`

ENERGY SHIELD

Integrated Cybersecurity Solution

for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

WP2 - VULNERABILITY ASSESSMENT & SECURITY BEHAVIOUR ANALYSIS

D2.2 – UPDATED SECURITY CULTURE FRAMEWORK AND TOOL

	Document info
Contractual delivery	**30/06/2020**
Actual delivery	**30/06/2020**
Responsible Beneficiary	**NTUA**

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

DOCUMENT INFO

Document ID:	D2.2
Version date:	26/06/2020
Total number of pages:	50
Abstract:	The aim of this deliverable is to present the underlying Security Culture Framework which shall allow automated planning and implementation of security culture programmes.
Keywords	cybersecurity culture, assessment, awareness, security behaviour

AUTHORS

Name	Organisation	Role
Spyros Mouzakitis	NTUA	Overall Editor
Anna Georgiadou	NTUA	Overall Editor
Michael Kontoulis	NTUA	Overall Editor
Kanaris Bounas	NTUA	Overall Editor

REVIEWERS

Name	Organisation	Role
Rosanna Babagiannou	KT	Overall Reviewer
Maria Atanasova	SC	QA Reviewer

VERSION HISTORY

0.1	13/05/2020	ToC
0.2	16/06/2020	First version
0.3	22/06/2020	Overall review comments version
0.4	23/06/2020	QA review ready version
0.5	26/06/2020	QA review comments version
1.0	30/06/2020	Final version, released to the EC

EXECUTIVE SUMMARY

The aim of this demonstration deliverable (D2.2) is to present the EnergyShield Security Culture Framework and Tool that aims to assess and map the socio-cultural behaviour of an organisation's workforce to cyberthreats. The tool is designed and implemented using a holistic approach to easily adapt and adjust to any business domain and, within the context of project, it is adapted to and will be validated by the EPES sector.

The main purpose of the cyber-security culture framework is to assess and evaluate the current security readiness of an organization's workforce. Having conducted a thorough review of the most commonly used security frameworks and pinpointed their gaps, weaknesses and overlaps, we have identified core security human related elements and classified them by constructing a domain agnostic security model. It consists of 10 different security dimensions analysed into 52 domains assessed by more than 500 controls examined under two different pillars: organisational and individual. Each of its components is being presented in detail while explaining how their quantification assists in achieving a feasible assessment methodology.

Both the assessment methodology and the underlying model are thereafter materialised via the development of a security culture evaluation tool. Respective tool focuses both on user friendliness and business effectiveness while clearly differentiating among the 3 distinctive security roles implemented: administrator, manager and user. Current version focuses on campaigns and self-assessments offering advanced graphical visualisations.

This deliverable presents:

- The cyber-security culture model designed along with its main concepts: levels, dimensions and domains.
- The evaluation methodology developed based on the suggested security culture model
- The architecture of the implementation tool and its underlying technologies
- The structure of the security evaluation tool in accordance with the corresponding assessment methodology

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
List of figures 5
List of tables 6
Acronyms 7
1. Introduction 8
1.1. Scope and objectives 8
1.2. Structure of the report 8
1.3. Task dependencies 8
2. Cyber Security Culture Framework 10
2.1. Model 11
2.1.1. Levels 13
2.1.2. Dimensions 13
2.1.3. Domains 15
2.2. Methodology 26
2.2.1. Methodology Usage Scenario 28
2.3. Tool 28
2.3.1. Architecture 28
2.3.2. Main Concepts 29
2.3.3. Structure 30
3. Conclusion and Next Steps 48
References 49

LIST OF FIGURES

Figure 1. EnergyShield Cyber-Security Culture Model: Main Concepts 11
Figure 2. Cyber-Security Culture Model: Levels & Dimensions 13
Figure 3. Domains consisting “Assets” dimension 16
Figure 4. Domains consisting “Continuity” dimension 17
Figure 5. Domains consisting “Access and Trust” dimension 18
Figure 6. Domains consisting “Operations” dimension 20
Figure 7. Domains consisting “Defence” dimension 21
Figure 8. Domains consisting “Security Governance” dimension 22
Figure 9. Domains consisting “Attitude” dimension 23
Figure 10. Domains consisting “Awareness” dimension 24
Figure 11. Domains consisting “Behaviour” dimension 25
Figure 12. Domains consisting “Competency” dimension 26
Figure 13. Security culture evaluation methodology 27
Figure 14. Security Behaviour Analysis tool architecture 29
Figure 15. Sign-in view 30
Figure 16. Console layout 31
Figure 17. Dashboard view 33
Figure 18. Users view 34
Figure 19. User profile view 35
Figure 20. Sign-up view 36
Figure 21. Create new user wizard 37
Figure 22. Groups view 38
Figure 23. Group details view 39
Figure 24. Create new group wizard 40
Figure 25. Reports view 41
Figure 26. Self-evaluations view 42
Figure 27. Execute new assessment view 43
Figure 28. Campaigns view 43
Figure 29. Campaign details view 44
Figure 30. Create new campaign view 45
Figure 31. Campaign assignment execution 46
Figure 32. Questionnaires view 47
Figure 33. Questionnaire details view 47

LIST OF TABLES

Table 1. Cyber-Security Culture Model 11
Table 2. Organisational dimensions 14
Table 3. Individual dimensions 15
Table 4. Domains consisting “Assets” dimension 16
Table 5. Domains consisting “Continuity” dimension 18
Table 6. Domains consisting “Access and Trust” dimension 19
Table 7. Domains consisting “Operations” dimension 20
Table 8. Domains consisting “Defence” dimension 21
Table 9. Domains consisting “Security Governance” dimension 22
Table 10. Domains consisting “Attitude” dimension 23
Table 11. Domains consisting “Awareness” dimension 24
Table 12. Domains consisting “Behaviour” dimension 25
Table 13. Domains consisting “Competency” dimension 26

ACRONYMS

ACRONYM	DESCRIPTION
DoA	Description of Action
EPES	
SBAM	Security Behaviour Analysis Module

1. INTRODUCTION

1.1. SCOPE AND OBJECTIVES

The scope of this demonstration deliverable (D2.2) is to present the EnergyShield Security Culture Framework and Tool that aims to assess and map the socio-cultural behaviour of an organisation's workforce to cyberthreats (Task 2.2). More specifically the objectives of this tool are:

- Perform the assessment of the Security Culture of an organization at different levels (organization, department units, and employees).
- Map the socio-cultural behaviour of end-users to specific cyber-threats.
- Provide insights for decision-making regarding improving the security culture of the company.
- Assist into planning and implementation of security culture training programs.

The results of the Security Culture tool assessments are further communicated to the EnergyShield Vulnerability Assessment tool through API, showing the effect of user's cyber awareness and skill in a holistic security context. The EnergyShield Security Culture framework will be integrated with the overall EnergyShield toolkit and further validated by the pilot users in the EPES sector.

1.2. STRUCTURE OF THE REPORT

This deliverable presents a cyber-security culture framework for evaluating the readiness an organization with emphasis on the aspects of the human factor. The aforementioned framework is being presented in a dedicated chapter divided into three sections:

- **First** section presents a holistic security culture model built upon security standards and frameworks, as well as a wide and diverse range of scientific studies related to cybersecurity behavioural analysis.
- **Second** section analyses the evaluation methodology used to assess the impact of each security factor represented in our model on the overall security culture readiness level.
- **Third** section focuses on the implemented security behavioural assessment tool presenting in detail its architecture, underlying technologies and provided user interfaces.

1.3. TASK DEPENDENCIES

This report presents the cyber-security culture framework as described in Task 2.2: *Map socio-cultural behaviour to cyberthreats and update the security culture tool to provide input to the vulnerability tool*, which is an essential module that interoperates with, the Vulnerability Assessment tool (Task 2.1: *Develop a threat model suitable to the EPES sector*). Moreover, it is aligned with the T1.1 (technical requirements) rolled-out in parallel with T1.2 (commercial requirements), T1.3 (regulatory requirements) and all the reports related to the landscape of

EnergyShield requirements. Lastly, this report is in alignment with the detailed architecture and technical specifications of the EnergyShield toolkit as documented in D1.4 *System architecture* (Task 1.4: *Design the overall system architecture*). The Security Culture Assessment tool will be integrated in the Energyshield Toolkit in the context of Task 5.1-Task 5.4 and further validated by the pilot users within WP6 tasks.

2. CYBER SECURITY CULTURE FRAMEWORK

Numerous cyber-security technological solutions, such as firewalls, antivirus software, intrusion detection systems, security operation centers and so on, are being adopted by the vast majority of the organisations in their effort to defend themselves against a tremendous variety of information security breaches. Individual phishing attacks leading to financial casualties; corporate network violations causing productivity losses; sensitive data exposure with major economical liabilities irreversibly damaging the reputation of an organisation [LAW11] are only a few examples of the contemporary digital hazards.

The scientific society focused on developing evaluation frameworks to assist corporations in assessing their security status while locating possible gaps and weaknesses. Yet, the vast majority of these frameworks don't dive deeper into what is considered by most the gravest security factor: **the human being**.

An organisation's biggest threat to privacy and security, even if not acknowledged, are their own staff [DOH05]. Employee security awareness is a key link to an organisation's security chain since even the most well-guarded corporation is defenceless with no security culture [RAN12, HOF00]. This term, "**security culture**", soon dominated in the area and has been attributed various definitions [WIL09]. All of them, more or less, agree that it "*exists when every participant in the information society, appropriately to their role, is aware of the relevant security risks and preventative measures, assumes responsibility and takes steps to improve the security of their information systems and networks*" [BUS04].

Security culture is cultivated via a long and time-consuming procedure affected by various factors with different weights. Different approaches and opinions have been put forward regarding its key elements and their assessment methodology. And, although, certain information security assessment techniques are established [SCA08], the same does not apply for the evaluation methods used by its corresponding culture.

This deliverable presents the EnergyShield security culture assessment framework to be adapted and used with the EPES sector. A model depicting the core **security culture levels, dimensions and domains** has been designed based on previously conducted scientific research while filling the gaps and inabilities among the different approaches. To intercept the cultural status of an organisation and, at the same time, pinpoint the neglected security regions the most widely used **assessment methods** have been used: testing, examination and interviewing [SCA08, RON09]. Our framework thereafter outlines linking the results of the assessment with valuable recommendations and practical ways of enforcing organisational and individual awareness, commitment and engagement towards cyber-security. Thus, through continuous assessment iterations, the ultimate goal is to diminish the human-related cyber-threats against an organisation.

2.1. MODEL

Having conducted a multidisciplinary research review and thoroughly studied several academic principles regarding information security, including technical analyses, algorithmic frameworks, mathematical models, statistical computations, behavioural, organisational and criminological theories, we have created a foundation combining the elements that constitute the critical cyber-security culture factors. Combining these different information security aspects, we have concluded in designing a globalised **model** attributing the cyber-security culture of an organisation via a hierarchical approach introducing the concepts of levels, dimensions, domains and controls as depicted in Figure 1.

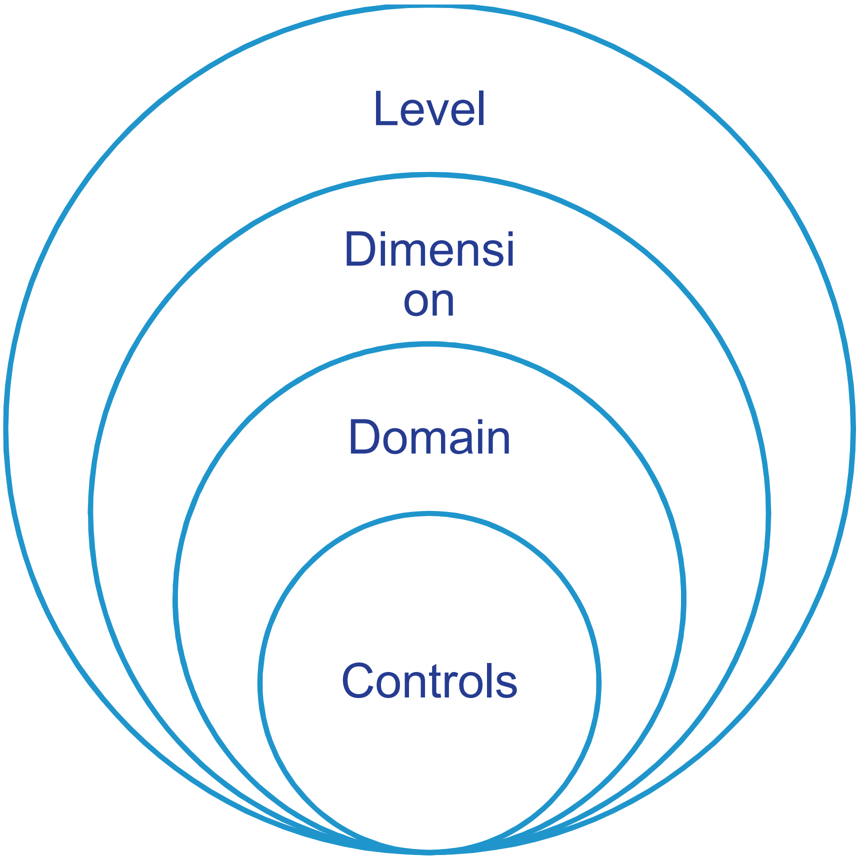


Figure 1. EnergyShield Cyber-Security Culture Model: Main Concepts

An overall presentation of the suggested model is contained in Table 1 whereas the remaining subsections analyse in detail each contributing element of our framework.

Table 1. Cyber-Security Culture Model

Organisational Level	Individual Level
Assets	**Attitude**
Application Software Security	Employee Climate
Data Security and Privacy	Employee Profiling
Hardware Assets Management	Employee Satisfaction
Hardware Configuration Management	**Awareness**
Information Resources Management	Policies and Procedures Awareness

Network Configuration Management	Roles and Responsibilities Awareness
Network Infrastructure Management	**Behaviour**
Software Assets Management	Policies and Procedures Compliance
Personnel Security	Security Agent Persona
Physical Safety and Security	Security Behaviour
Continuity	**Competency**
Backup Mechanisms	Employee Competency
Business Continuity & Disaster Recovery	Security Skills Evaluation
Capacity Management	Training Completion and Scoring
Change Management	
Continuous Vulnerability Management	
Access and Trust	
Access Management	
Account Management	
Communication	
External Environment Connections	
Password Robustness and Exposure	
Privileged Account Management	
Role Segregation	
Third-Party Relationships	
Wireless Access Management	
Operations	
Compliance Review	
Documentation Fulfilness	
Efficient Distinction of Development, Testing and Operational Environments	
Operating Procedures	
Organisational Culture and Top Management Support	
Risk Assessment	
Defence	
Boundary Defense	
Cryptography	
Email and Web Browser Resilience	
Information Security Policy and Compliance	
Malware Defense	
Security Awareness and Training Program	
Security Governance	
Audit Logs Management	
Incident Response and Management	
Penetration Tests and Red Team Exercises	
Reporting Mechanisms	
Security Management Maturity	

The suggested model applies to any size and kind of organisation regardless of its business domain, specialisation, technological status and security readiness. It can also be used by any operational structure demonstrating a definite distinction between a decision-making board and a production unit. It can be adjusted to any business field by calibrating metrics defined for each of its domains. Additionally, it can be expanded and updated with little effort to constantly keep pace with the continuously transforming business environment. New dimensions and domains can be introduced adjusting and broadening its application.

2.1.1. LEVELS

Our model clearly defines two levels:

1. **Organisational level** is meant to encompass all factors related to an organisation's security technological infrastructure, operations, policies and procedures.
2. **Individual level** is targeted on employee's attributes and characteristics with immediate impact on their security attitude and behaviour.

In other words, organisational level is meant to infiltrate all elements formulating the external environment, business, social, emotional, etc., inside of which individuals are expected to function, act, react and perform their daily working tasks. These external factors directly form the cyber-security corporate reality and indirectly affect the security performance, behaviour and attitude of the employees represented in the individual level of our model. This way the suggested model manages to combine both "external" human factors as well as "internal" driven individual notions attributing in full the cyber-security culture of an organisation.

2.1.2. DIMENSIONS

Each level is then broken down into different **dimensions,** as presented graphically in Figure 2.

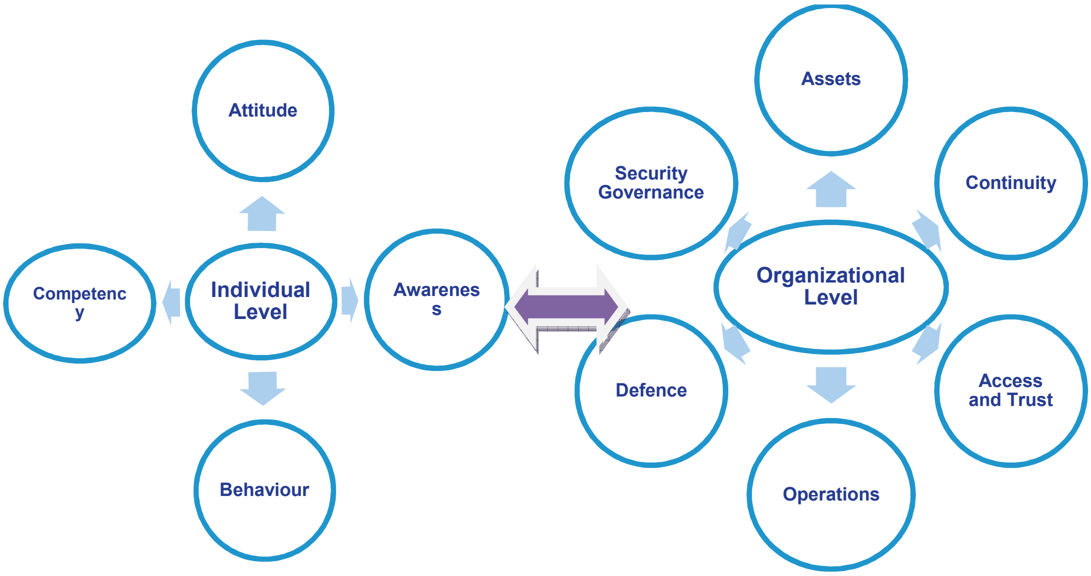


Figure 2. Cyber-Security Culture Model: Levels & Dimensions

Organisational level is divided into dimensions that include the designment, development, documentation and implementation of security policies and procedures that aim different business domains. Organisational dimensions are being presented in Table 2.

Table 2. Organisational dimensions

Dimension	Definition
Assets	This dimension includes the designment, development, documentation and implementation of security policies and procedures that aim to protect an organisation's assets (including people, buildings, machines, systems and information assets) by enforcing several levels of confidentiality, availability, and integrity controls.
Continuity	This dimension includes the planning, development, documentation and implementation of security policies and procedures that aim to ensure operations, services and production continuity for an organisation at predefined levels while safeguarding the reputation and interests of key stakeholders in cases of disruptive incidents.
Access and Trust	This dimension includes the designment, development, documentation and implementation of business processes, policies and procedures that aim to ensure appropriate access to resources across the organisation while clarifying different roles and permissions. In addition, it delimits any interactions the organisation has with third-party factors, such as suppliers, customers, authorities, etc.
Operations	This dimension refers to the administration of business practices to create the highest level of efficiency possible within an organisation while taking into account the security aspects that safeguard its final results.
Defence	This dimension focuses on the foresight to have planned, acquired and properly configured all technical assets necessary for the improvement and efficient operation of its information security.
Security Governance	This dimension includes the designment, development, documentation and implementation of policies so as to effectively plan, manage and improve organisation's information security.

On the other hand, individual level is consisted of dimensions that attribute human characteristics, approaches and performances towards cyber-security. Individual dimensions are being presented in detail in Table 3.

Table 3. Individual dimensions

Dimension	Definition
Attitude	This dimension refers to the feelings and beliefs employees have toward security protocols and issues.
Awareness	This dimension refers to the employees' understanding, knowledge and awareness of security issues and activities.
Behaviour	This dimension refers to the actions and activities of employees that have direct or indirect impact on the security of the organisation.
Competency	This dimension refers to the employees' abilities, skills, knowledge and expertise that enable them to conform with the security policies and procedures of the organisation.

2.1.3. DOMAINS

Each dimension is in turn analysed into **domains** with distinctive application areas and quantifiable indicators. Each domain is then broken down to a number of controls that vary from simple yes/no, likert scale or multiple questions to quantitative and qualitative ones. Each control bears different weight to the domain assessment result so as to attribute the different importance and, thus, impact specific factor has in the overall security culture formation.

Controls are being evaluated using different techniques depending on their nature and significance:

1. Questionnaires, widely used for the organisational level domain controls, remain brief, easy-to-understand and targeted to facilitate interviewees.
2. Simulations cover a wide range of artifacts such as phishing emails, social media fraud techniques, workstation virus contamination and so on.
3. Tests varying from real-time user-targeted ones, such as password robustness, email exposure, ransomware resilience, and extended organisational-aimed ones, such as domain spoofing, mail server resistance and various others.
4. Serious games are being used not only as a more reliable evaluation method but also due to their instructive nature and impressive effectiveness results.
5. Simple observation, reporting from different sources and cross-analysis of the collected information is also invoked.

Following sections present in detail each one of the dimensions presented previously analysing them into specific domains as currently identified.

2.1.3.1. ASSETS

This dimension includes the designment, development, documentation and implementation of security policies and procedures that aim to protect an organisation's assets (including people, buildings, machines, systems and information assets) by enforcing several levels of confidentiality, availability, and integrity controls.

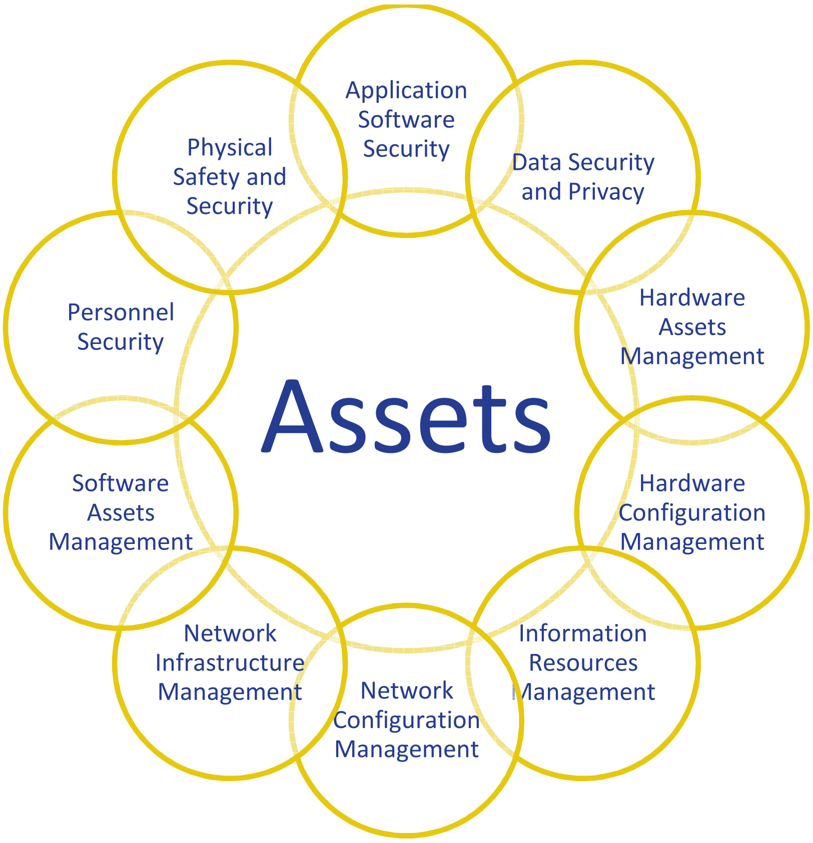

Assets
Application Software Security
Data Security and Privacy
Hardware Assets Management
Hardware Configuration Management
Information Resources Management
Network Configuration Management
Network Infrastructure Management
Software Assets Management
Personnel Security
Physical Safety and Security

Figure 3. Domains consisting "Assets" dimension

Table 4 presents in detail the domains consisting the "Assets" dimension.

Table 4. Domains consisting "Assets" dimension

Dimension	Definition
Application Software Security	Management of the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
Data Security and Privacy	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
Hardware Assets Management	Active documentation, inventory and management of all hardware devices (laptops, removable media, datacenters, etc.) or physical assets (hard copies of documents such as policies, records, contracts, etc.) so that effective protection is assured.
Hardware Configuration Management	Establishment, implementation, and active management of the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
Information Resources Management	Classification of all assets and information depending on their criticality, confidentiality and business value.

Network Configuration Management	Establishment, implementation, and active management of the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
Network Infrastructure Management	Management of the ongoing operational use of ports, protocols, and services on networked devices in order to minimise windows of vulnerability available to attackers.
Software Assets Management	Active documentation, inventory and management of all corporate software so that effective protection of them is ensured.
Personnel Security	Management of the proper authentication and authorisation level controlling personnel and/or visitors' access in the physical facilities of the organisation.
Physical Safety and Security	Establishment, implementation, and active management of facilities' physical security.

2.1.3.2. CONTINUITY

This dimension includes the planning, development, documentation and implementation of security policies and procedures that aim to ensure operations, services and production continuity for an organisation at predefined levels while safeguarding the reputation and interests of key stakeholders in cases of disruptive incidents.

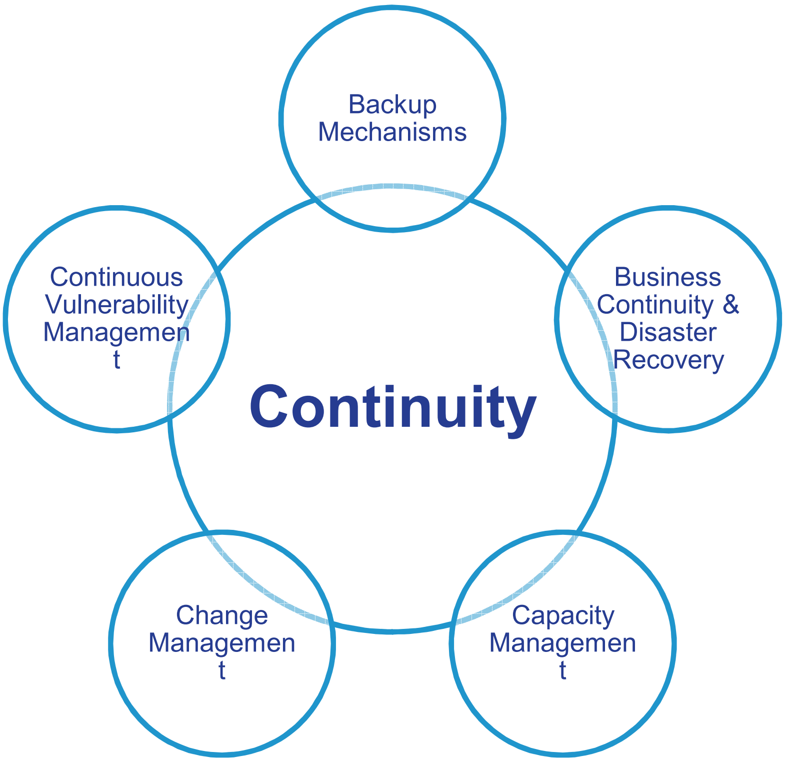

Backup Mechanisms
Continuous Vulnerability Managemen t
Business Continuity & Disaster Recovery
Continuity
Change Managemen t
Capacity Managemen t

Figure 4. Domains consisting "Continuity" dimension

Table 5 presents in detail the domains consisting the “Continuity” dimension.

Table 5. Domains consisting “Continuity” dimension

Dimension	Definition
Backup Mechanisms	The backup procedures that are in place in order to avoid loss of critical information and provide a level of acceptable business continuity in case of incidents.
Business Continuity & Disaster Recovery	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
Capacity Management	The procedures with which the organisation can ensure that information technology resources are right-sized to meet current and future business requirements in a cost-effective manner.
Change Management	The procedures used for the management of any changes in the organisation.
Continuous Vulnerability Management	Continuous acquisition, assessment, and elaboration on new information in order to identify vulnerabilities, remediate, and minimise the opportunity window for attackers.

2.1.3.3. ACCESS AND TRUST

This dimension includes the designment, development, documentation and implementation of business processes, policies and procedures that aim to ensure appropriate access to resources across the organisation while clarifying different roles and permissions. In addition, it delimits any interactions the organisation has with third-party factors, such as suppliers, customers, authorities, etc.

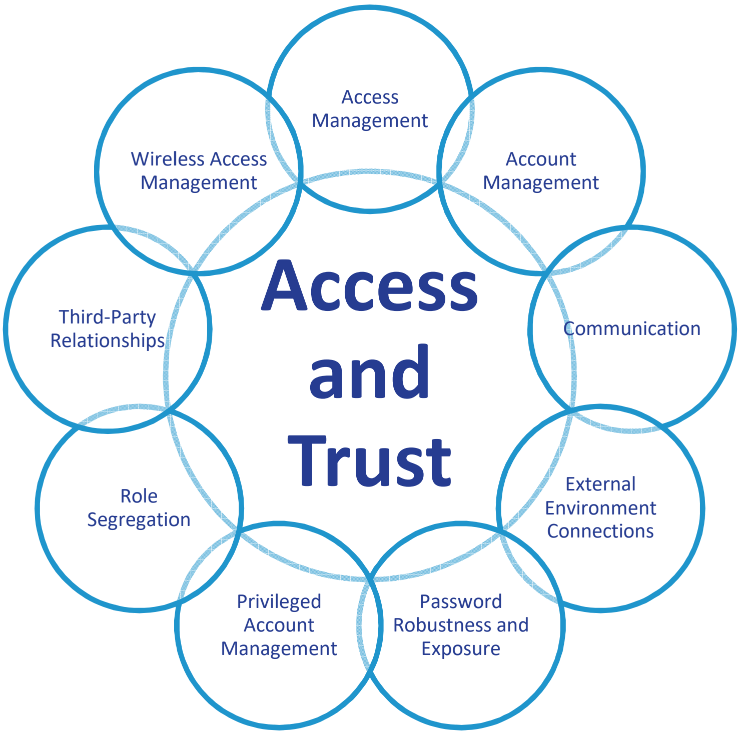

Access and Trust
Access Management
Account Management
Communication
External Environment Connections
Password Robustness and Exposure
Privileged Account Management
Role Segregation
Third-Party Relationships
Wireless Access Management

Figure 5. Domains consisting “Access and Trust” dimension

Table 6 presents in detail the domains consisting the “Access and Trust” dimension.

Table 6. Domains consisting “Access and Trust” dimension

Dimension	Definition
Access Management	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
Account Management	Active management of the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimise opportunities for attackers to leverage them.
Communication	Various controls aiming to protect data, information and systems during communication procedures.
External Environment Connections	Establishment and active management of the external environment connections of the organisation.
Password Robustness and Exposure	The measures taken by the organisation to ensure all passwords used are secure enough along with the policies developed to ensure the passwords confidentiality.
Privileged Account Management	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
Role Segregation	The proper appointment of roles and responsibilities ensuring their segregation in various processes and procedures, so as to avoid possible issues such as conflict of interests.
Third-Party Relationships	Determination of the necessary requirements a third party should have to be considered trusty, along with the implementation of the necessary procedures with which those requirements are fulfilled. Also includes the procedures used by the organisation in order to get in contact with relevant authorities when needed and the contacts maintained with various special groups, that may help it improve its information security
Wireless Access Management	The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

2.1.3.4. OPERATIONS

This dimension refers to the administration of business practices to create the highest level of efficiency possible within an organisation while taking into account the security aspects that safeguard its final results.

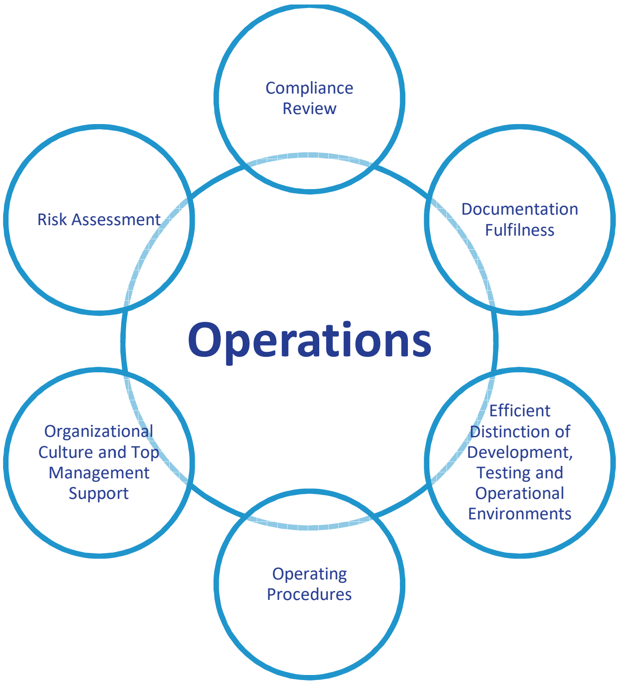

Compliance Review
Documentation Fulfilness
Efficient Distinction of Development, Testing and Operational Environments
Operating Procedures
Organizational Culture and Top Management Support
Risk Assessment
Operations

Figure 6. Domains consisting "Operations" dimension

Table 7 presents in detail the domains consisting the "Operations" dimension.

Table 7. Domains consisting "Operations" dimension

Dimension	Definition
Compliance Review	Various controls determining the security level appointed by security audit results.
Documentation Fulfillness	A checklist with all the necessary documentation an organisation is advised to have in order to maintain an appropriate level of information security.
Efficient Distinction of Development, Testing and Operational Environments	Proper segregation of the development, testing and operational environments.
Operating Procedures	Definition of operating procedures with focus on minimising the possibility of errors and malpractices.
Organisational Culture and Top Management Support	Identification, establishment, and active management of the organisational culture and top management support influencing and formatting the overall security culture of the organisation.
Risk Assessment	Conducting risk assessments in order to find any vulnerabilities in the organisation repeated at regular intervals or when significant changes occur.

2.1.3.5. DEFENCE

This dimension focuses on the foresight to have planned, acquired and properly configured all technical assets necessary for the improvement and efficient operation of its information security.

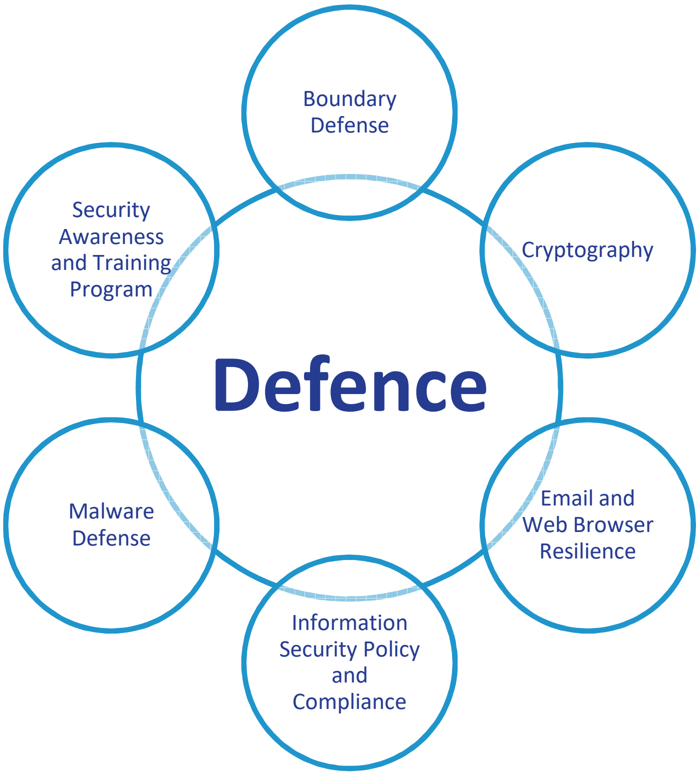

Boundary Defense
Cryptography
Email and Web Browser Resilience
Information Security Policy and Compliance
Malware Defense
Security Awareness and Training Program
Defence

Figure 7. Domains consisting "Defence" dimension

Table 8 presents in detail the domains consisting the "Defence" dimension.

Table 8. Domains consisting "Defence" dimension

Dimension	Definition
Boundary Defence	Detection/prevention/correction of the information flow transferring across networks of different trust levels with a focus on security-damaging data.
Cryptography	All of the cryptographic controls used by the organisation.
Email and Web Browser Resilience	Minimisation of the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.
Information Security Policy and Compliance	Establishment, implementation, and active management of information security policies and the compliance against them.
Malware Defence	Controls over the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defense, data gathering, and corrective action.
Security Awareness and Training	Targeting all functional roles in the organisation (prioritising those mission-critical to the business and its security).

Program	Identification of the specific knowledge, skills, and abilities needed to support defense of the enterprise; development and execution of an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programs.

2.1.3.6. SECURITY GOVERNANCE

This dimension includes the designment, development, documentation and implementation of policies so as to effectively plan, manage and improve organisation's information security.

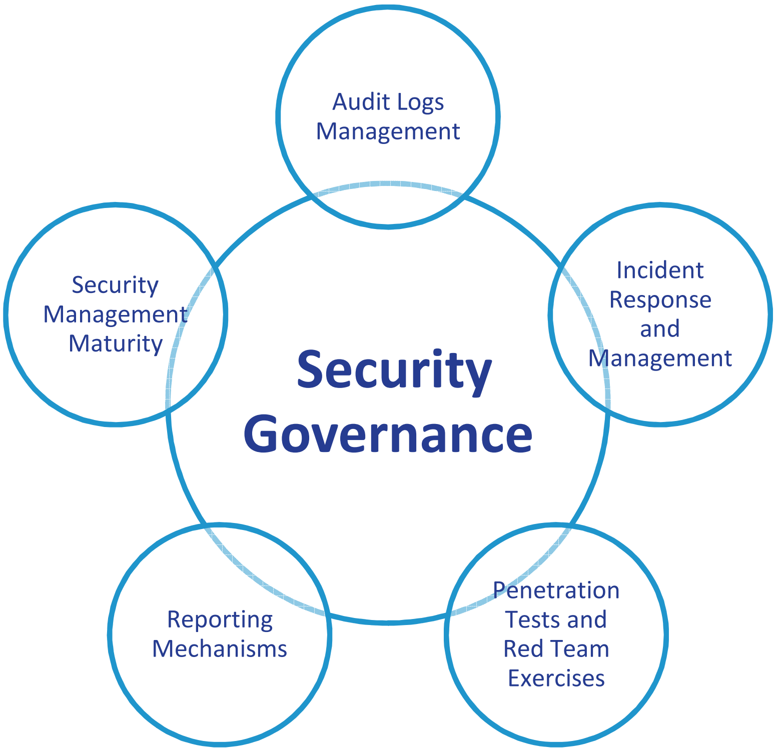

Audit Logs Management
Incident Response and Management
Security Governance
Security Management Maturity
Reporting Mechanisms
Penetration Tests and Red Team Exercises

Figure 8. Domains consisting "Security Governance" dimension

Table 9 presents in detail the domains consisting the "Security Governance" dimension.

Table 9. Domains consisting "Security Governance" dimension

Dimension	Definition
Audit Logs Management	Collection, management, and analysis of event logs that could assist in detecting, understanding, or recovering from attacks.
Incident Response and Management	Protection of the organisation's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight).
Penetration Tests	Testing the overall strength of an organisation's defense (the

and Red Team Exercises	technology, the processes, and the people) by simulating the objectives and actions of an attacker.
Reporting Mechanisms	The channels used by the organisation in order for employees or other relevant parties to report vulnerabilities or incidents detected.
Security Management Maturity	Evaluate the security management maturity of an organisation.

2.1.3.7. ATTITUDE

This dimension refers to the feelings and beliefs employees have toward security protocols and issues.

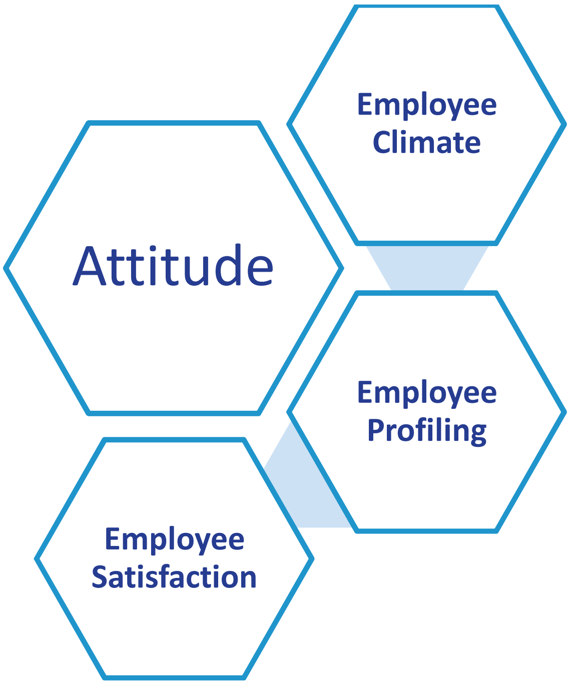


Figure 9. Domains consisting "Attitude" dimension

Table 10 presents in detail the domains consisting the "Attitude" dimension.

Table 10. Domains consisting "Attitude" dimension

Dimension	Definition
Employee Climate	The assessment of the satisfaction each employee has towards information security, directly affecting his/her security behavior.
Employee Profiling	A generic employee profile that shall assist in identifying possible security behavioral patterns.
Employee Satisfaction	The assessment of the satisfaction each employee has towards both the organisation and other colleagues directly affecting his/ her security behavior.

2.1.3.8. AWARENESS

This dimension refers to the employees' understanding, knowledge and awareness of security issues and activities.

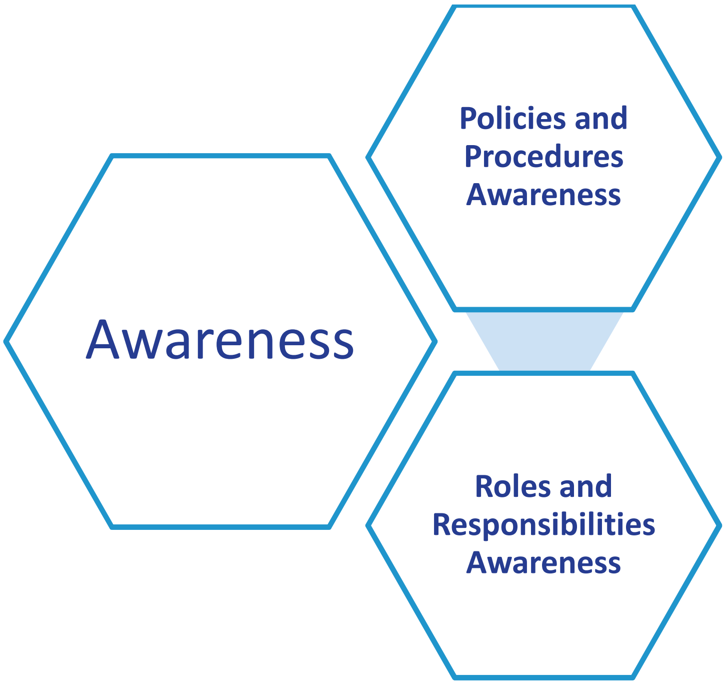

Awareness
Policies and Procedures Awareness
Roles and Responsibilities Awareness

Figure 10. Domains consisting "Awareness" dimension

Table 11 presents in detail the domains consisting the "Awareness" dimension.

Table 11. Domains consisting "Awareness" dimension

Dimension	Definition
Policies and Procedures Awareness	Assessment of the cognition each employee has regarding the organisation's security policies and procedures.
Roles and Responsibilities Awareness	Assessment of the cognition each employee has regarding his role and responsibilities related to information security.

2.1.3.9. BEHAVIOUR

This dimension refers to the actions and activities of employees that have direct or indirect impact on the security of the organisation.

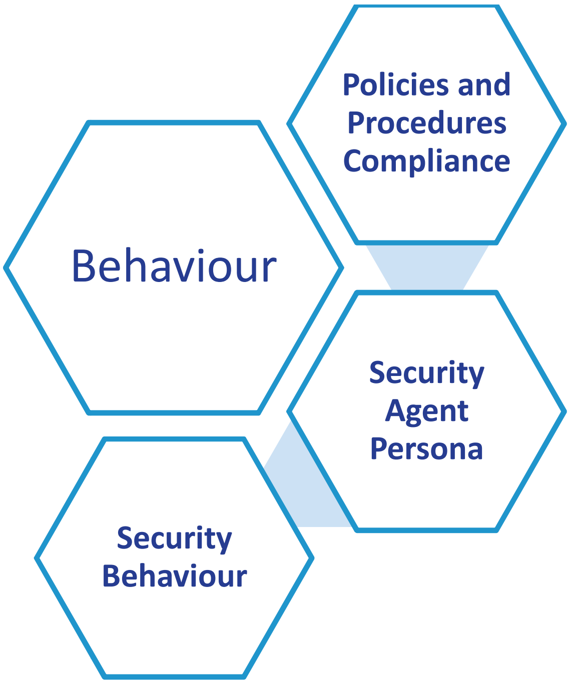


Figure 11. Domains consisting “Behaviour” dimension

Table 12 presents in detail the domains consisting the “Behaviour” dimension.

Table 12. Domains consisting “Behaviour” dimension

Dimension	Definition
Policies and Procedures Compliance	Controlling and logging any security policies and procedures incompliances or violations by employees or other affected parties.
Security Agent Persona	Identification of the kind of security-conscious behaviour individuals tend to exhibit on a day-to-day basis in their workplace.
Security Behaviour	Security-conscious behaviour exhibited on a day-to-day basis in the workplace.

2.1.3.10. COMPETENCY

This dimension refers to the employees’ abilities, skills, knowledge and expertise that enable them to conform with the security policies and procedures of the organisation.

Competency
Employee Competency
Security Skills Evaluation
Training Completion and Scoring

Figure 12. Domains consisting "Competency" dimension

Table 13 presents in detail the domains consisting the "Competency" dimension.

Table 13. Domains consisting "Competency" dimension

Dimension	Definition
Employee Competency	The identification and definition of the competency needed for each role and responsibility. Also, the documentation of the proof of competency of each employee.
Security Skills Evaluation	Measurement/Evaluation of the security skills, familiarity, awareness, etc.
Training Completion and Scoring	Record of any training programs attended by individuals along with scoring, completeness rate and assessment of their effectiveness.

2.2. METHODOLOGY

The proposed model represents the key security metrics to be measured along with their dependencies, influences and varieties. The next step was to define an evaluation methodology that not only enables an organisation to illustrate a uniform representation of its everyday reality but also assists in identifying its vulnerabilities and weaknesses. Knowledge based on figures and numbers is a powerful decision-making asset.

As depicted in Figure 13, the evaluation methodology consists of clearly defined and easily comprehendible steps. Starting from the decision of performing a security assessment process either due to an organisation board's initiative or (which is usually the case) driven by the need to defend against the numerous cyberthreats of current reality (possibly after an unexpected real-life incident). The decision-making group should set the initial goals and provide proper business requirements before the initiation of the evaluation procedure. Depending on their expectations, the entire methodology shall be respectively targeted in means of groups and security domains.

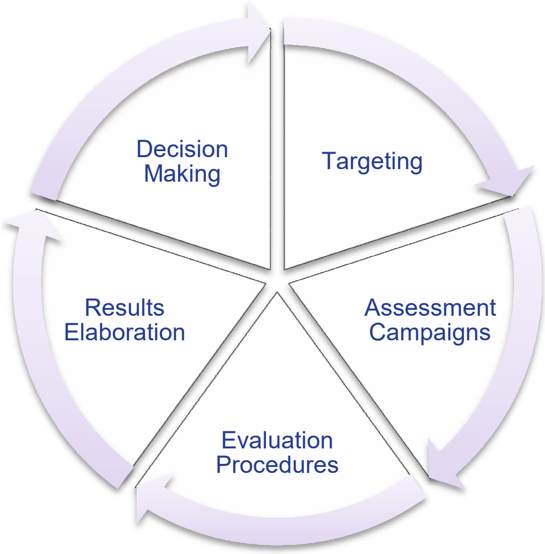


Figure 13. Security culture evaluation methodology

In the next step, evaluation iterations, so called **assessment campaigns**, are being planned by managers and team leaders with proper variations among the different user groups, teams or even organisation sections and departments. Bearing in mind the targeting results of the previous step, they calibrate and, carefully and collaboratively, design the **evaluation procedure** which takes place in the next step. Using proven techniques, such as testing, examination, interviewing [SCA08, RON09], simulation, gamification and many others [ABA14], gather as much information as possible from its participants.

Reaching to the most demanding step of the methodology, results are being gathered and analysed via a series of weighting algorithms and statistical computations generating a number of graphical representations and reports at an individual as well as organisational level. Using the score generated by the evaluation procedure for each targeted **individual** (analysed into the different dimensions and domains), the methodology proceeds in appropriately aggregating them along with the **organisational** related ones producing corresponding scores for sections, departments, units and ultimately for the organisation as a whole.

Finally, acquired results pinpoint the existing security weaknesses and gaps allowing security training programs' personalisation and adaptation to user specific needs. Suggestions and recommendations are being provided both to individuals and directors while decision-making board is armed with the knowledge of their security culture status along with its pain points.

2.2.1. METHODOLOGY USAGE SCENARIO

An indicative simplified scenario to serve as an example of all of the above would be as follows. The security officers of company X have been alerted by the security operation center (SOC) solution at hand that an excessive number of fraud emails are reaching their marketing department. After further investigating, have also verified a misuse of social channels from its employees. Consequently, they have reached the decision to run an assessment campaign targeting this specific department. Since their focus lies on the email, web and social media usage, they include to their campaign a number of relative questionnaires, phishing simulation tests, social engineering games and email and password exposure checks. After the expiration date of the campaign, the security officers gather the results and via a graphical representation are able to understand both the security vulnerabilities they are up against as well as their magnitude. Would the users accept and activate a virus received as an attachment via an email? Would someone reply to a phishing email providing important personal or corporate information? Do they understand the dangers they are up against by the exposure they have as members of the marketing department (email addresses available to the public)? Do they conform with the password policies of the company? Knowing where more employees failed to live up to the expectations, they can proceed in building their defense and calibrating existing technological assets to protect them and, more importantly, educate them and arm them against the cyber-threats they face. Not to mention that, via the evaluation process, they have already triggered them and initiated a security cultural zymosis.

2.3. TOOL

2.3.1. ARCHITECTURE

Security Behaviour Analysis tool has been designed, developed and implemented as a web application using a number of cut-edge technologies as presented in an overall architecture design in Figure 14. More specifically:

- ***Django***: a high-level open source Python Web framework that encourages rapid development while offering the ability to quickly and flexibly scale. Its security features enforce applications' protection against common security issues, such as SQL injection, cross-site scripting, cross-site request forgery and clickjacking.
- ***PostgreSQL***: a powerful, open source object-relational database system with strong reputation for reliability, feature robustness, and performance. It is used to host the logical data structure behind the entire application including the security culture model and the representation of the evaluation methodology along with its results and statistics.
- ***Web interface***: implemented using a combination of HTML, Bootstrap, CSS and JavaScript files to provide a user-friendly interface for all interacting actors of the tool.

- ***REST API***: a web interface allowing interaction of the Security Behaviour Analysis tool with the rest of the EnergyShield toolkit or with any other corporate operational system.

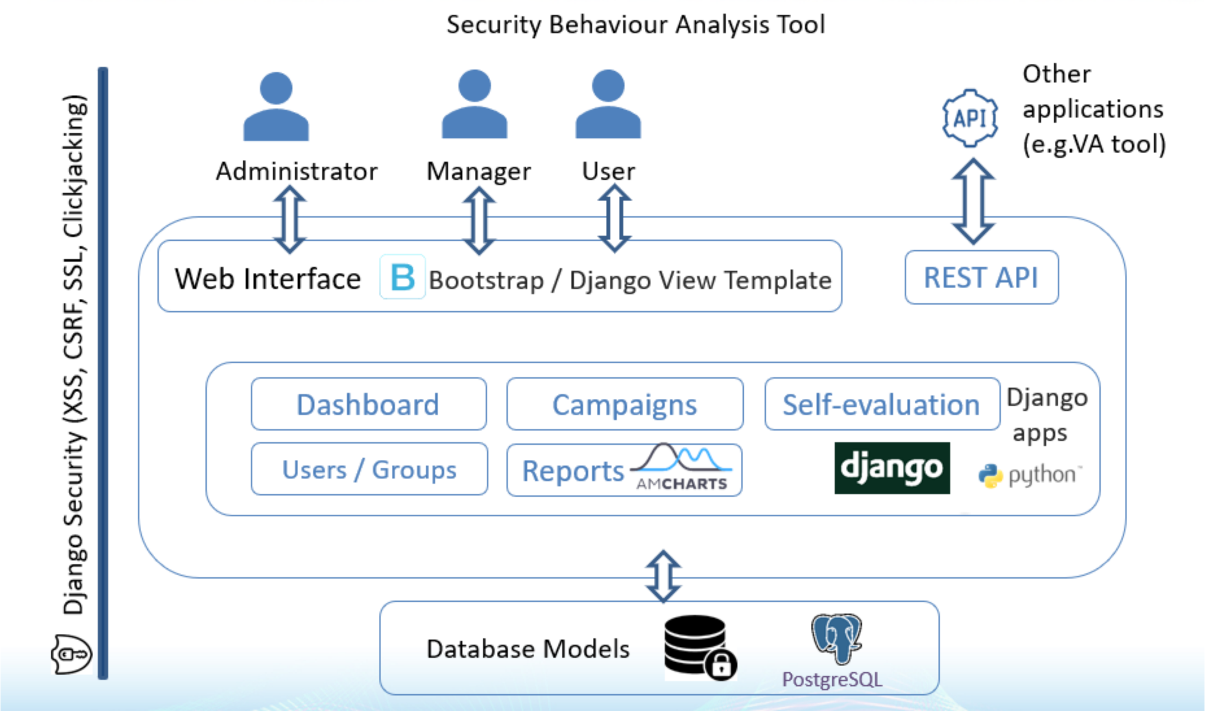


Figure 14. Security Behaviour Analysis tool architecture

Source code is being hosted on NTUA's gitlab environment.

2.3.2. MAIN CONCEPTS

Based on the security culture framework and evaluation procedure presented in detail in previous sections, there is a firm distinction among three different business user roles:

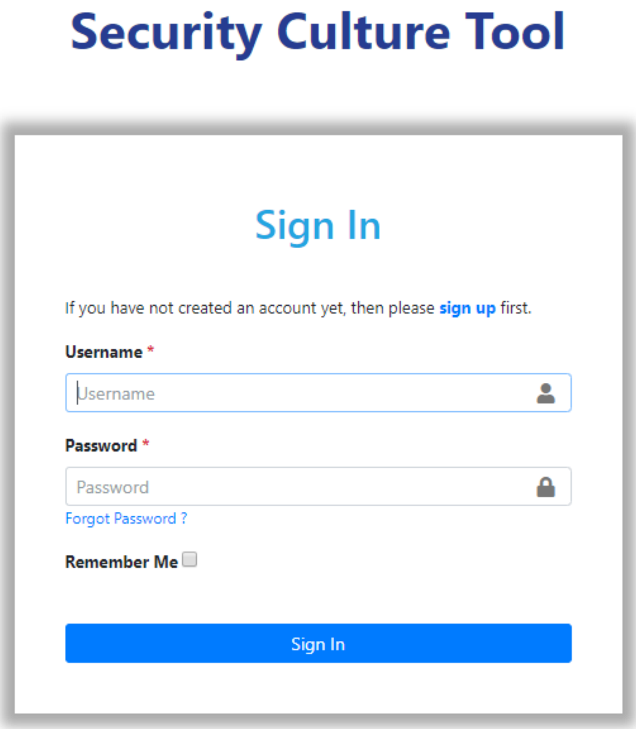
- ***Administrator*** (superuser privileges): usually a system administrator or security officer with full privileges over the security culture assessment life-cycle of the organisation and, therefore, of the SBAM tool. He/she is responsible for user management, global groups and campaigns creation and management.
- ***Manager***: any user which acts as a leader of an employee group and is responsible for their security assessment, evaluation and training. He/she is granted manager privileges within the SBAM tool allowing them to create new users (practically inviting them to access the tool), groups, campaigns (accessible only to themselves apart from the administrators) and monitor their status and progress by obtaining a number of graphical reports.
- ***User***: simple user able to participate to campaigns or perform a number of self-assessment iterations in order to evaluate their security culture status and sharpen their information security knowledge, familiarity and awareness.

Corresponding roles have been implemented in the SBAM tool offering customisation and personalisation of the security assessment experience. Other important security concepts presented within the tool are the following:

- ***Campaign***: a security culture assessment iteration designed by a manager targeting specific security domains and user groups or individuals. It has a certain duration (start and end date) and results in a number of assignments to participating employees with determined expiration. It provides a snapshot of the security culture status of a part of the organization giving useful insights and feedback to decision-makers.
- ***Self-assessment***: an interactive way of self-evaluating your security awareness, compliance and readiness while improving your security knowledge and culture. Via multiple repetitions, it can also be considered as a means of self-training both to the security policies and procedures of the organisation and on the various information security threats and current reality.

2.3.3. STRUCTURE

Security Culture Tool is a web-based application. To access the tool services, users need to first sign in (Figure 15).



Security Culture Tool

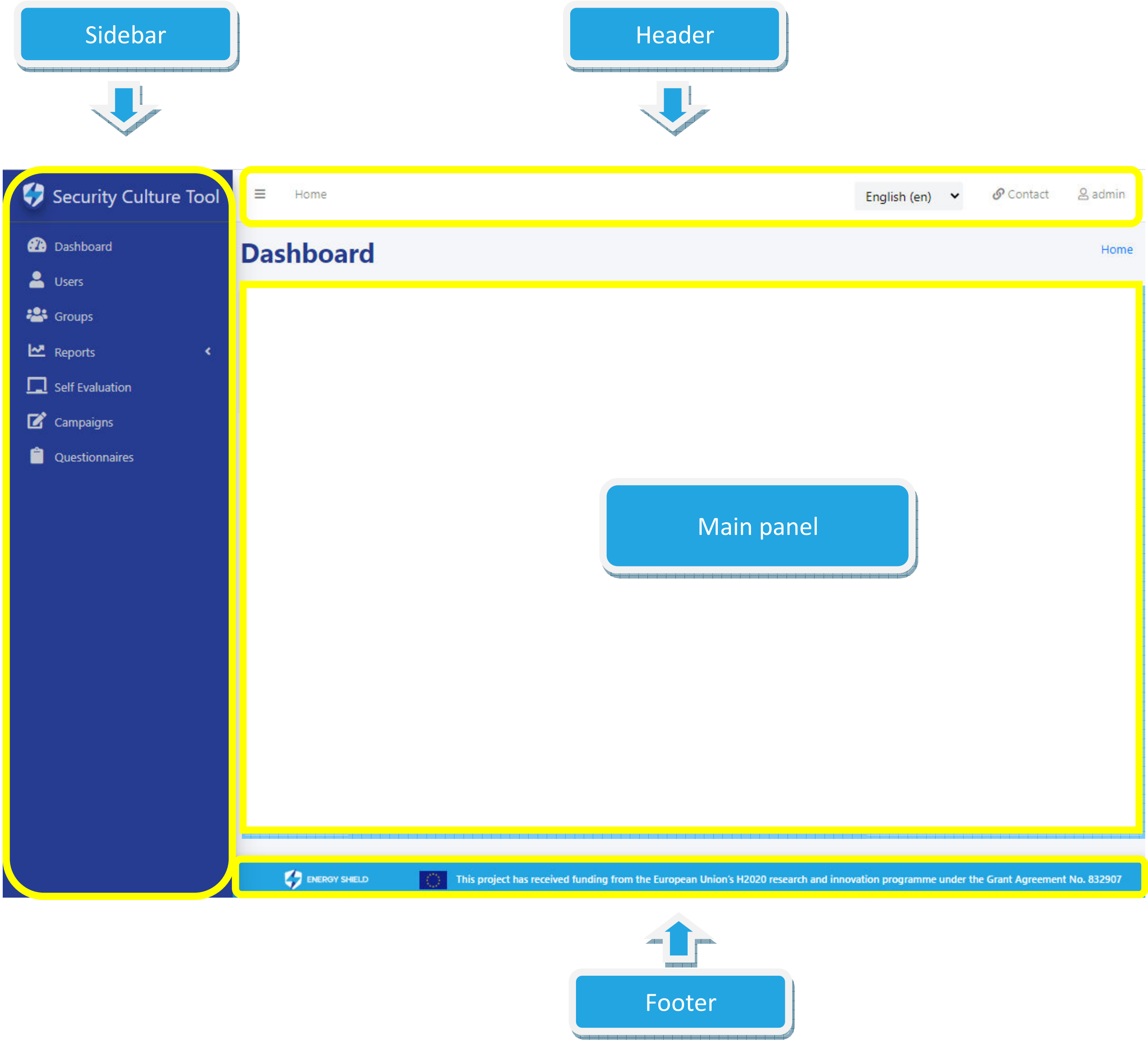
Sign In

If you have not created an account yet, then please **sign up** first.

Figure 15. Sign-in view

Proving valid credentials, leads the user to a personalized home page which defers depending on user role and privileges. The security culture tool console is divided into 4 main parts (Figure 16):

- ***Header***: offers localization possibilities via the “select language” menu, project contact information and a user submenu offering access to profile, change password and sign-out options.
- ***Sidebar***: offers access to different views of the tool (user role and privilege dependent).
- ***Footer***: contains project related information and a connection to project’s official website.
- ***Main panel***: is the main presentation part of the tool.



This project has received funding from the European Union’s H2020 research and innovation programme under the Grant Agreement No. 832907

Figure 16. Console layout

Depending on user role and privileges, sidebar offers a number of different options:

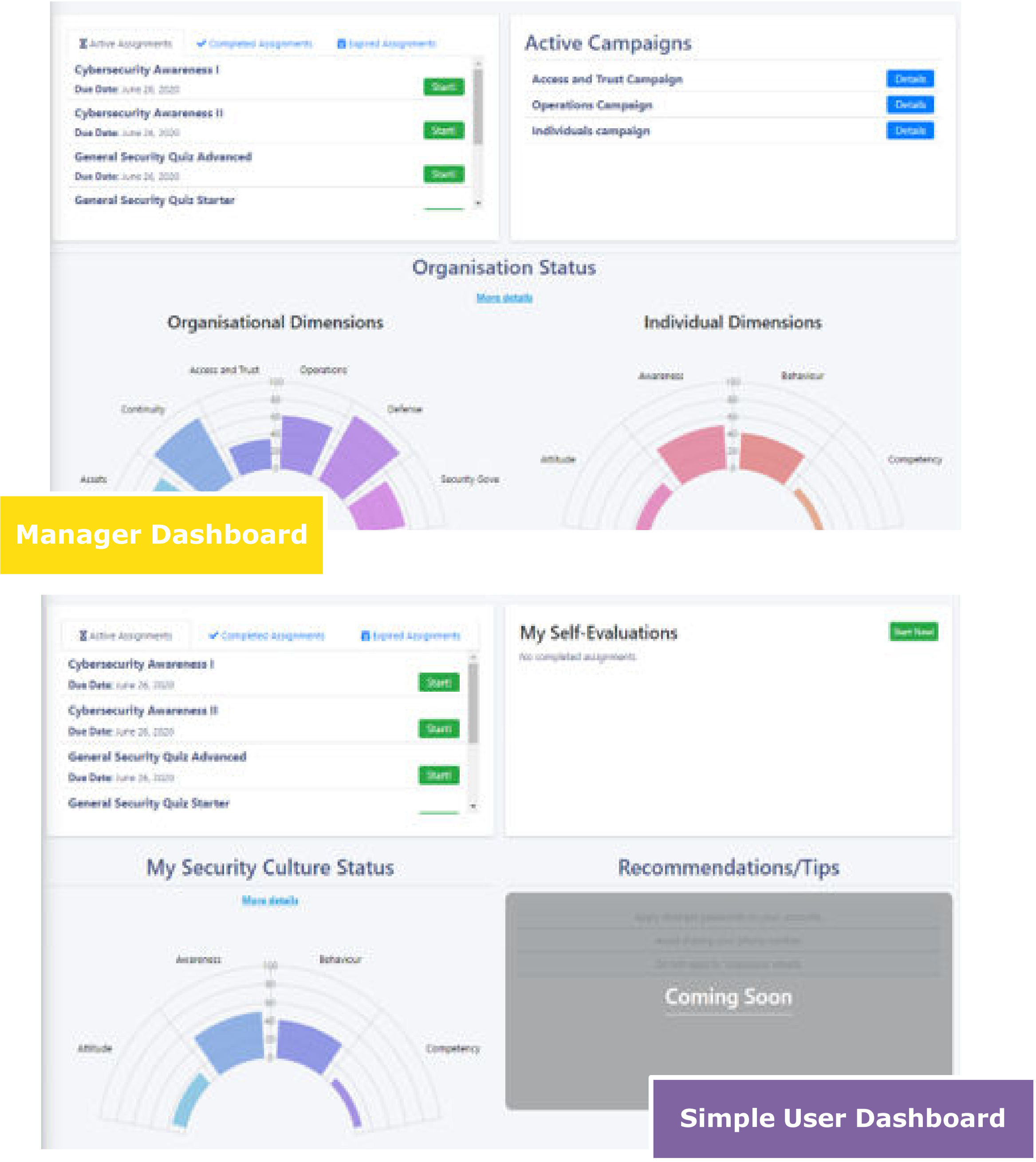
- ***Dashboard***: bears a different skeleton depending on user role allowing an overall functionality view and control of the tool.
- ***Users***: listing the participating members of the tool along with a number of organisational info.

- ***Groups***: listing the groups of the tool serving different evaluation purposes.
- ***Reports***: visualisation of the security culture assessment results and status.
- ***Self Evaluation***: offering to individuals the possibility to run a number of questionnaires and tests at their own pace.
- ***Campaigns*** (visible only to administrators and managers): materialisation of a security culture evaluation iteration with direct assignments of specific questionnaires and tests to dedicated individuals or groups.
- ***Questionnaires***: listing of available questionnaires of the tool while correlating them to security culture model.

Following paragraphs present in detail each one of the above options of the tool while correlating it to the corresponding security framework.

2.3.3.1. DASHBOARD

Having signed in, user lands in the dashboard screen which, depending on user role and privileges, provides an overall preview of the security culture tool functionality (including pending assignments, cyber-security status graphs and tips, etc.) while offering quick access to targeted submenus, as exhibited in Figure 17.



Active Assignments | Completed Assignments | Expired Assignments

Cybersecurity Awareness I
Due Date: June 26, 2020

Cybersecurity Awareness II
Due Date: June 26, 2020

General Security Quiz Advanced
Due Date: June 26, 2020

General Security Quiz Starter

Active Campaigns

- Access and Trust Campaign
- Operations Campaign
- Individuals campaign

My Self-Evaluations

No completed assignments.

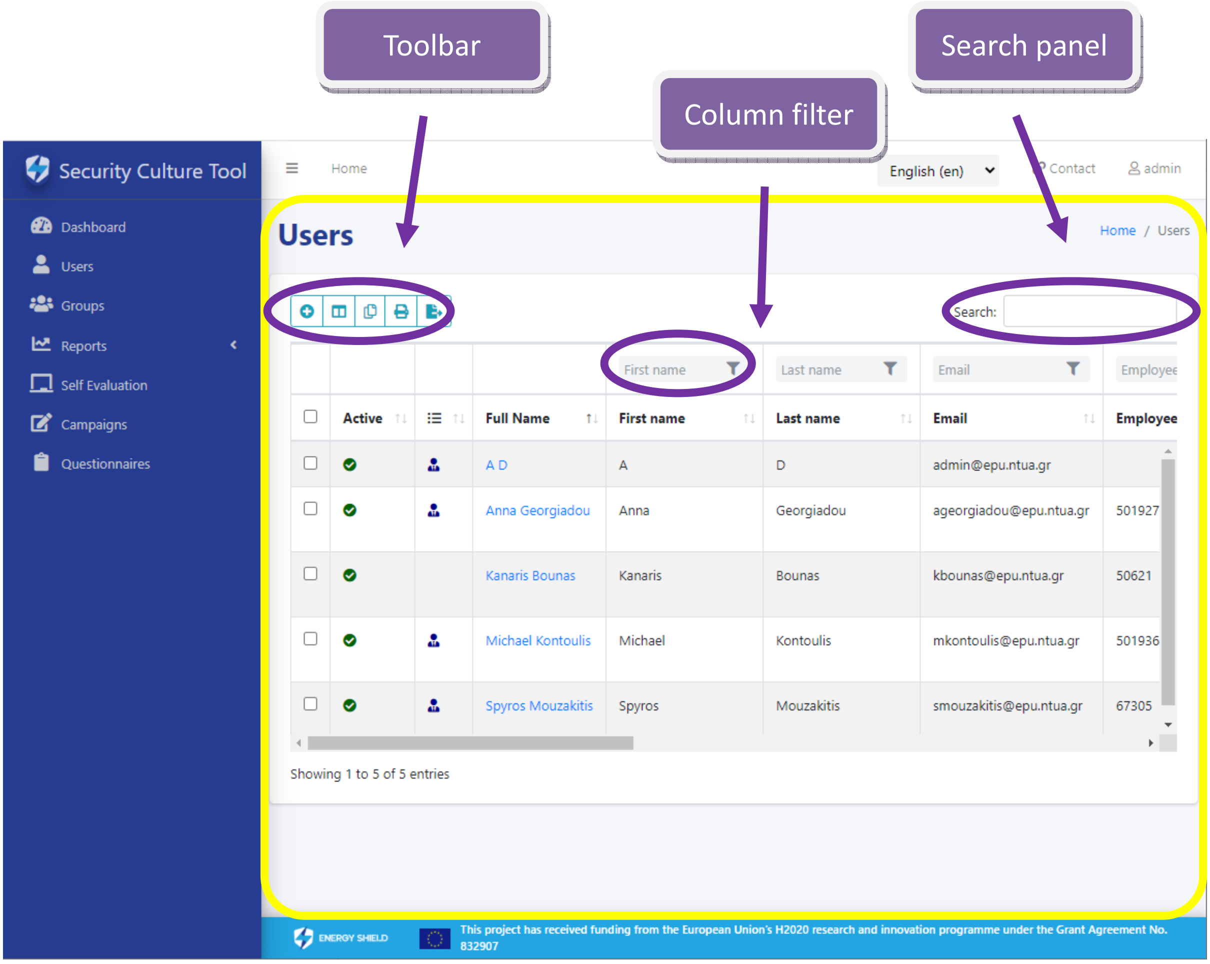
Figure 17. Dashboard view

2.3.3.2. USERS

This view displays users' information in a responsive table offering searching and multiple column filtering capabilities, as presented in Figure 18. Toolbar present in the upper left part contains the following buttons:

- ***Add*** (available only to administrators and managers): dropdown menu allowing creations of new user and group.
- ***Show/Hide columns***: control over column visibility.
- ***Copy***: copies selected table rows and columns to clipboard.

- ***Print***: prints selected table rows and columns while invoking web browser print menu.
- ***Export to file***: dropdown menu allowing export of the selected table rows and columns to different file formats (Excel, CSV and PDF).



☐	Active	☰	Full Name	First name	Last name	Email	Employee
				First name	Last name	Email	Employee
☐	✓	👤	A D	A	D	admin@epu.ntua.gr	
☐	✓	👤	Anna Georgiadou	Anna	Georgiadou	ageorgiadou@epu.ntua.gr	501927
☐	✓		Kanaris Bounas	Kanaris	Bounas	kbounas@epu.ntua.gr	50621
☐	✓	👤	Michael Kontoulis	Michael	Kontoulis	mkontoulis@epu.ntua.gr	501936
☐	✓	👤	Spyros Mouzakitis	Spyros	Mouzakitis	smouzakitis@epu.ntua.gr	67305

Showing 1 to 5 of 5 entries

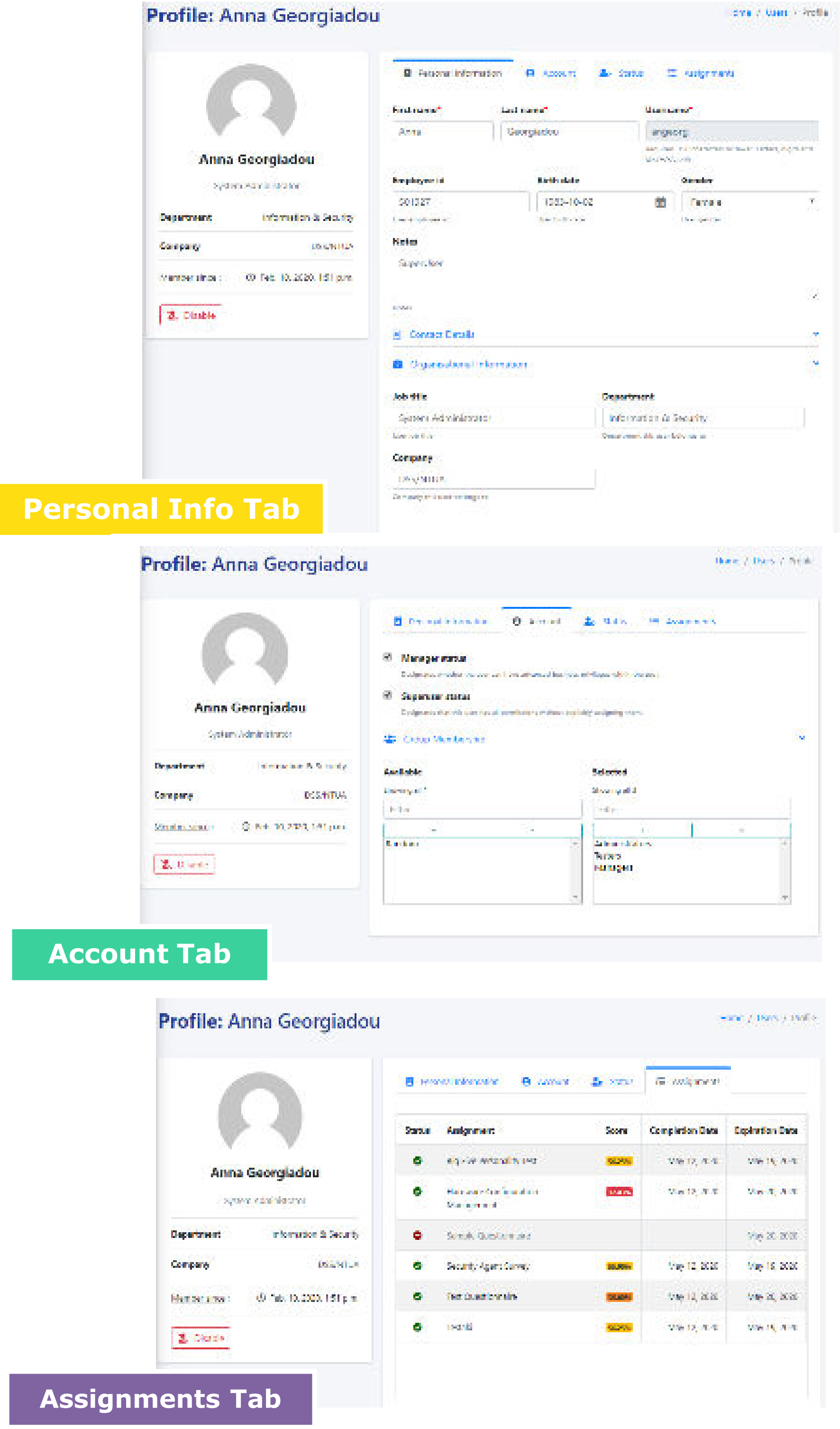
This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

Figure 18. Users view

Selecting one of the displayed users (by clicking on his/her full name) redirects you to the user profile view which, depending on access user role (administrator, manager or simple user) and privileges, presents user specific information and offers a number of different control actions.

As presented in Figure 19, user profile view contains:

- ***Summary panel***: generic user details (e.g. full name, job description)
- ***Personal Information Tab***: first and last name, contact details, organization info, and so on.
- ***Account Tab*** (visible only to administrators): account privileges and group membership.
- ***Assignments*** (visible only to administrators or profile owner): table view of all user assignments (completed, expired, pending) with score achievement, completion and expiration date and redirection link to assignment execution.



Profile: Anna Georgiadou

Anna Georgiadou
System Administrator

Department	Information & Security
Company	DS/NTUA
Member since :	Feb. 10, 2020, 1:51 p.m.

First name*: Anna
Last name*: Georgiadou
Username*: angeorg
Employee id: 301327
Birth date: [illegible]-10-02
Gender: Female
Notes: Supervisor
Job title: System Administrator
Department: Information & Security
Company: DS/NTUA

☑ Manager status
☑ Supervisor status

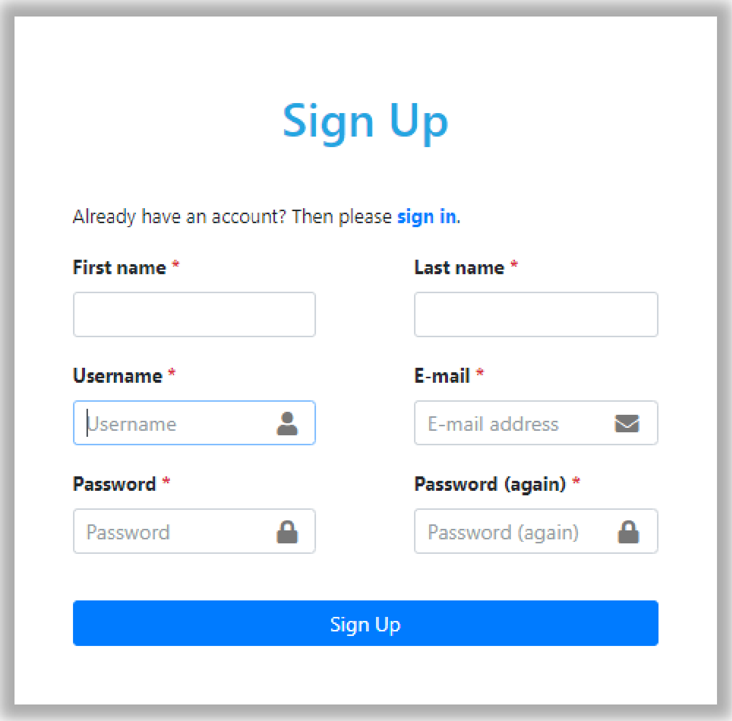
Available | Selected
Managers

Status	Assignment	Score	Completion Date	Expiration Date
✓	[illegible]	[illegible]	[illegible]	[illegible]
✓	[illegible]	[illegible]	[illegible]	[illegible]
●	Sample Questionnaire			May 20, 2020
✓	Security Agent Survey	[illegible]	May 12, 2020	May 19, 2020
✓	Test Questionnaire	[illegible]	May 12, 2020	May 20, 2020
✓	[illegible]	[illegible]	[illegible]	[illegible]

Figure 19. User profile view

For the creation of a new user, two options are available:

- ***Signup form*** (Figure 20): link to specific form could be distributed via any corporate tool or simply via email. Users need to complete their first and last name, username and password and an email, which shall be used as a security verification control, to sign up to security culture tool and gain access as simple user.



Sign Up

Already have an account? Then please sign in.

First name *

Last name *

Username *

Username

E-mail *

E-mail address

Password *

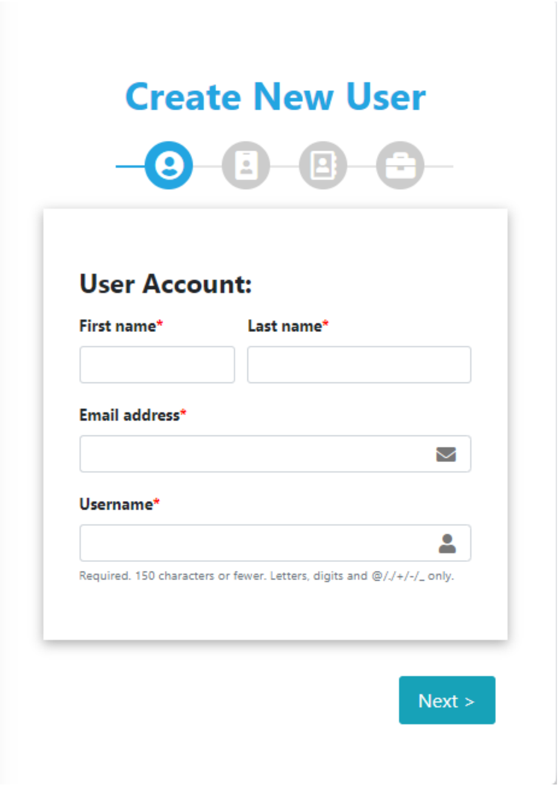
Password

Password (again) *

Password (again)

Figure 20. Sign-up view

- ***Create new user wizard*** (available only to administrators and managers): accessible via the users and groups view toolbar (Figure 21). Wizard guides you through the creation procedure of a new user offering the possibility to complete both required and optional fields. Upon successful completion, a verification email is sent to the newly created user and confirmation is expected for the account to be accessible.



Create New User

User Account:

First name*

Last name*

Email address*

Username*

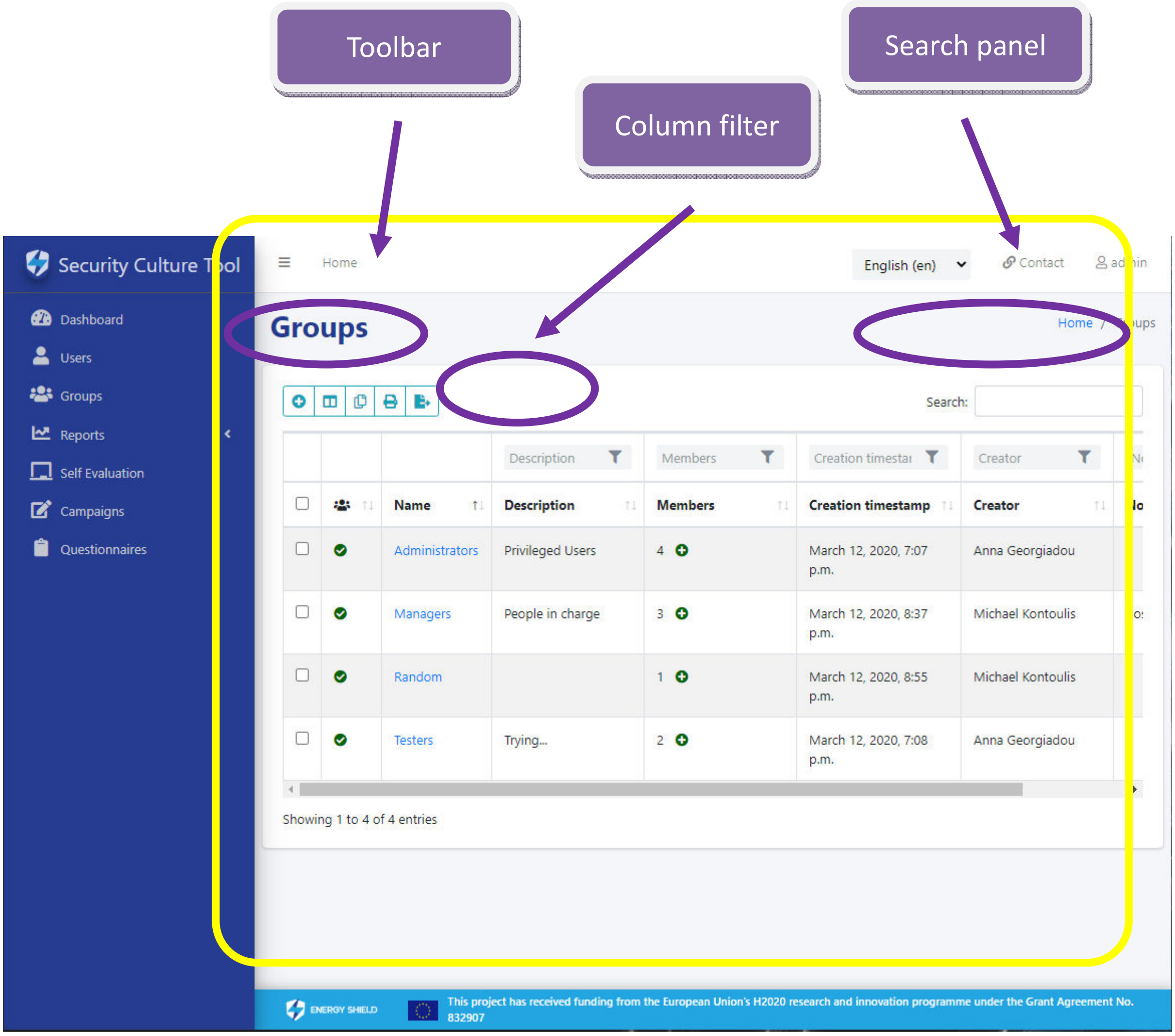
Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

Figure 21. Create new user wizard

2.3.3.3. GROUPS

This view displays groups' information in a responsive table offering searching and multiple column filtering capabilities, as presented in Figure 22. Toolbar present in the upper left part contains the following buttons:

- ***Add*** (available only to administrators and managers): dropdown menu allowing creations of new user and group.
- ***Show/Hide columns***: control over column visibility.
- ***Copy***: copies selected table rows and columns to clipboard.
- ***Print***: prints selected table rows and columns while invoking web browser print menu.
- ***Export to file***: dropdown menu allowing export of the selected table rows and columns to different file formats (Excel, CSV and PDF).



Groups

			Description	Members	Creation timesta	Creator	Ne
☐		Name	Description	Members	Creation timestamp	Creator	No
☐	✓	Administrators	Privileged Users	4 ⊕	March 12, 2020, 7:07 p.m.	Anna Georgiadou	
☐	✓	Managers	People in charge	3 ⊕	March 12, 2020, 8:37 p.m.	Michael Kontoulis	o:
☐	✓	Random		1 ⊕	March 12, 2020, 8:55 p.m.	Michael Kontoulis	
☐	✓	Testers	Trying...	2 ⊕	March 12, 2020, 7:08 p.m.	Anna Georgiadou	

Showing 1 to 4 of 4 entries

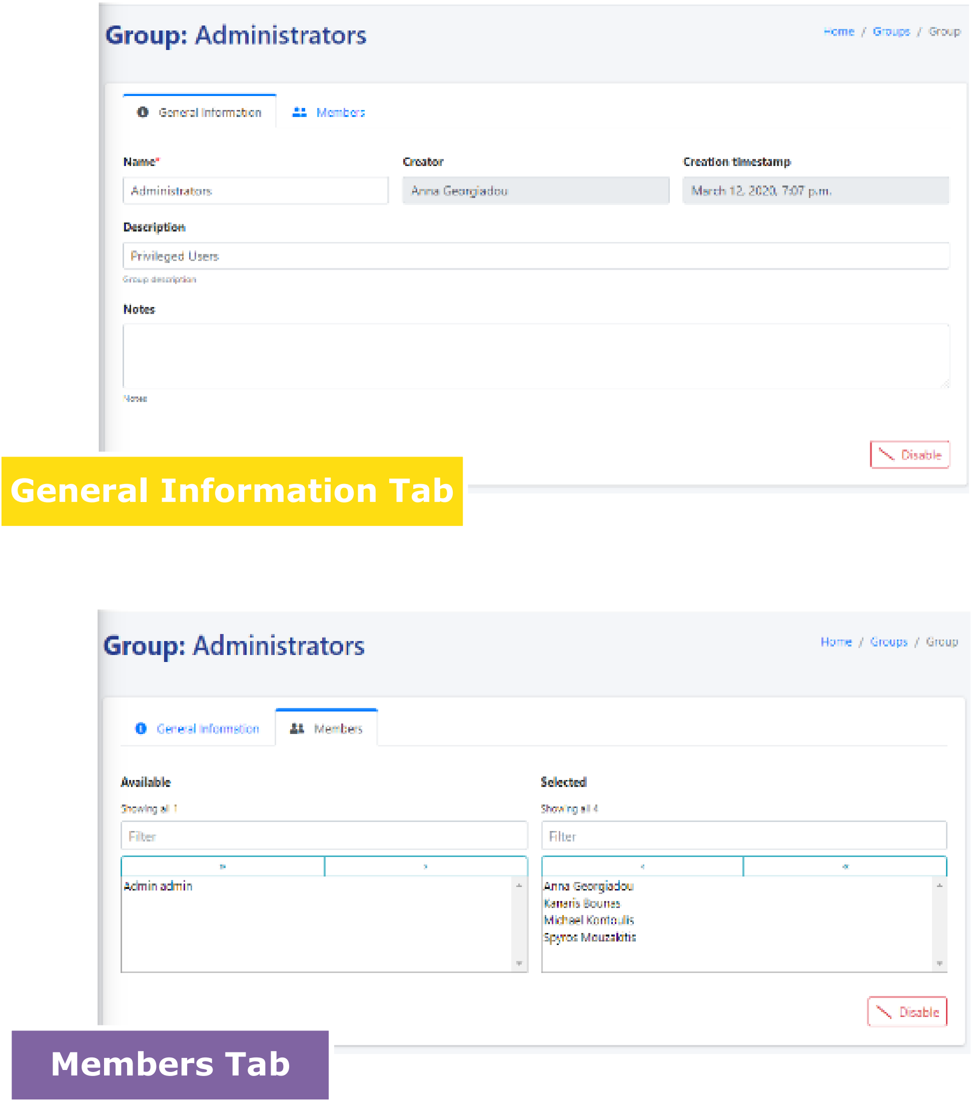
Figure 22. Groups view

Groups view exhibits ***global groups*** (description used for groups created by the administrators of the tool) to all users. If signed in user is a manager, along with global groups, table contains also the groups created by specific user. Administrators, as expected, have access and view to all groups available.

Selecting one of the displayed groups (by clicking on its name) redirects you to the group details view which presents group specific information and offers a number of different control actions.

As presented in Figure 23, group details view contains:

- ***General Information Tab***: name, creation details, description, and so on.
- ***Members Tab***: members of the group.



General Information Tab

Group: Administrators

Home / Groups / Group

Name*: Administrators

Creator: Anna Georgiadou

Creation timestamp: March 12, 2020, 7:07 p.m.

Description: Privileged Users

Group description

Notes:

Notes

Members Tab

Group: Administrators

Home / Groups / Group

Available

Showing all 1

Filter

Admin admin

Selected

Showing all 4

Filter

Anna Georgiadou
Kanaris Bounes
Michael Kontoulis
Spyros Mouzakitis

Figure 23. Group details view

Create new group wizard (available only to administrators and managers) is accessible via the users and groups view toolbar (Figure 24). Wizard guides you through the creation procedure of a new group offering the possibility to complete both required and optional fields.

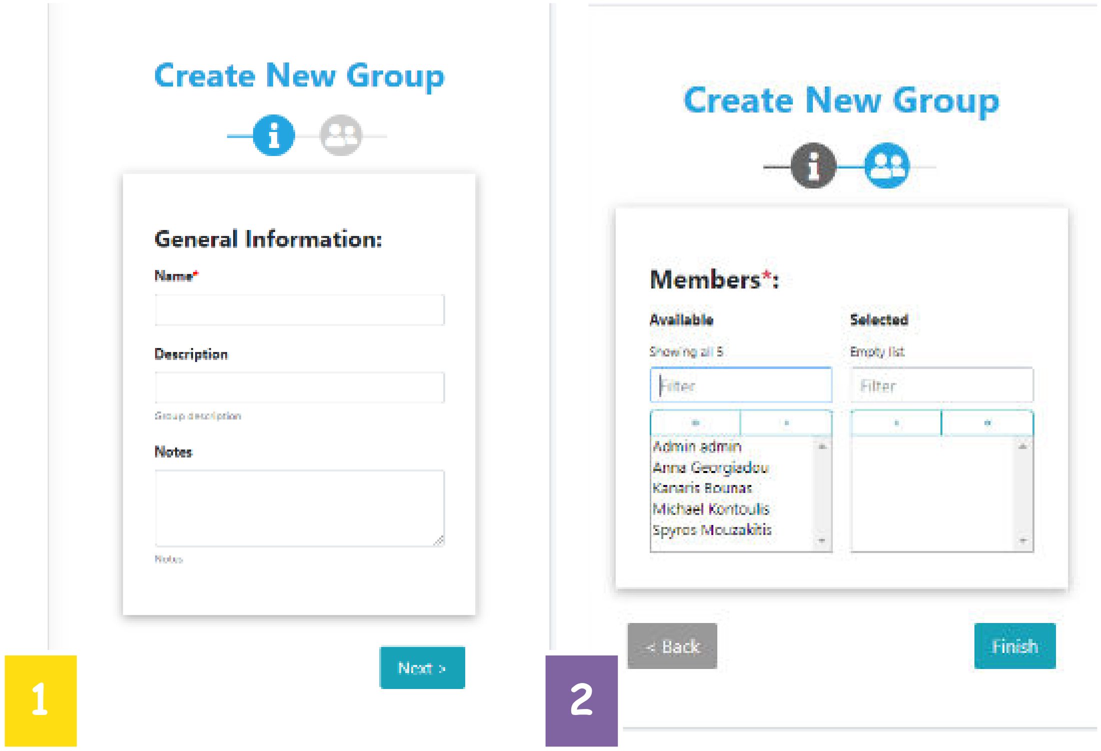


Figure 24. Create new group wizard

2.3.3.4. REPORTS

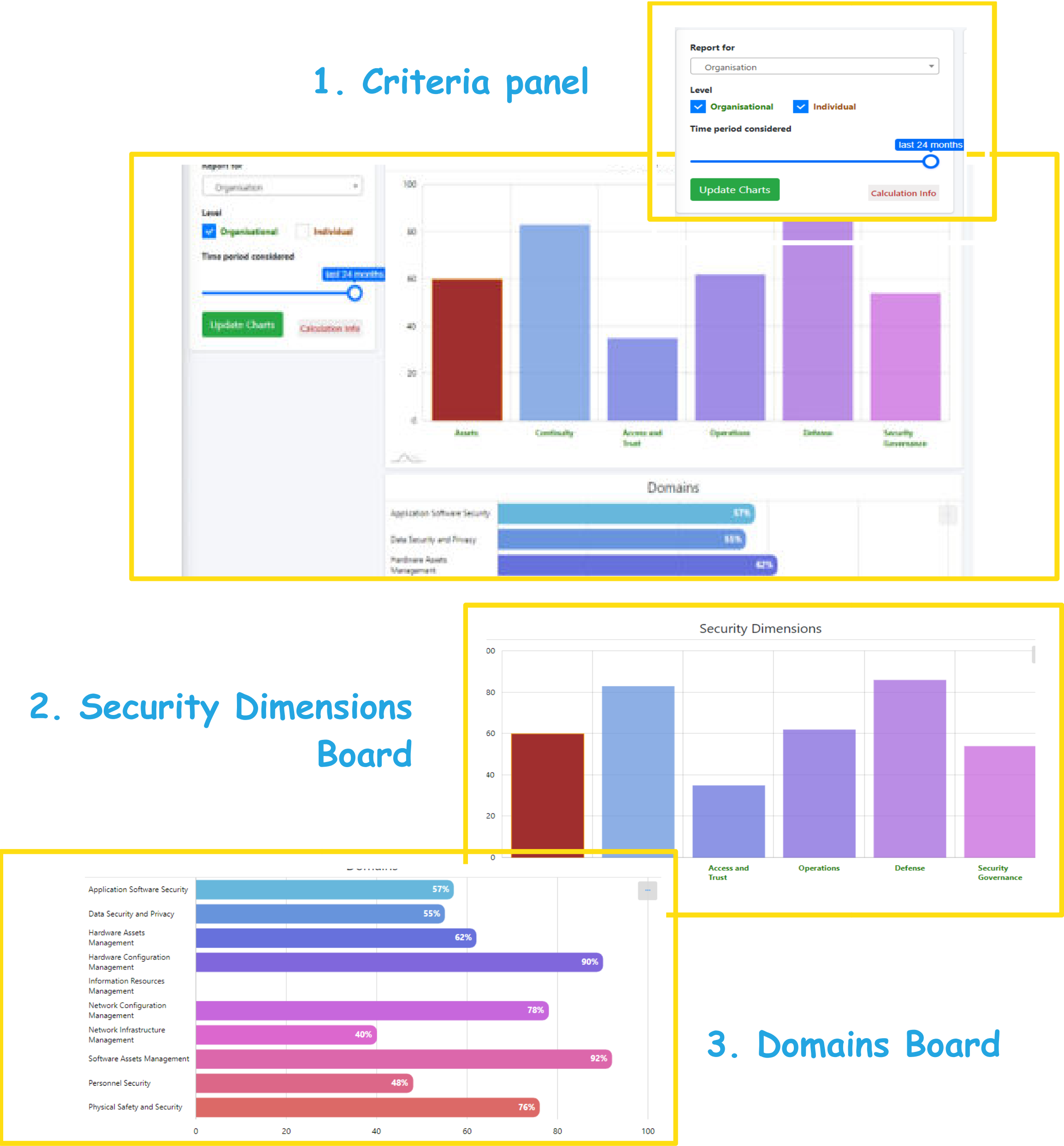
This view offers access to the reporting and visualization mechanism of the SBAM tool. Displayed information is properly filtered depending on user role and privileges guiding user through the creation of a suitable security culture assessment analysis report.

As presented in Figure 25, this view is consisted of three main parts:

- ***Criteria panel (visible only to manager and administrators):*** user can select to create an organisation, campaign or group report by making the corresponding choice from the drop-down menu. Depending on selection, the rest of the panel is updated to demonstrate available options. A level filter is also present at all cases to allow isolation of the different security culture levels (organisational and individual). At the bottom of the criteria panel, a time slide-bar enables user to further trim reported data adjusting time window (starting from a 24-months period). Having inserted desired reporting criteria, user may preview security dimensions status by simply clicking on the "*Update Charts*" button. "*Calculation info*" button pops up a new window offering a detailed preview of the survey responses that were used for the calculation of the metrics displayed on the charts. More specifically, calculation info is divided into the cyber-security culture model dimensions and domains and reach down to a questionnaire level.
- ***Security Dimensions board:*** contains a responsive vertical bar chart of the cyber-security dimensions. In the case of a simple user, it is limited down to

security culture individual level dimensions demonstrating data for specific user while, for managers and administrators, charts are formulated based on the criteria panel. Hovering over any element of the chart, gives an overview of its details while clicking on it updates the ***Domains board*** accordingly. At the upper right corner of the board, an export button is available offering a variety of formatting options (image, data, print).

- ***Domains board:*** contains a horizontal bar chart of the cyber-security domains related to selected dimension. At the upper right corner of the board, an export button is available offering a variety of formatting options (image, data, print).



1. Criteria panel

Report for: Organisation

Level: ☑ Organisational ☑ Individual

Time period considered: last 24 months

Update Charts
Calculation Info

2. Security Dimensions Board

Security Dimensions
0
20
40
60
80
00
Assets
Continuity
Access and Trust
Operations
Defense
Security Governance

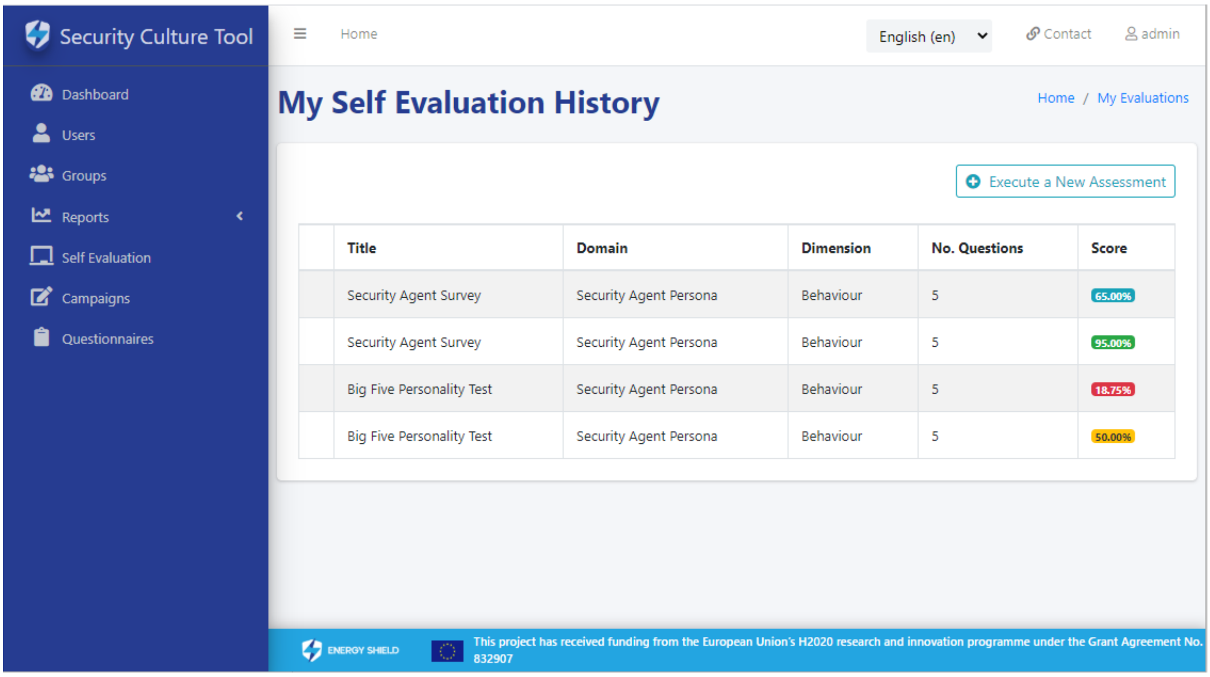
3. Domains Board

Domains
Application Software Security 57%
Data Security and Privacy 55%
Hardware Assets Management 62%
Hardware Configuration Management 90%
Information Resources Management
Network Configuration Management 78%
Network Infrastructure Management 40%
Software Assets Management 92%
Personnel Security 48%
Physical Safety and Security 76%
0
20
40
60
80
100

Figure 25. Reports view

2.3.3.5. SELF EVALUATION

This view offers access to the self-evaluation mechanism of the SBAM tool. It displays a self-evaluation history log containing all surveys completed by the sign-in user along with an achievement score and the affected security culture dimensions and domains as presented in Figure 26.



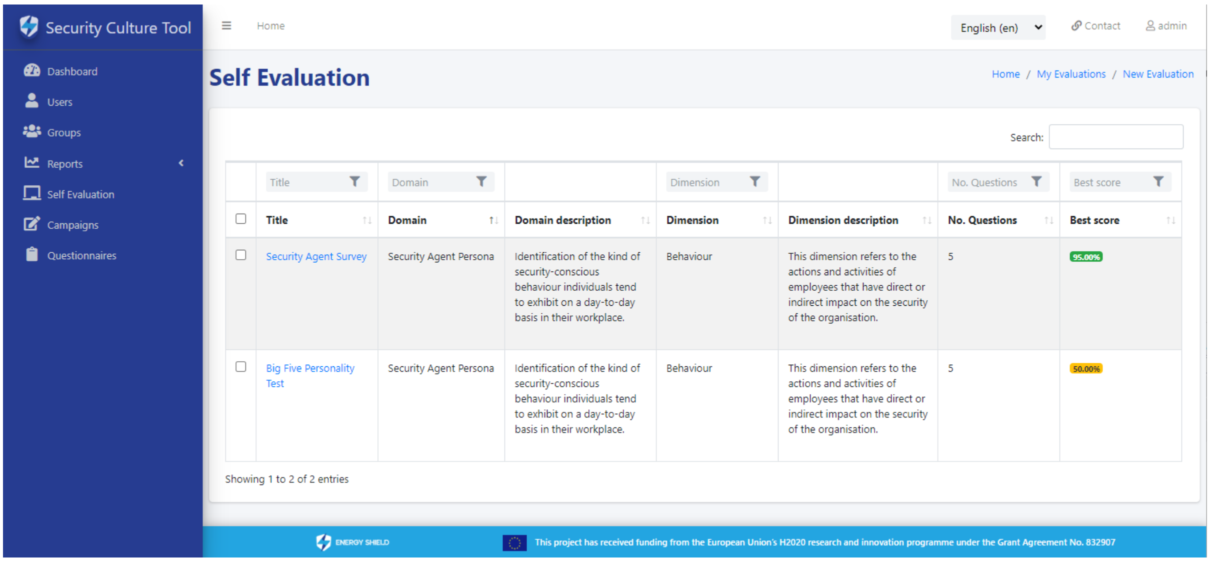
My Self Evaluation History

	Title	Domain	Dimension	No. Questions	Score
	Security Agent Survey	Security Agent Persona	Behaviour	5	65.00%
	Security Agent Survey	Security Agent Persona	Behaviour	5	95.00%
	Big Five Personality Test	Security Agent Persona	Behaviour	5	18.75%
	Big Five Personality Test	Security Agent Persona	Behaviour	5	50.00%

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

Figure 26. Self-evaluations view

On the upper right part an "Execute a New Assessment" button is available redirecting the user to the self-evaluation view presented in Figure 27 which displays all available individual level questionnaires along with a number of security culture model correlation details and the highest related achievement score. User can preview his/her cyber-security performance status and exercise via triggering the execution of any of the available assessment questionnaires by simply clicking on the questionnaire of interest.



Self Evaluation

Home / My Evaluations / New Evaluation

Search:

□	Title	Domain	Domain description	Dimension	Dimension description	No. Questions	Best score
□	Security Agent Survey	Security Agent Persona	Identification of the kind of security-conscious behaviour individuals tend to exhibit on a day-to-day basis in their workplace.	Behaviour	This dimension refers to the actions and activities of employees that have direct or indirect impact on the security of the organisation.	5	95.00%
□	Big Five Personality Test	Security Agent Persona	Identification of the kind of security-conscious behaviour individuals tend to exhibit on a day-to-day basis in their workplace.	Behaviour	This dimension refers to the actions and activities of employees that have direct or indirect impact on the security of the organisation.	5	50.00%

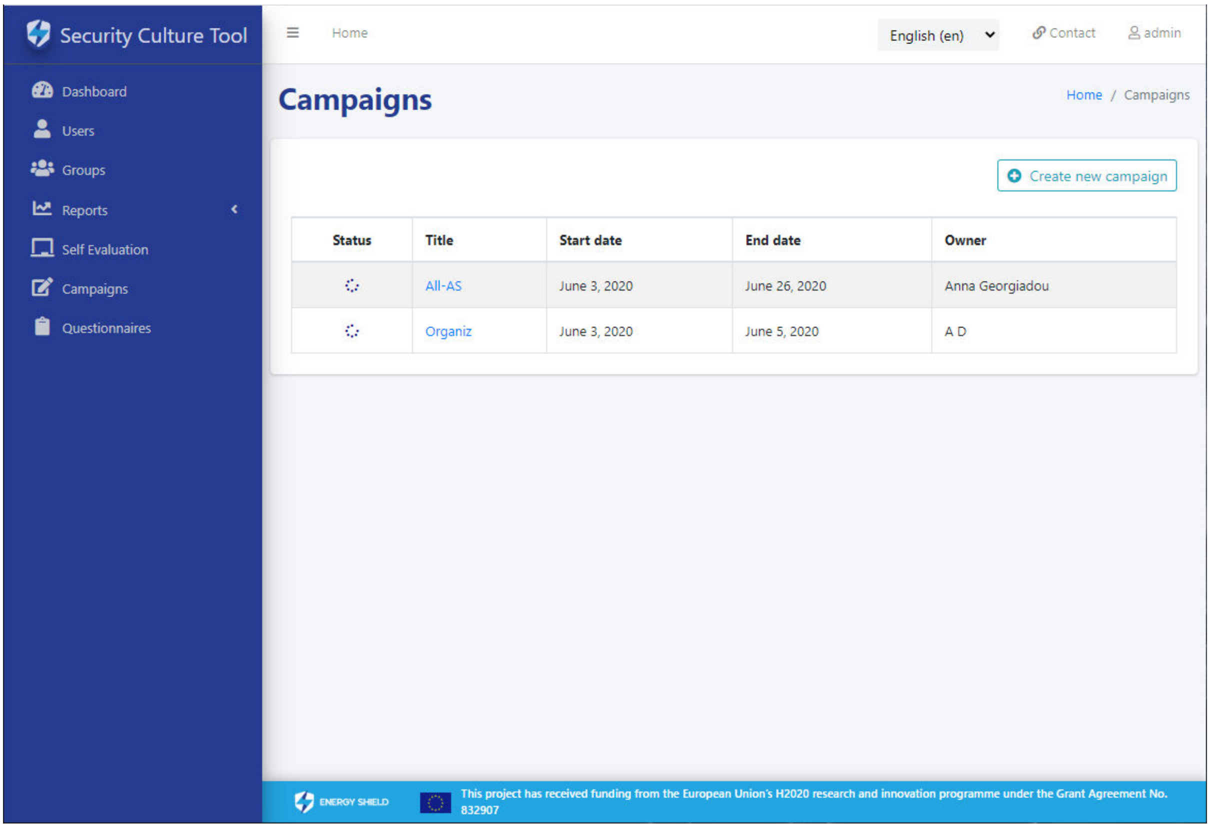
Showing 1 to 2 of 2 entries

ENERGY SHIELD This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

Figure 27. Execute new assessment view

2.3.3.6. CAMPAIGNS

This view (available only to administrators and managers) displays campaigns' information in a table as presented in Figure 28.



Campaigns

Home / Campaigns

Status	Title	Start date	End date	Owner
◌	All-AS	June 3, 2020	June 26, 2020	Anna Georgiadou
◌	Organiz	June 3, 2020	June 5, 2020	A D

ENERGY SHIELD This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

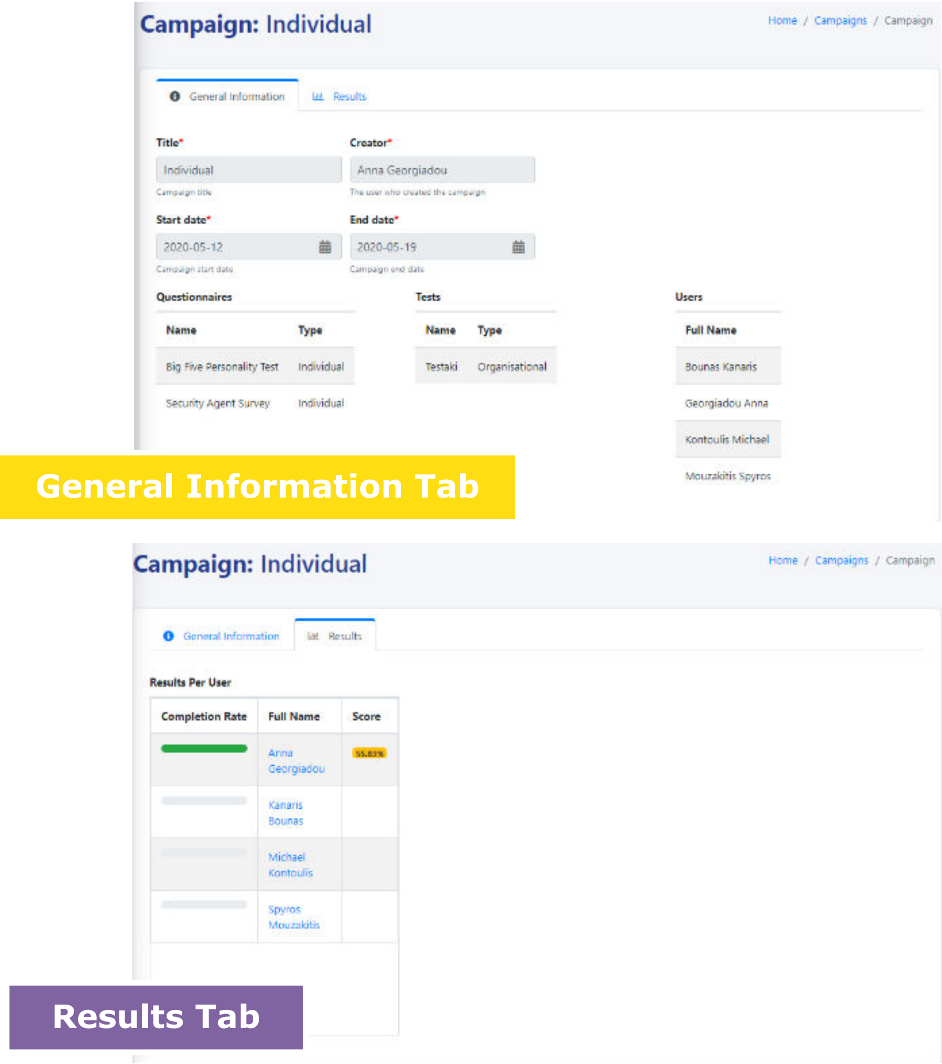
Figure 28. Campaigns view

Campaigns view exhibits ***global campaigns*** (description used for campaigns created by the administrators of the tool) to all users. If signed in user is a manager, along with global campaigns, table contains also the campaigns created by specific user. Administrators, as expected, have access and view to all campaigns available.

Selecting one of the displayed campaigns (by clicking on its title) redirects you to the campaign details view which presents campaign specific information and offers a number of different control actions.

As presented in Figure 29, campaign details view contains:

- ***General Information Tab***: title, creation details, start and end date, questionnaires and tests assigned and participants.
- ***Results Tab***: summary of the results per user along with progress status.



Campaign: Individual

Title*
Individual
Campaign title

Creator*
Anna Georgiadou
The user who created the campaign

Start date*
2020-05-12
Campaign start date

End date*
2020-05-19
Campaign end date

Questionnaires

Name	Type
Big Five Personality Test	Individual
Security Agent Survey	Individual

Tests

Name	Type
Testaki	Organisational

Users

Full Name
Bounas Kanaris
Georgiadou Anna
Kontoulis Michael
Mouzakitis Spyros

General Information Tab

Campaign: Individual

Results Per User

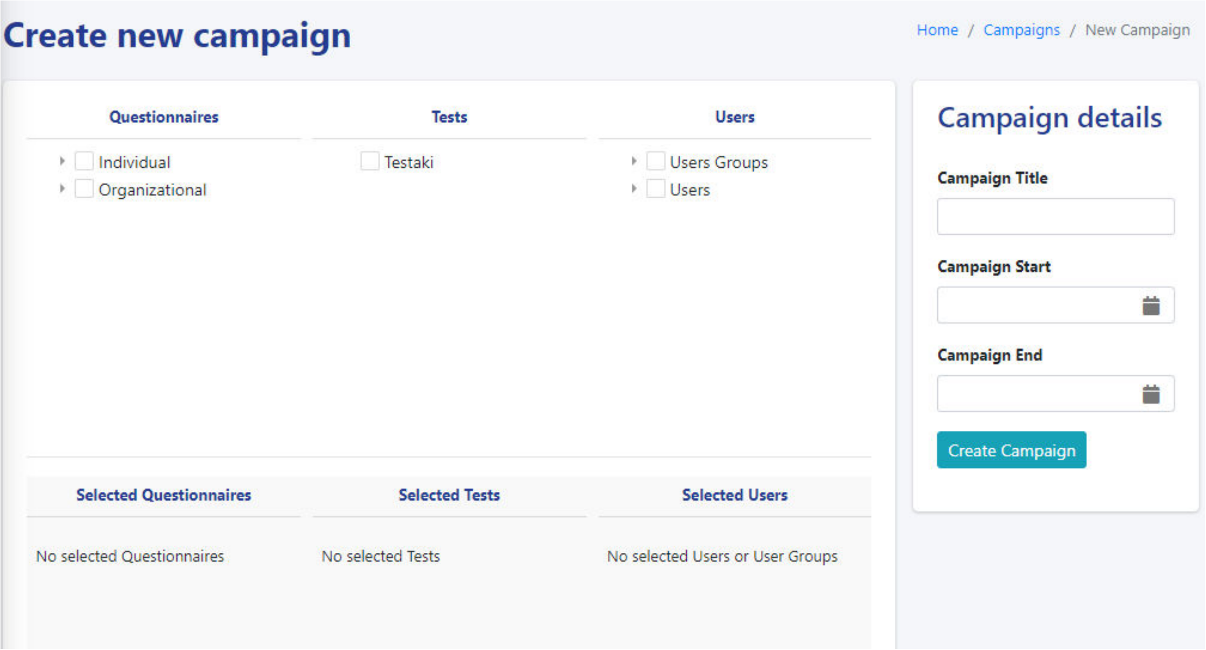
Completion Rate	Full Name	Score
🟩	Anna Georgiadou	55.83%
	Kanaris Bounas	
	Michael Kontoulis	
	Spyros Mouzakitis	

Results Tab

Figure 29. Campaign details view

On the upper right part of the campaigns view, a “Create New Campaign” button is available redirecting the user to the creation view presented in Figure 30. This view is consisted of:

- ***Assignment card***: presents, in a tree view, available questionnaires, tests, users and groups. Selecting any of these results in listing them on the lower part of the card while making correlated assignment between security culture controls and corresponding participants of the campaign.
- ***Campaign details card***: holds the campaign title along with the start and end date of the assessment period.



No selected Questionnaires

No selected Tests

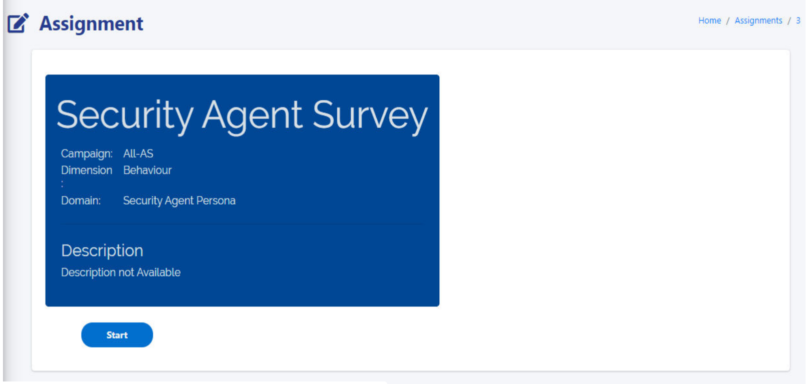
No selected Users or User Groups

Figure 30. Create new campaign view

Upon creation of a campaign, a number of assignments are created and presented to corresponding assignees to:

- ***Dashboard –> Assignments Card***: presents and offers access to active assignments. Additionally, it lists the completed and expired ones in different tabs.
- ***User profile -> Assignment Tab***: presents user assignments along with a number of details offering access to the pending ones.

When an active assignment is selected by its assignee, if it refers to a questionnaire, the survey execution mechanism is triggered and an evaluation iteration is initiated guiding the user through its completion. Upon submission an achievement score is presented to the end user.



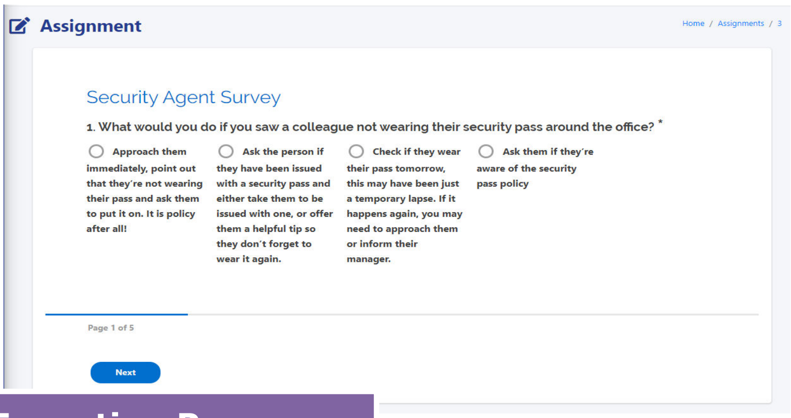
Assignment

Security Agent Survey

Campaign: All-AS
Dimension: Behaviour
Domain: Security Agent Persona

Description
Description not Available

Initial Survey Page



Assignment

Security Agent Survey

1. What would you do if you saw a colleague not wearing their security pass around the office? *

○ Approach them immediately, point out that they're not wearing their pass and ask them to put it on. It is policy after all!

○ Ask the person if they have been issued with a security pass and either take them to be issued with one, or offer them a helpful tip so they don't forget to wear it again.

○ Check if they wear their pass tomorrow, this may have been just a temporary lapse. If it happens again, you may need to approach them or inform their manager.

○ Ask them if they're aware of the security pass policy

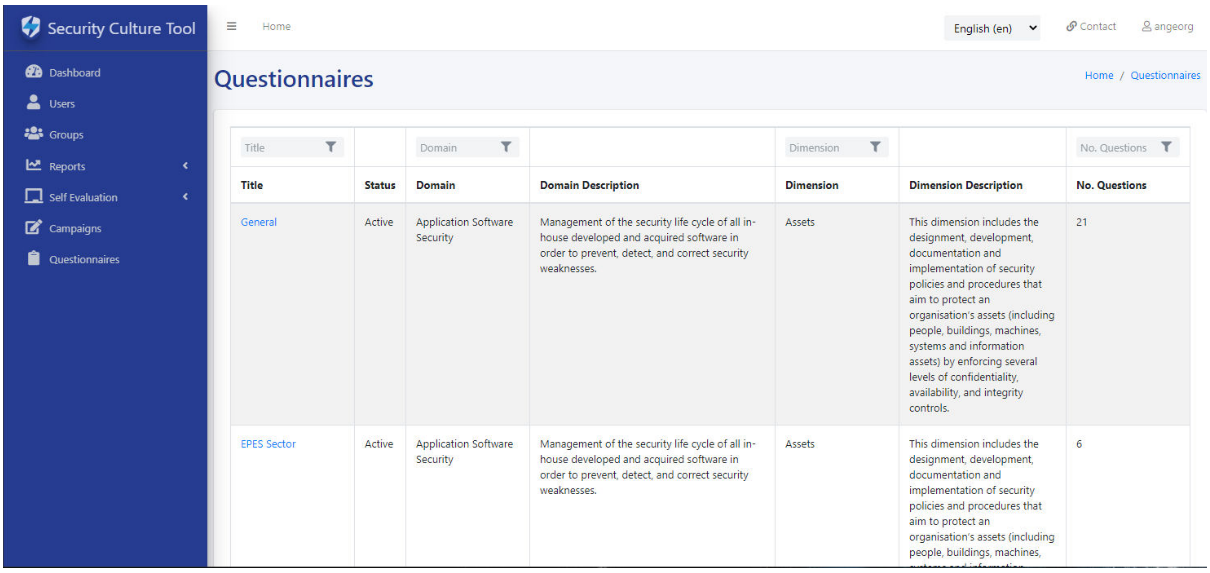
Page 1 of 5

Execution Page

Figure 31. Campaign assignment execution

2.3.3.7. QUESTIONNAIRES

This view displays the available cyber-security culture questionnaires while correlating them with the suggested model (levels, dimensions and domains) as presented in Figure 32.



Questionnaires

Home / Questionnaires

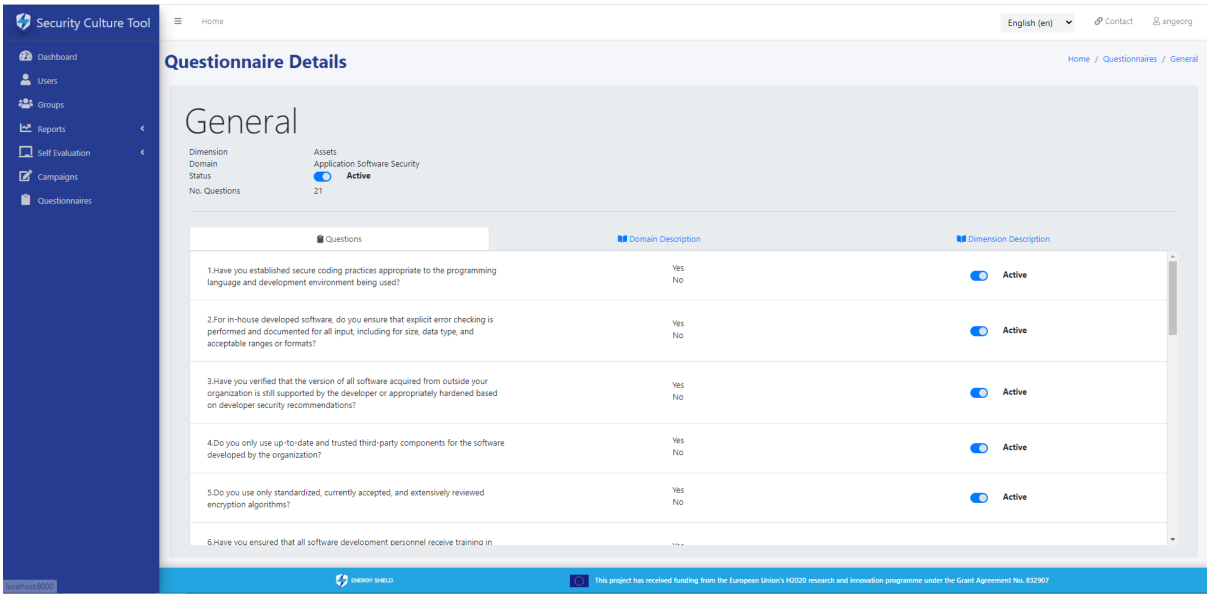
Title	Status	Domain	Domain Description	Dimension	Dimension Description	No. Questions
General	Active	Application Software Security	Management of the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	Assets	This dimension includes the designment, development, documentation and implementation of security policies and procedures that aim to protect an organisation's assets (including people, buildings, machines, systems and information assets) by enforcing several levels of confidentiality, availability, and integrity controls.	21
EPES Sector	Active	Application Software Security	Management of the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	Assets	This dimension includes the designment, development, documentation and implementation of security policies and procedures that aim to protect an organisation's assets (including people, buildings, machines,	6

Figure 32. Questionnaires view

Selecting one of the displayed questionnaires (by clicking on its title) redirects you to the questionnaire details view which presents questionnaire specific information offering control over its activity status.

As presented in Figure 33, questionnaire details view presents:

- Information correlating questionnaire with the underlying cyber-security culture model.
- Questions contained with available options and control over their activity status.



Questionnaire Details

Home / Questionnaires / General

General

Dimension Assets
Domain Application Software Security
Status Active
No. Questions 21

1.Have you established secure coding practices appropriate to the programming language and development environment being used?	Yes No	Active
2.For in-house developed software, do you ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats?	Yes No	Active
3.Have you verified that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations?	Yes No	Active
4.Do you only use up-to-date and trusted third-party components for the software developed by the organization?	Yes No	Active
5.Do you use only standardized, currently accepted, and extensively reviewed encryption algorithms?	Yes No	Active
6.Have you ensured that all software development personnel receive training in		

Figure 33. Questionnaire details view

3. CONCLUSION AND NEXT STEPS

This deliverable presented the security culture framework and tool designed and implemented in order to facilitate the assessment, cultivation and improvement of the cyber-security culture status of an organisation via a holistic approach. Numerous security elements and factors have been identified, listed and grouped into different levels, dimensions and domains offering a hierarchical representation of the cyber-security readiness and overall reality of an organisation. Role segregation, key assessment concepts and specific evaluation methodology have been presented in detail providing a useful guide through this rather demanding business procedure.

Future steps in our work include, but are not limited to, the following:

- Calibrating the security culture framework by adjusting the weights of each security element contained within the suggested model.
- Enriching the available tool content by introducing new questionnaires adjusted to the needs of the pilots for the EPES sector.
- Introducing tests and a gamification mechanism to further assess cybersecurity culture domains (e.g. mail phishing simulations, password-related games, security IQ).
- Mapping the assessment results of different security culture domains to specific cyber-security threats based on the MITRE ATT&CK knowledge base.
- Offering recommendations of existing security training programs/actions based on the evaluation results and aiming to the improvement of the identified security weaknesses.
- Evaluating and further improving both the suggested framework and tool based on the provided by the pilots' feedback.
- Integrating SBAM tool with the EnergyShield toolkit.

A detailed list of the next tool features is included in T1.1 (technical requirements) deliverable.

REFERENCES

[ABA14] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237-248. doi:10.1080/0144929X.2012.708787

[BUS04] Business and Advisory Committee to the OECD. (2004). *Securing your business. An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems:Towards a culture of security.* International Chamber of Commerce: OECD.

[CAM03] Campbell, K., Lawrence, G. A., Martin, L. P., & Lei, Z. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448. doi:10.3233/JCS-2003-11308

[DOH05] Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18*(4), 21-40. doi:10.4018/irmj.2005100102

[GAR03] Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security, 11*(2), 74-83. doi:10.1108/09685220310468646

[HOF00] Hoffman, N., & Klepper, R. (2000). Assimilating New Technologies: The Role of Organizational Culture. *Information Systems Management, 17*(3), 1-7. doi:10.1201/1078/43192.17.3.20000601/31239.6

[LAW11] Lawrence, G. A., Loeb, M. P., & Lei, Z. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 19*(1), 33-56. doi:10.3233/JCS-2009-0398

[RAN12] Rantos, K., Fysarakis, K., & Manifavas, H. (2012, 01). How Effective Is Your Security Awareness Program? An Evaluation Methodology. *Information Security Journal: A Global Perspective, 21*, 328-345. doi:10.1080/19393555.2012.747234

[RON09] Ronald , R. S. (2009). *Recommended Security Controls for Federal Information Systems and Organizations.* Special Publication (NIST SP) - 800-53 Rev 3.

[SCA08] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment.* Computer Security Resource Center.

[WIL09] Williams, P. (2009). What Does Security Culture Look Like For Small Organizations? *7th Australian Information Security Management Conference.* Perth, Western Australia.

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

www.energy-shield.eu