			

The CONCORDIA Certification Framework





Examination Mechanism



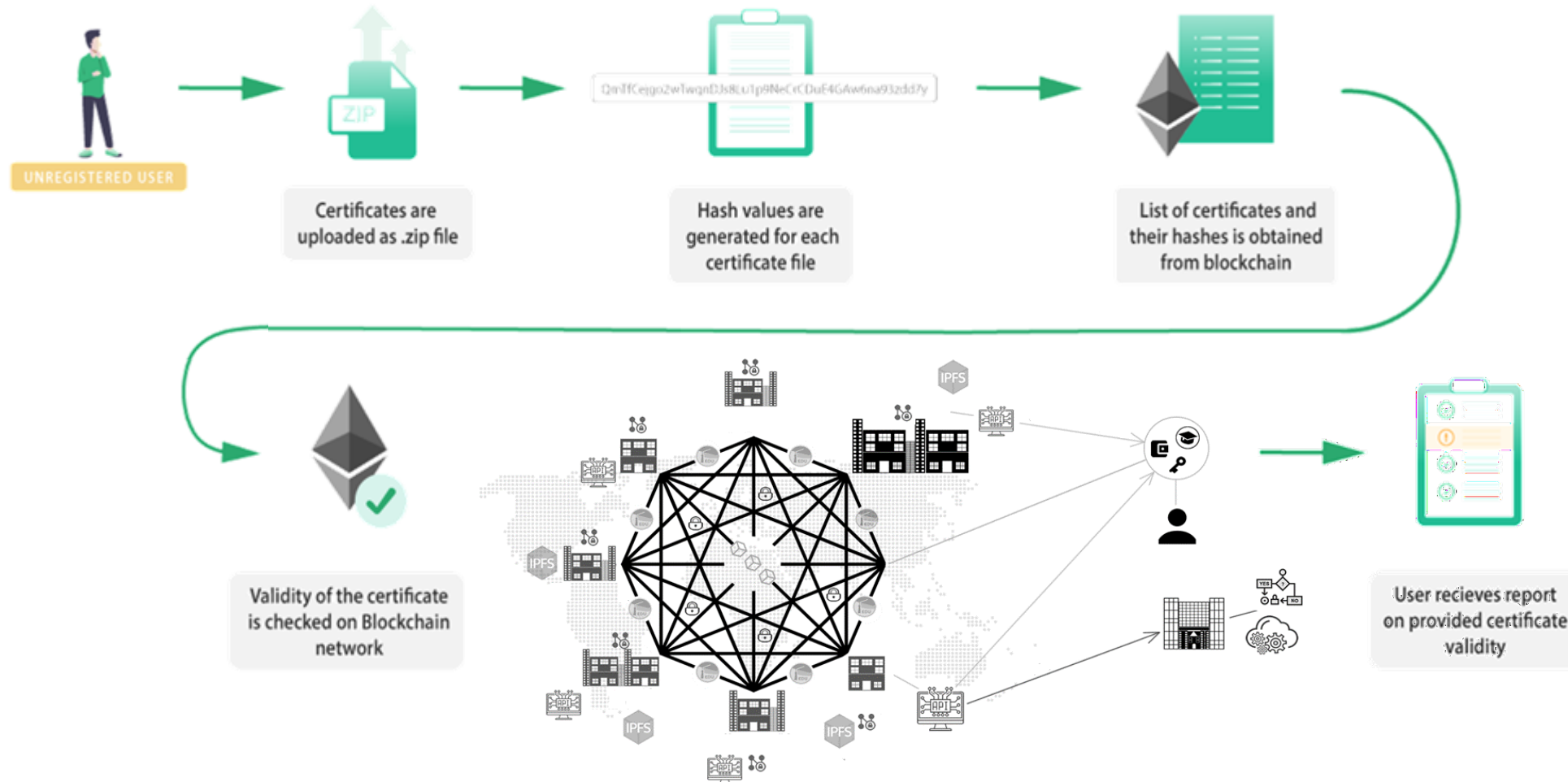
Theoretical examinations, will focus on the verification of the knowledge of the candidate regarding basic terms, definitions, rationale, tools, methods and theories. The existence of such knowledge is required as a basis before the practical part.



In the practical examinations, secure online (test) environments will be used in which subject-related matters can be simulated and where the chance of fraudulent acts by the students is kept to a minimum. [Usage of Cyberranges]



Blockchain as a tool



Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us



www.concordia-h2020.eu



www.twitter.com/concordiah2020



www.facebook.com/concordia.eu



www.linkedin.com/in/concordia-h2020

Thank You !
