SECONOMICS

D1.4 - Model Validation

A. Pollini, A. Tedeschi (DBL), W. Shim, M. De Gramatica (UNITN), U. Turhan, B. Acikel (AU)

Pending of approval from the Research Executive Agency - EC

Document Number	D1.4
Document Title	Model Validation
Version	2.0
Status	Final
Work Package	WP 1
Deliverable Type	Report
Contractual Date of Delivery	30.04.2014
Actual Date of Delivery	30.04.2014
Responsible Unit	DBL
Contributors	AU, UNITN, UJRC, ISASCR, NGRID
Keyword List	Validation, models.
Dissemination level	PU

SEVENTH FRAMEWORK PROGRAMME

SECONOMICS Consortium

SECONOMICS "Socio-Economics meets Security" (Contract No. 285223) is a Collaborative project) within the 7th Framework Programme, theme SEC-2011.6.4-1 SEC-2011.7.5-2 ICT. The consortium members are:

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Project Manager: prof. Fabio MASSACCI Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy www.dblue.it	Contact: Alessandra TEDESCHI Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.fraunhofer.de/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle TulipanS/N, 28933, Mostoles (Madrid), Spain	Contact: Prof. David Rios Insua david.rios@urjc.es
5	1495 UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) whose principal administrative office is at King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Dr Matthew Collinson matthew.collinson@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITA DE BARCELONA SA, Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	Atos	ATOS ORIGIN SOCIEDAD ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Alicia Garcia Medina alicia.garcia@atos.net
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOÚ Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom	Contact: Dr Ruprai Raminder Raminder.Ruprai@uk.ngrid.com
11	ANADOLU ÜNİVERSİTESİ	ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION Iki Eylul Kampusu, 26470, Eskisehir, Turkey	Contact: Nalan Ergun nergun@anadolu.edu.tr
12	Durham University	The Palatine Centre, Stockton Road, Durham, DH1 3LE, UK	Contact: Prof. Julian Williams julian.williams@durham.ac.uk

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	30/01/2014	Draft	A . Tedeschi (DBL) A . Pollini (DBL)	Draft
0.2	4/03/2014	Draft	A . Tedeschi (DBL) A . Pollini (DBL) M. De Gramatica, W. Shim, F. Massacci (UNITN) U. Turhan (AU)	First complete version including AU and UNITN contributions.
1.0	7/03/2014	Draft	A . Tedeschi (DBL) A . Pollini (DBL)	Minor changes in the deliverable and Annexes added.
1.1	18/03/2014	Draft	W. Shim, M. de Gramatica (UNITN)	Scientific Review
1.2	21/03/2014	Draft	E. Chiarani (UNITN)	Quality change. Some improvements in the format requested. Some minor changes requested.
1.3	26/03/2014	Draft	R. Ruprai (NGRID)	Scientific Review. Minor changes requested
1.4	10/04/2014	Draft	A . Tedeschi (DBL) A . Pollini (DBL)	Final version
1.4	14/04/2014	Draft	W. Shim, E. Chiarani (UNITN)	Second Quality check and review
2.0	18/04/2014	Final	A . Tedeschi (DBL) A . Pollini (DBL)	Final version

INDEX

Executive summary

D1.4 deliverable describes the methodologies, the activities and the outcomes of the model validation task, which informs and supports the technical WPs (4-5-6), in order to develop the risk, economic and social models of security. The complexity and the innovation of the proposed solutions in different domains make the process of validating the results a challenging task. Just as the security, social and economic issues, addressed by the project, are heterogeneous, so are the results expected for each technical Work Package, ranging from theoretical models to policy guidelines and software toolkit for decision support. Therefore, it was necessary to perform different and customized validation activities. Such activities and results are described according to the main phases of the overall implementation process: model scoping, model building and model validation.

The validation pursues both the achievement, meaning the in itinere validation to steer the models in the right direction; and the assurance of the project results, i.e. the final validation to ensure that the final models are correct from the airport stakeholders' perspective. The WP1 Airport Security validation framework has been defined according to the theoretical framework, the validation objectives and the validation criteria described in D7.1 Validation Plan.

The validation objectives and criteria of the Airport Case Study concern the acceptance of WP5 and WP6 models by Airport domain experts (e.g. security managers in airport organizations, airlines, air navigation service providers and regulators) and potential end-users (e.g. airport organizations and policy makers).
Each validation activity involved Airport domain experts in order to assess the models from practitioner's viewpoint and to identify opportunities for the exploitation of project results within the Aviation and Airport Security domain.

Main validation activities in the Airport Case Study fall into four major categories: Focus Groups and Interviews with Stakeholders, Methodology Evaluation through modeling activities, Models' Walkthrough activities involving step-by-step explanation and discussion of the SECONOMICS framework with Airport domain experts.
In particular, this report highlights that, and describes how, SECONOMICS solutions can be used in the application domain and further improvements can be achieved in other to align well with industry practices.

Annexes to the present deliverable will include the protocols, the scripts and the questionnaires designed as tools supporting the model validation process, as well as the tables of the results.

1. Introduction

WP1 Model Validation consisted of an iterative and incremental process through which a variety of user research and analysis, as well as simulation and validation activities have been carried out. The process aimed to evaluate both the suitability of the modeling approach and the models consistency and validity from an operational point of view.
The main Y2 validation activities progressed according to the Task 1.2 Model Validation activities described in D1.3. In particular, three different activities have been carried out:

- Phase 1 – Scoping of the models (M12-M16)
- Phase 2 - Models building (M17-M19)
- Phase 3 – Models validation (M20-M24)

The last year of the project will see WP1 stakeholders mainly involved in validating the decision-making tool, by means of live trials that will be held during the development of the tool.

The validation process has been informed and developed through a participatory approach where relevant stakeholders have been involved in presentation, discussion and iterative refinement of working and final versions of the models and the scenarios. Validation panels varied across validation phases and included Consortium Partners (Domain Experts and End-Users), Domain Stakeholders, Policy Makers (National Regulators and EU Organisations Representatives). Each phase made use of specific validation tools depending on the validation dimension and the type of selected validators.
Errore. L'origine riferimento non è stata trovata. below summarizes this process.

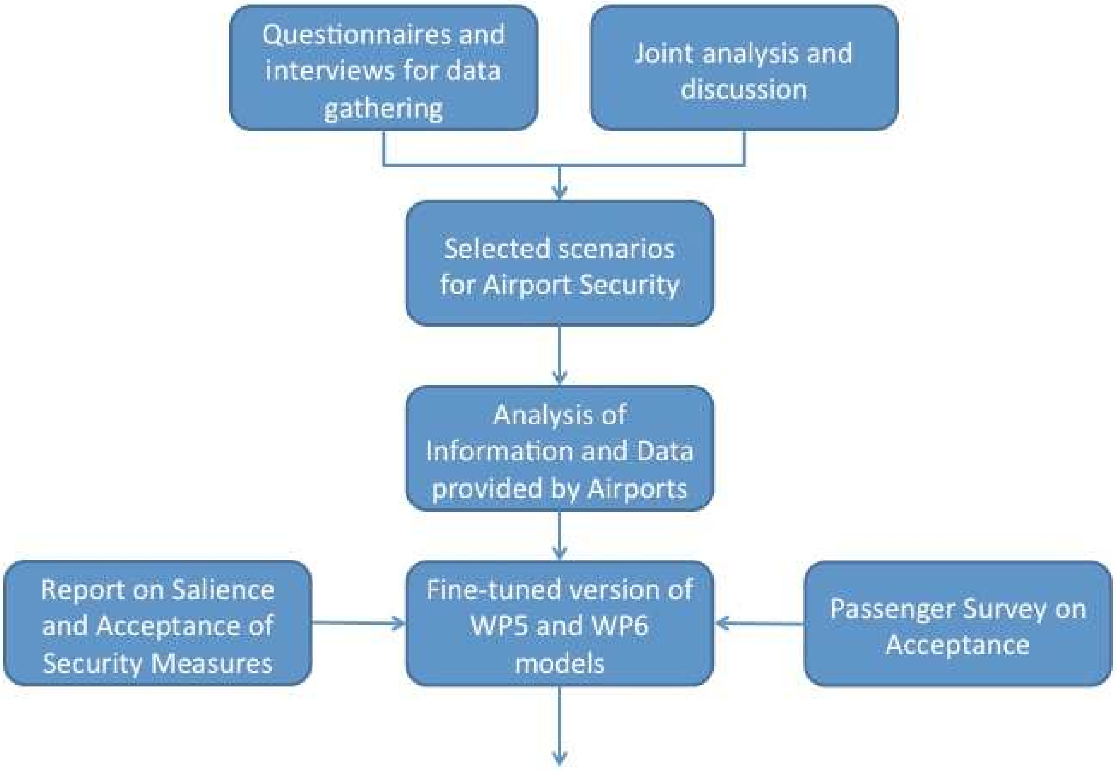

Questionnaires and interviews for data gathering
Joint analysis and discussion
Selected scenarios for Airport Security
Analysis of Information and Data provided by Airports
Report on Salience and Acceptance of Security Measures
Fine-tuned version of WP5 and WP6 models
Passenger Survey on Acceptance

Figure 1: Model Scoping Process (to be continued in Figure 5: Model Building Process)

Along Phase 1, WP1 has consolidated the Airport Security case study scenarios and provided support to WP5 and WP6 model development by mean of extensive data collection campaigns and direct stakeholders engagement and contribution (see description in Section 3). The final Airport Security scenarios leading model development are:

- The "Cyberthreat – Emerging Threat" scenario
- The "Attack to Tower" scenario
- The "Towards effective airport security regulations" scenario

See Section. 2.2 for the final Airport Security scenarios. As a continuation of Phase 1, Phase 2 saw stakeholders involvement in in-depth focused activities aiming at model finalization. The consolidation of the case study scenarios and the model building activities allowed the preparation of an Airport Security customized validation framework.

State-of-the-art validation methods, like the European Operational Concept Validation Methodology (E-OCVM) and Participatory & User Centred Design approach and techniques, have been applied in the Airport Security case study. In particular WP1 has integrated established methods into a customized framework for validating Security and ICT-oriented methods and models, according to what the D7.1 Validation Plan describes.
The high-level validation objectives defined across the three case studies were User Acceptability, Domain Suitability and Technical Usability. These objectives have been measured through their 'decomposition' into more measurable entities, thus leading to identification of various key validation criteria and indicators. Validation criteria are described in Section 4.

The scenario and model validation process has been structured within a comprehensive framework. Such framework encompassed the definition of a variety of validation activities, such as workshop activities with Airport Security managers and directors; expert judges with information and airport security experts; interviews with policy makers; online and on-site airport security questionnaires targeting passengers.
The integration among the different activities listed above resulted in a comprehensive and coherent evaluation of the airport security case study, to which WP4, WP5 and WP6 contributed on both contents and methodologies. See the validation results at Section.4.3.

Table 1 summarizes the Y2 Model validation activities.

Table 1: Year 2 Model Validation activities

Year 2 Model Validation Activites			
	PHASE 1	**PHASE 2**	**PHASE 3**
Duration	M12-M16	M17-M19	M20-M24
Objective	Scoping of Models	Models building	Models Validation

Involved Stakeholders	Technical Partners, Domain Experts	Consortium Partners, Technical Partners, Domain Experts	Airport Stakeholders, Policy Makers
Activities	Questionnaires on WP5 models (on IT infrastructure and Airport Security cost structure) Questionnaires and Interviews on WP6 model (on Airport Security decision making)	Questionnaires on WP5 models (on Cyberthreat countermeasure implementation maturity) Questionnaires and Interviews on WP6 model (on Security technology usage and costs) Airport Security Media Analysis (WP4 Prague Graduate School in Comparative Qualitative Analysis 2013) Istanbul Ataturk International Airport passenger survey Policy Makers presentation and feedback on intermediate model Focused travellers online survey	Validation Questionnaire Workshop in Falconara Airport Workshop in Anadolu Airport Focused Interviews Expert Judge Policy Makers presentation and feedback on final model Stakeholders Workshop

2. Model Scoping

WP5 and WP6 model scoping relied on the consolidation of Airport Security scenarios identified during Phase 1. This phase also prepared the Airport Security case study customized validation plan.

2.1 Consolidation of Scenarios

The high level policy and the operational airport security scenarios were described into details in D1.3 (i.e. the *Security Measures* scenario, the *Training of Airport Personnel* scenario and the *Unlawful Access to Tower* scenario). During the project lifecycle they have been modified according to stakeholders' needs and scientific WPs research interests. Two of them (i.e. the Security Measures scenario and the Unlawful access to tower) respectively evolved into the current "Towards effective airport security regulations" scenario (developed within WP6) and the "Attack to Tower" scenario (developed within WP5) as the scientific framework also matured reaching its final shape.

The *Training of Airport Personnel* scenario (see [1] as result) has been replaced by the *Cyberthreat – Emerging Threat scenario* developed WP5. The whole new Cyberthreat scenario and model specifically deals with this specific emerging threat in airport information security. The Cyberthreat – Emerging Threat scenario has been evaluated as of impact in the Airport Security domain since it envisions an information security attack that is widespread in many critical infrastructures and that could easily affect airport security in the near future.

2.1.1 Stakeholders engagement

Models have been presented and discussed with relevant stakeholders in the Airport Security domain, then refined iteratively by consortium partners.

Iterative meetings with two Security Instructors certified by the International Air Transport Association (IATA) have been organized to collect information to feed preliminary models versions, to steer and review the intermediate models provided by WP5 and WP6 partners, and to evaluate final versions of the models and discuss the results provided. A number of conference calls and phone interviews have been carried out with Operational and Security experts from Esjberg (DK), Brno (CZ) and Pescara (IT) Airports.

A cyber-security expert has been involved in the refinement and assessment of the Cyberthreat – Emerging Threat scenario modeled and analysed by WP5.

The following activities have been carried out during M13-M15 (see Table 1) in order to evaluate, evolve and, in one case, replace the high level policy and the operational Airport Security scenarios that are described in D1.3:

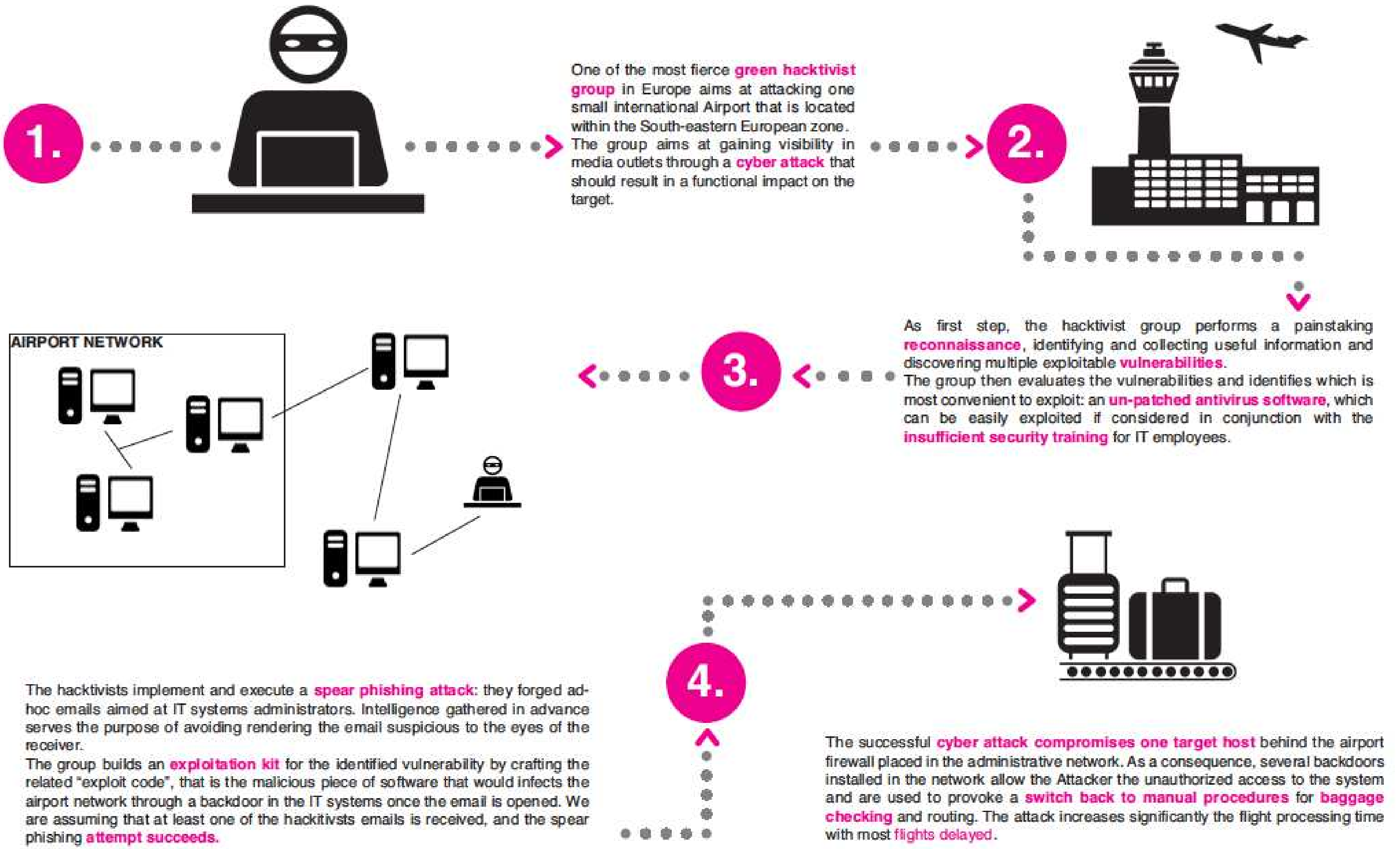
- Interview with one Civil Aviation Authority Security Instructors,
- Informal contact with ICT Airport Security Solution Industry,
- Questionnaires for Airport Security Managers (total of 22 Questionnaires sent, 10 Questionnaires back) (see Annex 1),
- Skype Interviews with Airport Security Managers (3 Interviews done).

Different techniques, like informal contacts, structured and focused interviews as well as multiple choices questionnaire are some of the techniques used to support the stakeholders' engagement in the validation process. The results of these activities have been analyzed and elaborated into the final Airport Security scenarios presented in the next section.

2.2 Airport Security Scenarios

This section includes the infographic representation of the Airport Security scenarios. The graphic visual representations of the scenarios help conveying complex information and data in a quick and clear way. The infographics were made necessary in order to effectively communicate the outputs of the project to the stakeholders and were used to facilitate both the discussion around the scenarios, and feedback collection about the models and their preliminary results.

Cyberthreat – Emerging Threat scenario



One of the most fierce green hacktivist group in Europe aims at attacking one small international Airport that is located within the South-eastern European zone. The group aims at gaining visibility in media outlets through a cyber attack that should result in a functional impact on the target.

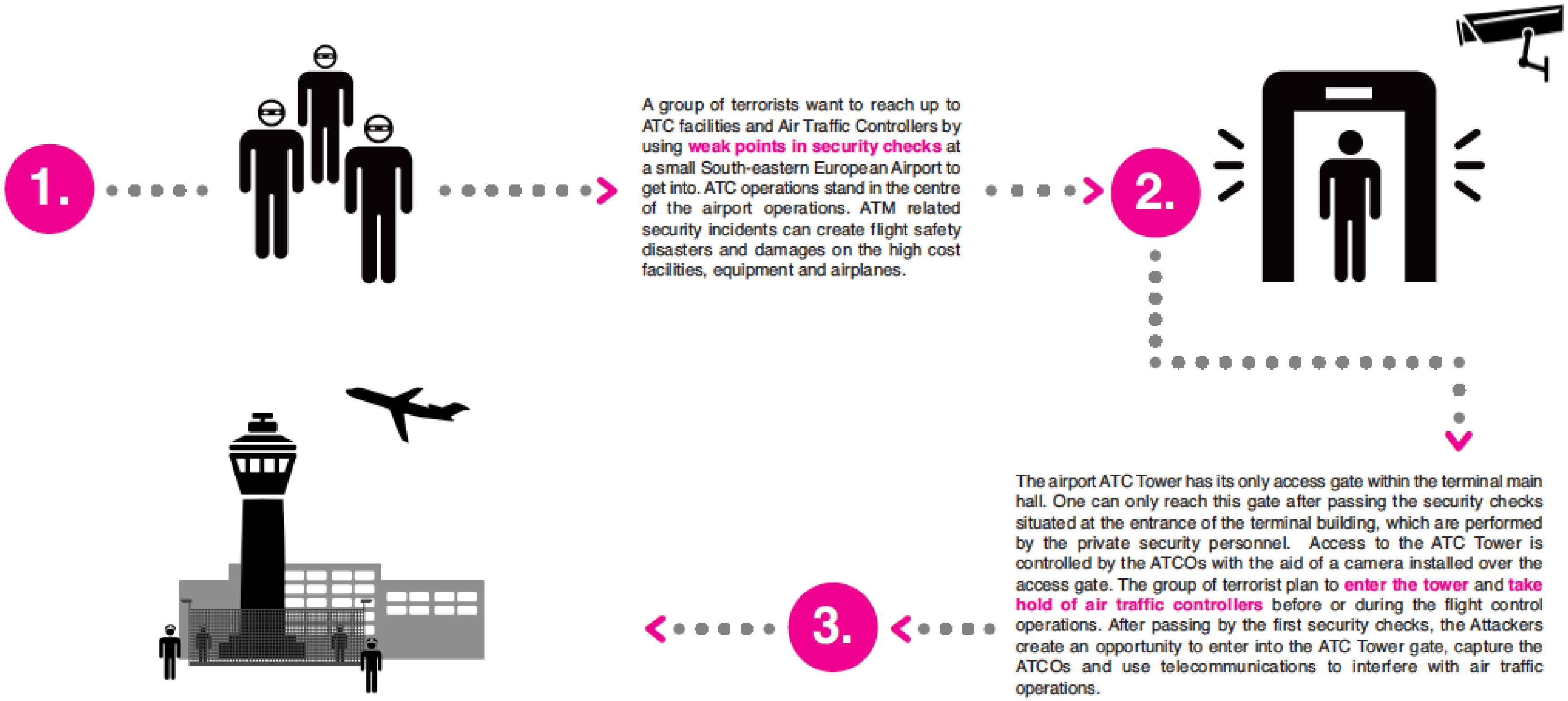
As first step, the hacktivist group performs a painstaking reconnaissance, identifying and collecting useful information and discovering multiple exploitable vulnerabilities. The group then evaluates the vulnerabilities and identifies which is most convenient to exploit: an un-patched antivirus software, which can be easily exploited if considered in conjunction with the insufficient security training for IT employees.

The hacktivists implement and execute a spear phishing attack: they forged ad-hoc emails aimed at IT systems administrators. Intelligence gathered in advance serves the purpose of avoiding rendering the email suspicious to the eyes of the receiver.
The group builds an exploitation kit for the identified vulnerability by crafting the related "exploit code", that is the malicious piece of software that would infects the airport network through a backdoor in the IT systems once the email is opened. We are assuming that at least one of the hackitivsts emails is received, and the spear phishing attempt succeeds.

The successful cyber attack compromises one target host behind the airport firewall placed in the administrative network. As a consequence, several backdoors installed in the network allow the Attacker the unauthorized access to the system and are used to provoke a switch back to manual procedures for baggage checking and routing. The attack increases significantly the flight processing time with most flights delayed.

Figure 2: Cyberthreat – Emerging Threat scenario

Attack to the Tower scenario



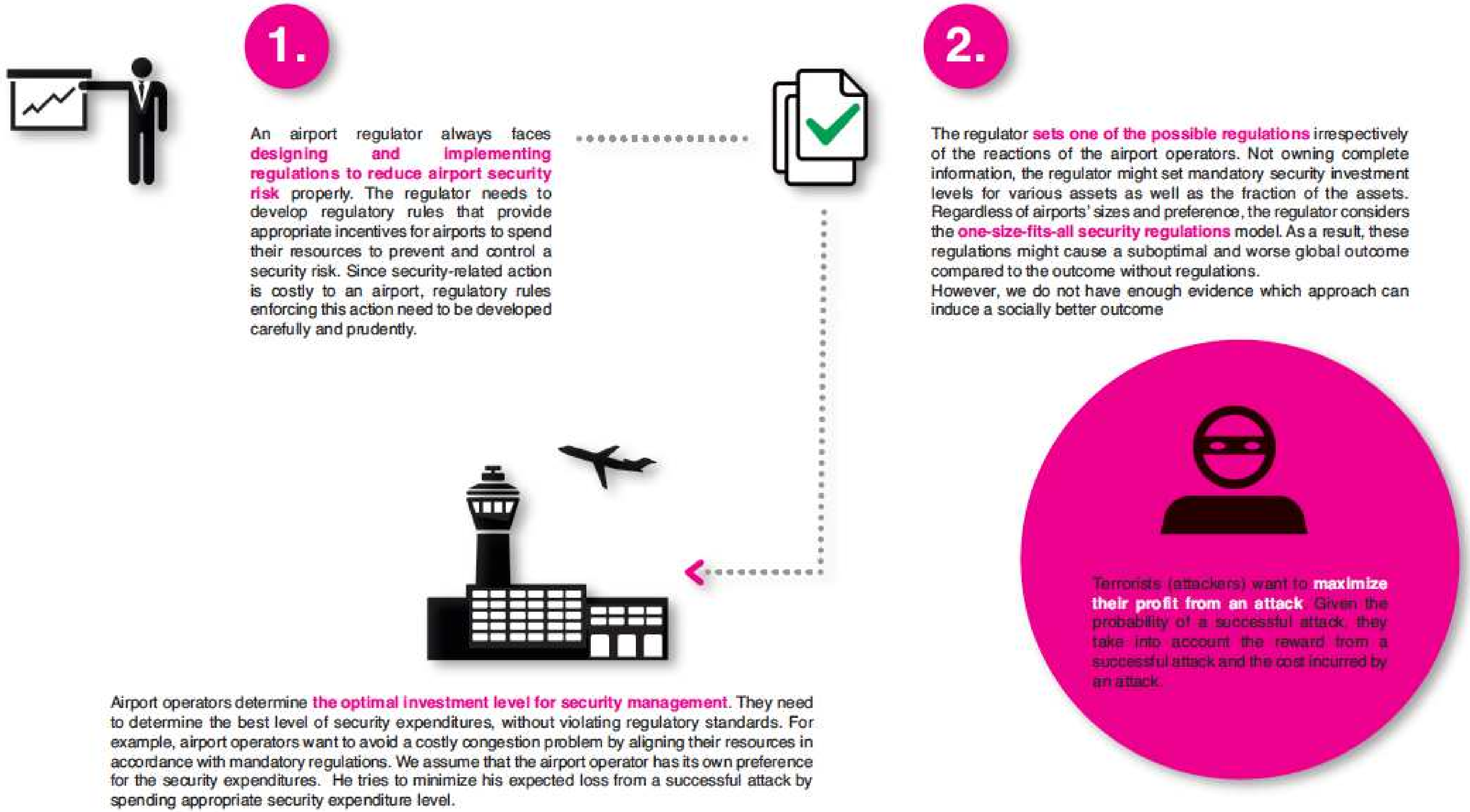
1. A group of terrorists want to reach up to ATC facilities and Air Traffic Controllers by using **weak points in security checks** at a small South-eastern European Airport to get into. ATC operations stand in the centre of the airport operations. ATM related security incidents can create flight safety disasters and damages on the high cost facilities, equipment and airplanes.

2. The airport ATC Tower has its only access gate within the terminal main hall. One can only reach this gate after passing the security checks situated at the entrance of the terminal building, which are performed by the private security personnel. Access to the ATC Tower is controlled by the ATCOs with the aid of a camera installed over the access gate. The group of terrorist plan to **enter the tower** and **take hold of air traffic controllers** before or during the flight control operations. After passing by the first security checks, the Attackers create an opportunity to enter into the ATC Tower gate, capture the ATCOs and use telecommunications to interfere with air traffic operations.

3. Main impacts of the attack will be crisis for air traffic operations in the air field and airspace. The **flight safety will be negatively affected** and air traffics should be diverted to the other ATC unit or air field. All flight operations are **cancelled or diverted** to alternative airfields. Beside the safety and security impacts the cancellation cost can be enormous with the connected national and international flights and airports/airspace.
Media will probably inform people immediately about the situation. This will cause new emergencies around the airport facilities and operators. Moreover, the situation will led to a **negative security perception for airport** users and could cause a decrease of air traffic in the short-term.

Figure 3: Attack to the Tower scenario

Towards Effective Airport Security Regulation scenario



1.

An airport regulator always faces **designing and implementing regulations to reduce airport security risk** properly. The regulator needs to develop regulatory rules that provide appropriate incentives for airports to spend their resources to prevent and control a security risk. Since security-related action is costly to an airport, regulatory rules enforcing this action need to be developed carefully and prudently.

2.

The regulator **sets one of the possible regulations** irrespectively of the reactions of the airport operators. Not owning complete information, the regulator might set mandatory security investment levels for various assets as well as the fraction of the assets. Regardless of airports' sizes and preference, the regulator considers the **one-size-fits-all security regulations** model. As a result, these regulations might cause a suboptimal and worse global outcome compared to the outcome without regulations.
However, we do not have enough evidence which approach can induce a socially better outcome

Terrorists (attackers) want to **maximize their profit from an attack**. Given the probability of a successful attack, they take into account the reward from a successful attack and the cost incurred by an attack.

Airport operators determine **the optimal investment level for security management**. They need to determine the best level of security expenditures, without violating regulatory standards. For example, airport operators want to avoid a costly congestion problem by aligning their resources in accordance with mandatory regulations. We assume that the airport operator has its own preference for the security expenditures. He tries to minimize his expected loss from a successful attack by spending appropriate security expenditure level.

Figure 4: Towards effective airport security regulation scenario

3. Model Building

In parallel with scenario consolidation, an extensive data gathering campaign has been conducted across Phase 1 (M12-16) and Phase 2 (M12-M19) (see Table 1) with the aim of supporting WP5 and WP6 model development, respectively Cyberthreat and Attack to Tower, and Towards effective security measure selection.
Figure 5 below summarizes this process.

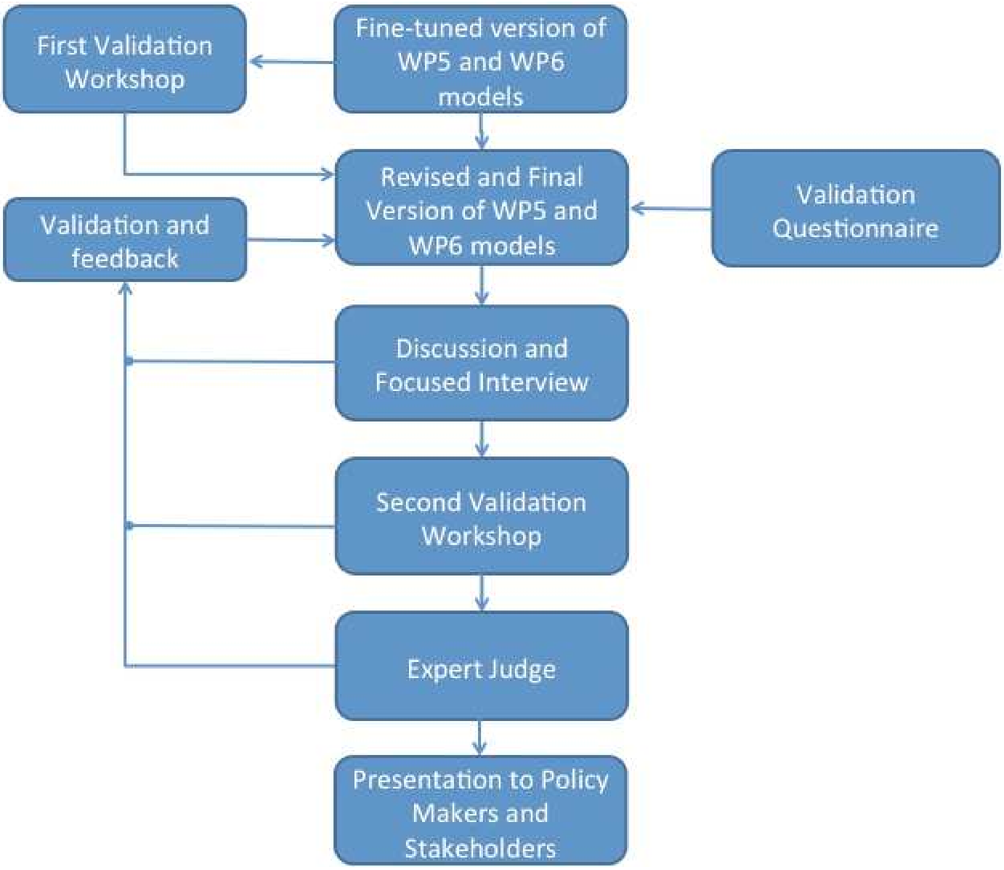

First Validation Workshop
Fine-tuned version of WP5 and WP6 models
Revised and Final Version of WP5 and WP6 models
Validation Questionnaire
Validation and feedback
Discussion and Focused Interview
Second Validation Workshop
Expert Judge
Presentation to Policy Makers and Stakeholders

Figure 5: Model Building Process

3.1 WP5 models

The airport in AU has been firstly targeted for repeated investigations about its security infrastructure and cost structure (see Annex 2). Inputs provided by AU have been reviewed by DBL in order to inform the development of the Unlawful Attack to Tower Model finalised by URJC.
By mean of dedicated questionnaires, the second round of data collection allowed WP1 to focus on AA IT Infrastructure (see Annex 3) and on the maturity of AA cyberthreat countermeasure (Annex 4). Inputs provided by them informed the development of the preliminary version of the Cyberthreat model by URJC [2].
Additional interviews with Falconara and Esbjerg Airport Security Managers allowed WP1 to evaluate specific aspects of the models (see Annex 5 for the interview script).

3.2 WP6 models

Baggage and passenger screeening devices have been targeted by questionnaires administered to AA, Esbjerg Airport and Ancona-Falconara Airport (Annex 6). This activity allowed to gather information and data about screening devices costs and performance that constituted the parameter inputs to the CBA model for the Airport Security Measures model proposed by UNITN.

Contacts with X-Ray Machine, Metal Detector, Body Scanners vendors have been also realized to assure the validity of the data gathered through field investigation.

Questionnaires and focused interviews with Civil Aviation Authority Security Instructors have also carried out in order to contribute to the Airport Security Training context description, comparison and evaluation as joint action with UNITN (see Annex 7).

Further opportunities to present, discuss and foster the development of the intermediate versions of both WP5 and WP6 models were provided in the meetings with policy makers and decision makers at national (i.e. Ente Nazionale per l'Aviazione Civile – ENAC, the Italian CAA) and international levels (i.e. Eurocontrol and the Airport Council International - ACI Europe) (see Annex 8 for the questionnaires used to gather feedback).

3.3 WP4 contribution to Airport Security models

The investigation of social aspects of WP5 and WP6 models was supported by a variety of activities: the media analysis about the 3D body scanner held as one of the case study of the Prague Graduate School in Comparative Qualitative Analysis 2013 (see D4.4 – Discourses and Justification of Security and Risk for further details); the Istanbul Ataturk International Airport passenger survey (see D4.3 – Communication patterns and effective channels of communication for further details); and the focused traveller online survey.

The focused traveller online survey (M24) has been designed on the basis of the Istanbul Ataturk International Airport passenger survey administered by AU during the Models' Finalization phase. The online survey consisted of a reduced and adapted version of the full passenger survey with the aim of focusing on Acceptance of Security Measures by Airport Passengers (See Annex 11 for the online survey).

The following traveller forums have been selected, from the most popular, e.g. LonelyPlanet forums, to the most specialised, e.g.:

- TravelTalk Travel Safety/Security > Checkpoints and Borders Policy Debate traveltalk.com
- Travel Buddy travbuddy.com
- Travel Blog travelblog.org
- Forum Viaggiatori forumviaggiatori.com
- Selected LinkedIn and Facebook groups, including:
    - Airport Security – AVSEC
    - Aviation & Aerospace Professionals
    - World Travellers
    - Aviation Professionals

Personal and company business contacts have also been targeted by the survey (e.g. company contact list, frequent flyers, holiday travellers).

The survey has reached 287 responses from all over the world in 45 days of online publication.

3.4 Final version of Airport Security Models

In the following paragraphs the infographics showing the final versions of the models and their results are presented. This deliverable only presents a limited description of the models. Please refer to D5.2 - Case Studies in Security Risk Analysis and D6.3 - Law and Economics for a full and comprehensive description of respectively WP5 and WP6 models.

3.4.1 WP5 Models

The Adversarial Risk Analysis (ARA) modeling approach (see D5.1 - Basic Models for Security Risk Analysis for details) is used for WP5 models: Cyberthreat – Emerging Threat [2] and Attack to tower [4] (see D5.2 Case studies in security risk analysis). According to the ARA approach, two intelligent adversaries' (the Defender and the Attacker) decisions and actions are modeled. The utility functions, aggregating all relevant information about costs, revenues, payoffs, etc, are used with the goal of modeling each adversary's preferences and utilities.

Utility functions are built from the costs and revenues relevant for each actor. The additional feature of utility functions is that they can reflect the attitude of the adversaries towards risk. It is important to note that in the revenue function also not monetary rewards can be included (e.g., for the Cyberthreat – Emerging Threat scenario, the revenues in terms of fame, recognition among peers, etc. are considered).

Both adversaries are expected utility maximizers, i.e. they both will try to obtain the maximum profit from their actions, making the corresponding decision.

The final output of the model will be to give advice to airport authorities for devising a security plan, i.e. providing them with an optimal portfolio of defensive measures.

Cyberthreat – Emerging Threat Model

The Cyberthreat – Emerging Threat model is developed through the following high-level steps:

1. the **Attacker's problem** solution: the attacker evaluates all the possible defensive measures that the Defender could deploy and evaluate the most convenient attack (by mean of calculating its own utility function) to him, choosen among a pre-defined set of attack varying along times of completion and probability of success. The Attacker Utility function depends on both the benefits he or she may get from a successful attack and the costs entailed to implement him/her decision.

   Attacker's main actions are:

   - Reconnaissance
   - Weaponize
   - Cyber attack execution

   The Attacker must accomplish successfully all the three identified attack steps for the overall attack to be successful. The attack phases are incremental, i.e. they build one upon the other; and the presented model assumes that the Attacker will execute them only once.

2. the **Defender's problem** solution: given all possible attacks that the Attacker may perform according to certain probabilities of being launched, calculated on the attacker problem, the defender has to maximize its expected utility.
   Defender's main actions are:
   - Implement the five security control areas (governance and people, policy, processes, procedures, technical controls),
   - Execute continuous monitoring, periodic analysis, audit and update
   - Deploy incident response[1]

The costs have been estimated on the profile of a South-eastern Europe small-size international airport, with an average budget of 2-3 M€ per year, with around 5% of the total budget spent on security and hosting less than 10 flight connections per day.
The probability of success for each attack action is a function of the 'effectiveness' of the defense measures and of the money and effort invested by the Attacker. The effectiveness of a security measure, in the context of this research, is the product of its maturity and its relevance.
The main source of uncertainty for the Defender is how well trained and skilled are the attackers, and how much do they know about the weak points of airport's IT infrastructure and organization: skilled terrorists will need less resources and time to perpetrate a cyber-attack than do inexperienced ones.

As preliminary results of the model we can summarize that:

- When the attack is perpetrated by highly skilled groups (case 1), the defender will tend to invest on the most effective measures, although they are also the most expensive ones, and this fact prevents the defender from investing in other cheaper but less effective areas;
- When the cyber-terrorist threat is not so high, because of the inexperience of the attacking group (case 2), airport authorities would tend to invest in more measures, aiming at covering as many control areas as possible, although not necessarily investing in the most effective ones.

A full representation of the Cyberthreat – Emerging Threat model and its preliminary results is provided by Figure 4 and Figure 5.

Attack to Tower Model

The Attack to Tower model sees the airport authorities first deploying a set of preventive measures to protect, among other targets, the access to the ATC Tower. The Attacker, who observes such measures, will decide on whether or not to launch an attack. The Attacker may consider different severity options for the attack, which will be modeled through the number of terrorists taking part in the attack.
Finally, should an attack be successful, airport authorities will try to recover from it and minimize its consequences by deploying additional measures, which in our case will imply calling the Special Police Force. There is actually no decision associated to it but,

[1] 'Deploy incident response' is not included in the first version of the model. It will be included in further developments of the model.

rather, an automatic response: in case of a successful attack, the Special Police Force will be immediately called on. The defender's actions will then consist in:

- Defining a portfolio of security measures aiming at improving the detection capability of prohibited things/suspicious people and a deterrence for potential attacks,
- Managing a possible attack by terrorists and supporting the request from the special police,
- Handling the consequences of a possible attack and performing the recovery actions subsequent to the police intervention.

No additional resources will be summoned if the attack fails, since we assume, in that case, that the terrorists have been killed or detained by ordinary police and/or private security personnel or, eventually, some of them managed to escape.

The preliminary results of the model show that, considering three possible conditions (i.e. low, medium and high traffic level), which are representative of the usual activity at the incumbent airport, under the scenario of an airport which will incur in big losses if a terrorist attack occurs, the terrorists would behave in the following manner:

- They tend to be cautious when they see that the defensive measures are too intense, typically choosing attacking with, at most, only one terrorist;
- Otherwise, if they feel that the ATC Tower is vulnerable they would launch the most powerful attack they can;
- Only in case of doubt, when they do not perceive with clarity any of the situations mentioned above, they would opt for an intermediate strategy, sending between two to four attackers.

However, should the terrorists feel that the damages inflicted to the airport will not be so considerable, their strategy would radically change. Although they are considered as risk seekers, they also put a certain value to their lives and, therefore, they will not put themselves in unnecessary risk if the chances of causing spread and costly damages to airport authorities are reduced.

3.4.2 WP6 Model

Please refer to D6.3 - Law and Economics for a full and comprehensive description of the WP6 model.

The model on "Towards Effective Security Regulations" applies a Law and Economics approach and focuses particularly on identifying socially optimal combinations of security regulatory mechanisms (i.e., customized vs. uniform) and financial rules (i.e., centralized vs. decentralized) for different types of aviation networks (see ANNEX 1 in D6.3). The model incorporates security interdependence between airports as well as different airport types in the airport network configurations. In detail, relying on an approach of Public and Political Economics, the model analysed different combinations of regulatory and financing mechanisms, and compared the trade-offs between these mechanisms. Using a comparative static anaylsis (see D6.3 for more details), the model identified how the relative performance of different regulatory and financing rules changes with the different characteristics of the aviation network and interdependence. In sum, the model provides an insight on what a regulator should do to design regulatory and financing standards to produce an outcome close to social optimum.

In the model, the exemplar case of a country with two airports (either identical or heterogeneous) and a regulator (who is a benevolent social planner and tries to maximize the social welfare) was considered, while the model could be extended to include n airports with the same line of reasoning. The country was assumed to select a different combination of regulatory and financing structures with respect to airport security (see Table 2 below). The regulator may use one of the four mechanisms, or a uniform or customized regulation with the combination of centralized and decentralized financing systems.

Table 2: Regulatory structures & financing systems: A heterogeneous airport case.

		Financing Systems	
Regulatory Structures		CENTRALIZED	DECENTRALIZED
	UNIFORM	Uniform / Centralized	Uniform / Decentralized
	CUSTOMIZED	Customized / Centralized	Customized / Decentralized

In designing an economic model, we considered an individual expected loss function of an airport and an aggregated expected loss function for the regulator. The expected loss functions were designed to encompass various factors including the airport's security preference, potential losses from a successful attack and the degree of security externality. The functions were also developed to be able to take into account different aviation network configurations with respect to the ownership (i.e., publicly or privately owned). The airports were assumed to be:

- a profit maximizer if the airport is private.
- a social welfare maximizer if the airport is public.

A political economics modeling approach was used to solve a problem: the regulator sets financial and regulatory rules as a first mover, and airports that stochastically experience a security accident make corresponding defensive effort in response to the rules. Solving a problem gives the optimal regulatory and financing mechanisms for different aviation network configurations: the solutions describe the outcomes produced by different regulatory and financing mechanisms and how the regulator can design a security rule that can produce a socially optimal outcome (or at least an outcome close to the social optimum).

In order to provide further insight into airport security rules, we conducted an illustrative analysis with a fully specified setup. In the analysis, it was assumed that there are one big private airport and one medium-sized public airport with either private or public ownership. The following two cases were further defined:

- A regulatory rule is fixed to be either customized or uniform, and the regulator can only determine which financing mechanism (i.e., decentralized, centralized or the combination) to be used; or

- A financing mechanism is fixed and the regulator can only determine whether he will choose a customized or uniform regulatory rule.

In the illustration process, we made realistic assumptions with respect to the parameters required for the analysis, and collected the related information on the parameters. As for the airports, the following assumptions were made:

- Security expenditures: each airport makes a particular security spending based on the number of passengers.
- Security preference: each airport has different security preference for security protection (e.g. depending on the number of passengers).
- Externalities: The security level of one airport is determined not only by its own security investment but also by the investment of other airports. For example, if the externality is absent, airports are not affected by security conditions of other airports; if the externality is maximal, airport security is equally determined by security conditions of all airports.
- Probability of a successful attack: it depends on the level of security expenditures and the number of passengers.

As for the regulators, we made assumption for the following parameters:

- Security charges: the regulator can determine which security funding mechanism the government will use. He has three options:
    - Only airport security charges: all of the security expenditures are funded by the airport. We call this as "Decentralized Financing System"
    - Only state security charges: security spending is funded by the government. We call this as "Centralized Financing System"
    - The combination of two financing systems
- Regulatory rules: the regulator can used either customized or uniform (i.e., one-size-fits-all) regulation that mandates a certain level of security expenditures.

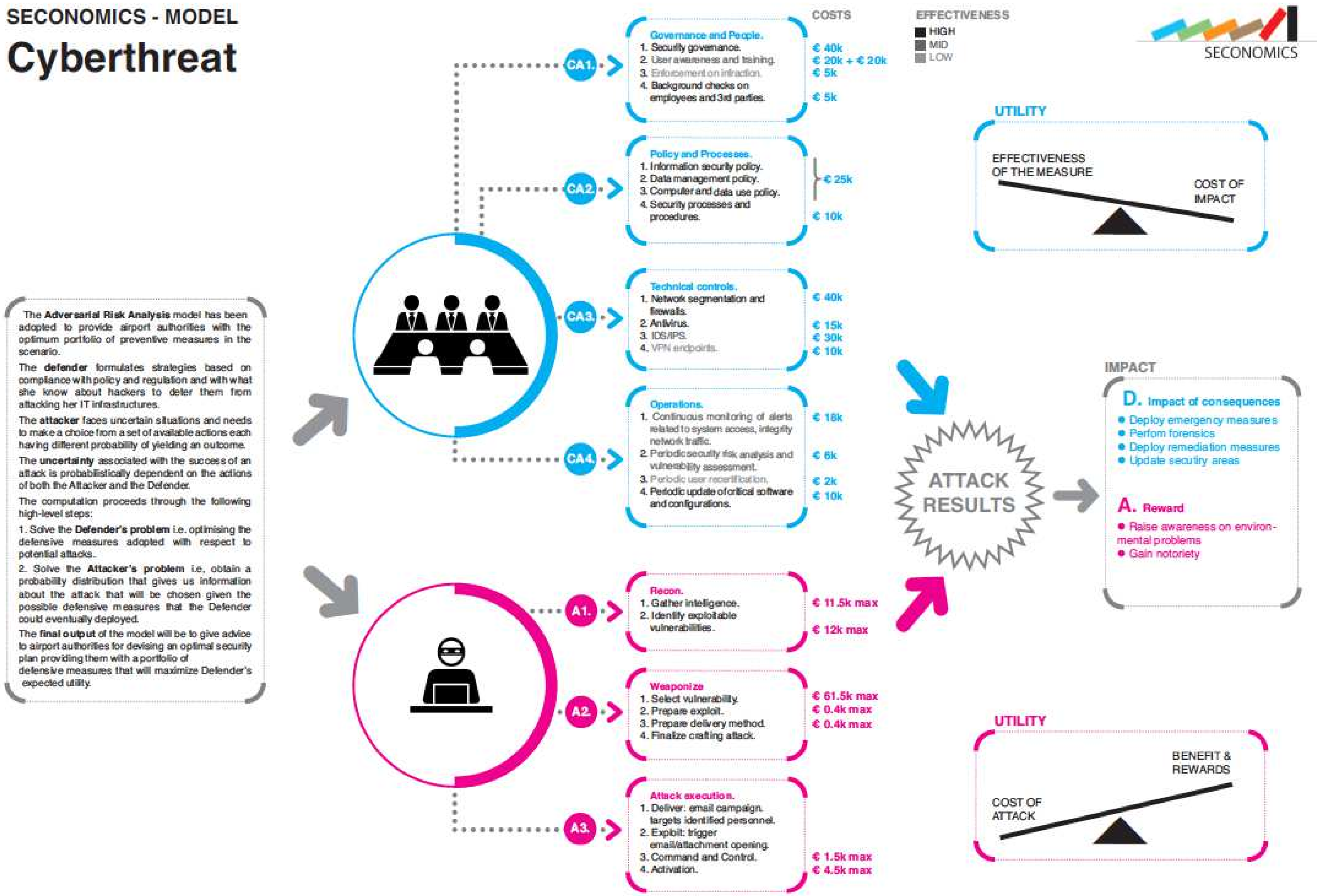
Based on the information from various sources, we estimated the values of the parameters and used them in the analysis.

The results of both theoretical and illustrative analyses provided various useful implications, including:

- The outcome of a specific combination of regulatory and financing rule depends on the interdependence between the airports. Specifically,
    - If the interdependence is low, decentralized financing with a customized regulation can provide a socially better outcome than other mixes of the mechanisms.
    - However, if the interdependence is high, a customized regulation might produce a socially worse outcome than a uniform regulation.
- Combining centralized and decentralized financing schemes would be better for obtaining a socially optimal outcome than relying solely on one of the financing schemes.

It is clear from the results that the model can provide information on whether a particular security regulatory and financing setting can induce socially optimal expenditures of the airports, and what the optimal setting under a certain condition is. The results of the model will be able to be used by the regulator in designing an optimal mix of regulatory and financing rules (e.g., selection of appropriate portfolio and optimal compliance level) and in developing new regulatory and financing strategies.

It should be noted that WP6 model aligns well with WP5 model: WP6 model provides information on a certain amount of money that should be mandated to be spent by an airport to achieve an optimal outcome, whereas WP5 model addresses an issue regarding how such an amount of money can be allocated optimally to employ different security measures in an airport.



SECONOMICS - MODEL

Cyberthreat

The **Adversarial Risk Analysis** model has been adopted to provide airport authorities with the optimum portfolio of preventive measures in the scenario.

The **defender** formulates strategies based on compliance with policy and regulation and with what she know about hackers to deter them from attacking her IT infrastructures.

The **attacker** faces uncertain situations and needs to make a choice from a set of available actions each having different probability of yielding an outcome.

The **uncertainty** associated with the success of an attack is probabilistically dependent on the actions of both the Attacker and the Defender.

The computation proceeds through the following high-level steps:

1. Solve the **Defender's problem** i.e. optimising the defensive measures adopted with respect to potential attacks.
2. Solve the **Attacker's problem** i.e, obtain a probability distribution that gives us information about the attack that will be chosen given the possible defensive measures that the Defender could eventually deployed.

The **final output** of the model will be to give advice to airport authorities for devising an optimal security plan providing them with a portfolio of defensive measures that will maximize Defender's expected utility.

		COSTS
CA1.	**Governance and People.**	
	1. Security governance.	€ 40k
	2. User awareness and training.	€ 20k + € 20k
	3. Enforcement on infraction.	€ 5k
	4. Background checks on employees and 3rd parties.	€ 5k
CA2.	**Policy and Processes.**	
	1. Information security policy.	€ 25k
	2. Data management policy.	
	3. Computer and data use policy.	
	4. Security processes and procedures.	€ 10k
CA3.	**Technical controls.**	
	1. Network segmentation and firewalls.	€ 40k
	2. Antivirus.	€ 15k
	3. IDS/IPS.	€ 30k
	4. VPN endpoints.	€ 10k
CA4.	**Operations.**	
	1. Continuous monitoring of alerts related to system access, integrity network traffic.	€ 18k
	2. Periodic security risk analysis and vulnerability assessment.	€ 6k
	3. Periodic user recertification.	€ 2k
	4. Periodic update of critical software and configurations.	€ 10k
A1.	**Recon.**	
	1. Gather intelligence.	€ 11.5k max
	2. Identify exploitable vulnerabilities.	€ 12k max
A2.	**Weaponize**	
	1. Select vulnerability.	€ 61.5k max
	2. Prepare exploit.	€ 0.4k max
	3. Prepare delivery method.	€ 0.4k max
	4. Finalize crafting attack.	
A3.	**Attack execution.**	
	1. Deliver: email campaign. targets identified personnel.	
	2. Exploit: trigger email/attachment opening.	
	3. Command and Control.	€ 1.5k max
	4. Activation.	€ 4.5k max

EFFECTIVENESS

■	HIGH
■	MID
■	LOW

IMPACT

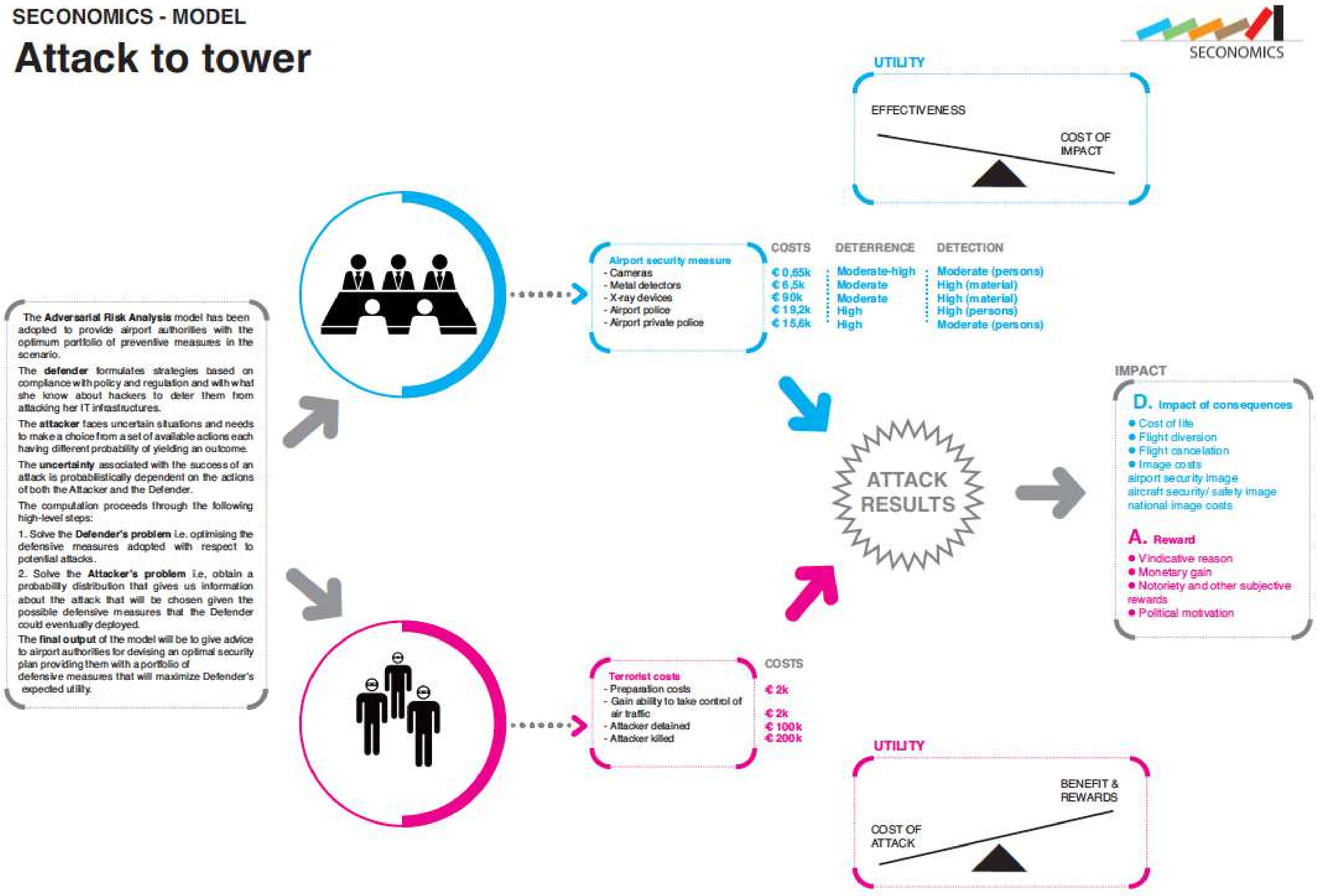
D. Impact of consequences

- Deploy emergency measures
- Perfom forensics
- Deploy remediation measures
- Update secutiry areas

A. Reward

- Raise awareness on environmental problems
- Gain notoriety

Figure 6: Cyberthreat Model



SECONOMICS - MODEL

Attack to tower

The **Adversarial Risk Analysis** model has been adopted to provide airport authorities with the optimum portfolio of preventive measures in the scenario.

The **defender** formulates strategies based on compliance with policy and regulation and with what she know about hackers to deter them from attacking her IT infrastructures.

The **attacker** faces uncertain situations and needs to make a choice from a set of available actions each having different probability of yielding an outcome.

The **uncertainty** associated with the success of an attack is probabilistically dependent on the actions of both the Attacker and the Defender.

The computation proceeds through the following high-level steps:

1. Solve the **Defender's problem** i.e. optimising the defensive measures adopted with respect to potential attacks.

2. Solve the **Attacker's problem** i.e, obtain a probability distribution that gives us information about the attack that will be chosen given the possible defensive measures that the Defender could eventually deployed.

The **final output** of the model will be to give advice to airport authorities for devising an optimal security plan providing them with a portfolio of defensive measures that will maximize Defender's expected utility.

Airport security measure	COSTS	DETERRENCE	DETECTION
- Cameras	€ 0,65k	Moderate-high	Moderate (persons)
- Metal detectors	€ 6,5k	Moderate	High (material)
- X-ray devices	€ 90k	Moderate	High (material)
- Airport police	€ 19,2k	High	High (persons)
- Airport private police	€ 15,6k	High	Moderate (persons)

Terrorist costs	COSTS
- Preparation costs	€ 2k
- Gain ability to take control of air traffic	€ 2k
- Attacker detained	€ 100k
- Attacker killed	€ 200k

IMPACT

D. Impact of consequences

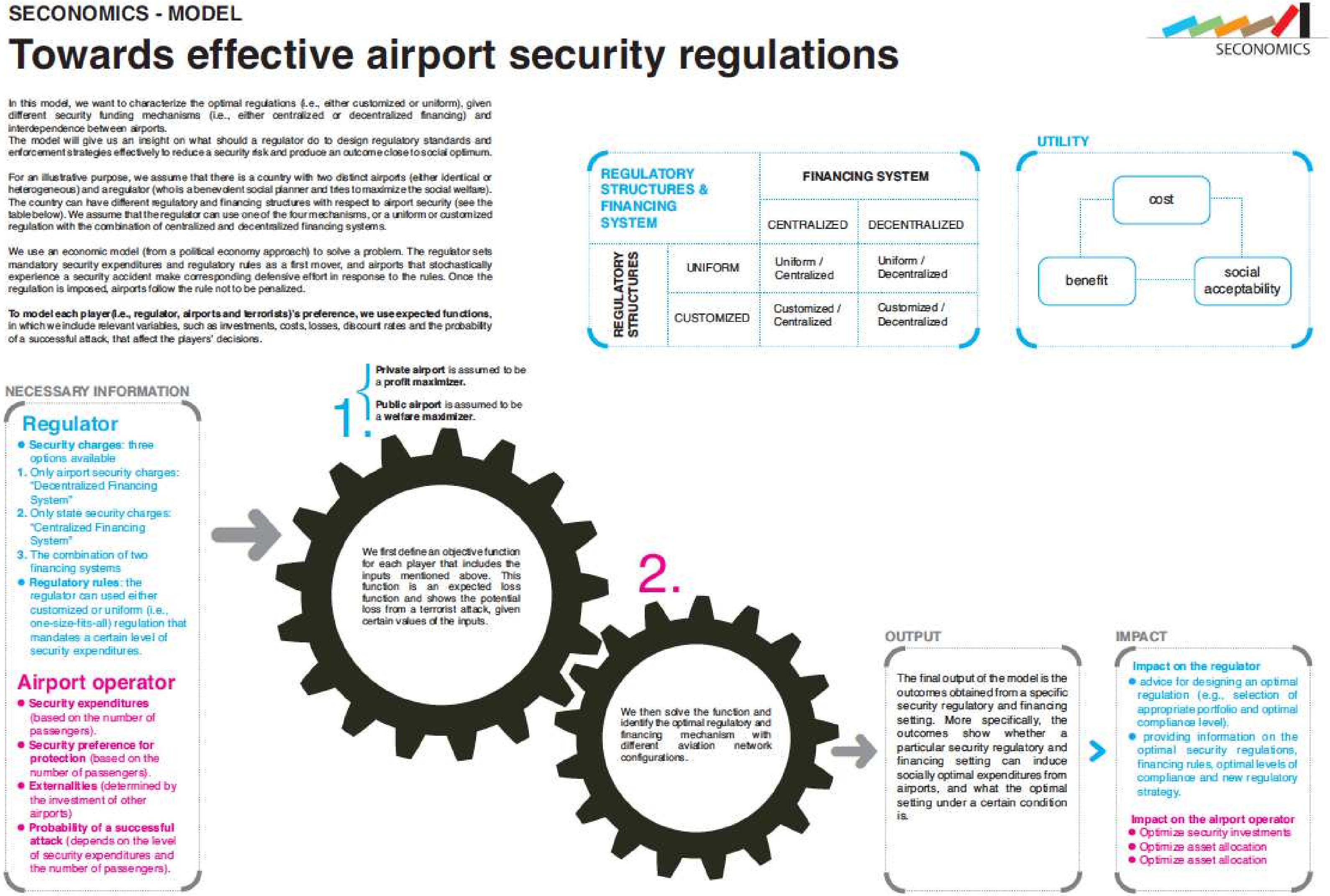
- Cost of life
- Flight diversion
- Flight cancelation
- Image costs

airport security image
aircraft security/ safety image
national image costs

A. Reward

- Vindicative reason
- Monetary gain
- Notoriety and other subjective rewards
- Political motivation

Figure 7: Attack to tower Model



SECONOMICS - MODEL

Towards effective airport security regulations

SECONOMICS

In this model, we want to characterize the optimal regulations (i.e., either customized or uniform), given different security funding mechanisms (i.e., either centralized or decentralized financing) and interdependence between airports.
The model will give us an insight on what should a regulator do to design regulatory standards and enforcement strategies effectively to reduce a security risk and produce an outcome close to social optimum.

For an illustrative purpose, we assume that there is a country with two distinct airports (either identical or heterogeneous) and a regulator (who is a benevolent social planner and tries to maximize the social welfare). The country can have different regulatory and financing structures with respect to airport security (see the table below). We assume that the regulator can use one of the four mechanisms, or a uniform or customized regulation with the combination of centralized and decentralized financing systems.

We use an economic model (from a political economy approach) to solve a problem. The regulator sets mandatory security expenditures and regulatory rules as a first mover, and airports that stochastically experience a security accident make corresponding defensive effort in response to the rules. Once the regulation is imposed, airports follow the rule not to be penalized.

To model each player (i.e., regulator, airports and terrorists)'s preference, we use expected functions, in which we include relevant variables, such as investments, costs, losses, discount rates and the probability of a successful attack, that affect the players' decisions.

REGULATORY STRUCTURES & FINANCING SYSTEM		FINANCING SYSTEM	
		CENTRALIZED	DECENTRALIZED
REGULATORY STRUCTURES	UNIFORM	Uniform / Centralized	Uniform / Decentralized
	CUSTOMIZED	Customized / Centralized	Customized / Decentralized

UTILITY

NECESSARY INFORMATION

Regulator

- **Security charges**: three options available
1. Only airport security charges: "Decentralized Financing System"
2. Only state security charges: "Centralized Financing System"
3. The combination of two financing systems
- **Regulatory rules**: the regulator can used either customized or uniform (i.e., one-size-fits-all) regulation that mandates a certain level of security expenditures.

Airport operator

- **Security expenditures** (based on the number of passengers).
- **Security preference for protection** (based on the number of passengers).
- **Externalities** (determined by the investment of other airports)
- **Probability of a successful attack** (depends on the level of security expenditures and the number of passengers).

1.

Private airport is assumed to be a **profit maximizer.**

Public airport is assumed to be a **welfare maximizer.**

We first define an objective function for each player that includes the inputs mentioned above. This function is an expected loss function and shows the potential loss from a terrorist attack, given certain values of the inputs.

2.

We then solve the function and identify the optimal regulatovy and financing mechanism with different aviation network configurations.

OUTPUT

The final output of the model is the outcomes obtained from a specific security regulatory and financing setting. More specifically, the outcomes show whether a particular security regulatory and financing setting can induce socially optimal expenditures from airports, and what the optimal setting under a certain condition is.

IMPACT

Impact on the regulator

- advice for designing an optimal regulation (e.g., selection of appropriate portfolio and optimal compliance level),
- providing information on the optimal security regulations, financing rules, optimal levels of compliance and new regulatory strategy.

Impact on the airport operator

- Optimize security investments
- Optimize asset allocation
- Optimize asset allocation

Figure 8: Attack to tower Mod

4. Airport Security Model Validation

Section 4 describes the validation framework for the Airport Security case study, and the details of the validation criteria defined, as well as the main validation activities that have been carried out and the results. Within the Airport Security case study validation process, the following issues have been targeted:

a. Stakeholders' decision making
b. Models' structure and computational mechanisms
c. Models' results
d. Models' generalization and customization

First issue (a) has been targeted in the validation since the analysis of the current decision-making processes provides a reference knowledge base for evaluating whether the model overarching reasoning mechanism does suit with the domain requirements. Validation of the other three issues, (b), (c) and (d), directly aims at disentangling the models' structure and main components, capability to being generalized and quality of the outputs.

The instruments that have been administered during the validation process (i.e. questionnaires, inverview questions, expert judgement schema) are presented as annexes of the Deliverable (see Annexes 1-12).

4.1 Validation Criteria

The Airport security validation framework stems out from a critical review and integration of the following validation methodologies: the Method Evaluation Model (MEM) [5], the Technology Acceptance Model (TAM) [6][7], the European Operational Concept Validation Methodology (E-OCVM) [8], user-centred evaluation methodologies, like cognitive walkthrough and expert judge.

Differently from the validation of technology, the objective of models' validation should not be to demonstrate that the method is right but rather to demonstrate of being effective on the pragmatic level. The development of a customized framework has been made necessary since models and methods have basically a pragmatic value, i.e. can only be effective or ineffective on the basis of applicative success in practice.

Subjective and objective measures of the validation objectives stated in D7.1 (i.e. User acceptability, Domain suitability and Technical usability) have been selected within the validation framework in order to assure a comprehensive assessment of the models. Among the subjective measures, the perceived efficacy based on perceived ease of use and perceived usefulness, the perceived effectiveness based on the quality of results [6][7] and the technical soundness are considered. Among the objective measures, the technical usability components, like memorability, efficiency and reusability have been included.

See Table 3 for an overview of the validation criteria adopted.

Table 3: Validation Criteria

TARGET	VALIDATION OBJECTIVES & CRITERIA		
	User Acceptability	**Domain Suitability**	**Technical Usability**
a. Stakeholders' decision making		- Resilience - Domain scoping - Content and completeness of information - Coverage of Airport Security DM	
b. Models' structure and computational mechanisms	- Perceived ease of use and perceived usefulness (-> Perceived Efficacy) - Perceived enjoyment - Human effort (at least equivalent to manual) - Scalability - Technical and scientific soundness (Automation, Reducing complexity, Increasing knowledge, Predictability) - Trust	- Applicability - Human effort - Domain scoping - System functionalities - Analyzability (Suitability of the reasoning techniques) - Coverage of Airport Security DM	- Efficiency - Understandability (also referred to as Comprehensibility) - Memorability
d. Models' Output	- Quality of the results (-> Perceived Effectiveness) - Perceived ease of use and perceived usefulness (-> Perceived Efficacy) - Perceived enjoyment - Human effort (to be at least equivalent to manual)		- Efficiency - Understandability (also referred to as Comprehensibility) - Memorability
d. Models' generalization and customization		- In-situ applicability (Conditions and factors for the specific airport environment&logistics and work practices) - Compliance with regulations and procedures	- Reusability

4.2 Validation Activities

Validation Questionnaire (M20 – M24)

A comprehensive questionnaire has been defined as validation support instrument to investigate the validation objectives described in Table 3 and assess each model[2] towards such criteria. See Annex 9 for details of the questionnaire.

The validation support questionnaire has been administered to:

- Falconara Airport Workshop participants,
- Anadolu Airport Workshop participants,
- Experts involved in the expert judge,
- Anadolu Stakeholders Workshop participants,

for a total of 32 questionnaires. See Annex 12 for the full tables of results related to the Cyberthreat, the Attack to tower and the Towards effective security measure regulation models.

Workshop in Falconara Airport – Management and Security Board (M20)

The Validation Workshop at Falconara Airport has been held on 16th and 17th September 2013.

Within the broader scope of evaluating the potentials of the SECONOMICS outputs towards the functional and security requirements featuring the airport security decision-making, the specific objectives of the Workshop were:

- To present the SECONOMICS Project, its research objectives and the ongoing results (M20 progress) to airport security stakeholders,
- To discuss and validate the first version of the models for airport security decision making developed within the Project.

Together with Falconara Airport personnel, partners from DBL and UNITN participated into the event as airport security case study responsible.

A total of 7 people from the Airport operation management were involved in the Worskhop activities: the Security Manager, the ENAV Tower responsible, the Aerdorica Safety manager, the Landside and Innerside Activities responsible, the Aerdorica Maintenance, the Quality Responsible and the Information systems responsible.

Validation session in Anadolu Airport – Management and Security Board (M22)

The final version of the SECONOMICS methodological framework has been presented and evaluated in a successful Workshop taking place November 14 and 15 at AU, Eskisehir, Turkey.

Main objectives of the Anadolu Workshop were:

- To present the SECONOMICS Project, its research objectives and results
- To discuss and validate a second and refined version of the models for airport security decision making developed within the Project

Together with AA personnel and University researchers, partners from DBL and UNITN participated into the event as airport security case study responsible. 15

[2] Different versions of the WP5 and WP6 models have been investigated during the intermediate and final validation session through the questionnaire. Further details are provided in the next paragraphs.

people from both the University Airport operation management and the Faculty of Aeronautics and Astronautics were involved in the Worskhop activities. They were presented the current results from the project, e.g. the models developed in WP5 and WP6 and the first version of the SECONOMICS tool, and were asked to evaluate the potentials of SECONOMICS with regards to the functional and security requirements featuring the airport security decision making. Workshop participants contributed also to case study modeling and refinement thanks to their deep aviation knowledge and experience.

During both the Falconara and the Anadolu Workshops, the following activities have been carried out (see Annex 5 for details):

- Security incident scenario-based simulation, aiming to elicit decision making processes as baseline for Models evaluation,
- Focus groups dedicated to each model walkthrough, during which the models' structure and the computational mechanisms have been presented and discussed,
- Presentation of the visualization tool, aiming at gathering feedback on the quality of model output and data visualization.

In particular, models' walkthrough activities involved the participants in step-by-step evaluation of the SECONOMICS framework. This allows to assess the proposed methodologies and to identify alternative usages (with respect to current practices within the Airport Security domain).

Semi-structured Interviews (M22 – M24)

In addition to the methodologies abovementioned, another method has been selected and used in order to support the validation activities required by the Airport Security validation framework in reference to the economic model proposed.

With the aim of collecting relevant comments and observations from the stakeholders involved in the airport domain, semi-structured interviews were planned to evaluate and better calibrate the model presented. Experts at national and international levels involved in the AA and Falconara airport workshops provided feedbacks from the final users' point of view.

More than 15 people among airport managers, airport operative staff, airport security managers, aviation security regulators, training regulators and private security company representatives have been interviewed. They also provided valuable parameter inputs about cost, efficiency and performance of detection devices, such as X-ray machines, metal detector and body scanners in order to populate the CBA model initially proposed.

Expert Judgement (Models Walkthrough) (M23)

Experts from both aviation and IT security domains have been involved in analysing the Airport Security case study through the expert judge.

In particular the following three specialists have evaluated the models from the specific domain perspective:

- one security instructor certified by IATA,
- one former air traffic controller and aviation expert,
- and one IT and cyber-security expert.

The expert judges identified a list of potential and existing problems and provided recommendations for how to develop the models further. Expert analysis revealed insights and concerns currently not covered by the models. At this stage, the purpose of the analysis was to discover and address critical problems on the conceptual level.

Dissemination and Validation Stakeholders Workshop (M25)

The dissemination and validation workshop (M25) for airport security studies was performed at Anadolu University, 27-28th of February 2014 with the objectives of:

1. Sharing information about SECONOMICS project studies Airport and ATM security professionals as stakeholders,
2. Gathering the stakeholders feedback about project scenarios, models and outputs.

AU involved Turkish and South Eastern European professionals about airport security in two main activities:

- Presentation and discussion of the general SECONOMICS project and WP1 and WP4 studies presentations related to security perception,
- Focused presentations of WP1 scenarios and models on airport security and discussions.

The workshop participants were mainly from Turkish civil aviation environment who are professionals from European Commission, Turkish CAA-DGCA (Directorate of General Civil Aviation), Turkish ANSP-DHMI (General Directorate Of State Airports Authority), Airliners, Sabiha Gokcen (Istanbul) airport, Air Traffic Controller's Association (TATCA), researchers and project experts from AU.

Project partners, guest speakers and DGCA airport security representative performed the workshop presentations.

4.3 Validation Results

The Airport Security case study validation results are presented according to:

- Project framework and approach
- Airport security scenarios
- Models and results.

In the following paragraph both qualitative and quantitative results are shown.

4.3.1 Validation of project framework and approach

Stakeholders involved in the final Validation and Dissemination Workshop found the scenarios and models about airport security very meaningful. As one of the main reason for that, the Stakeholders think that airport security operations need to be standardized and optimized for everyone in the airport environment.

The security management activities can be seen as important as airport safety management activities and also both sectors should be collaborated and coordinated. Especially ATM security is very sensitive to interact with flight safety and its impact level should be considered as high social and economic cost generations. The security incident reporting data should be considered as the most important input for risk analysis and for applying adversarial modeling.

Establishing security culture in airport operations can be seen as a long term strategy to favour the perception of security operations for all users and operators.

All the policy-making stakeholders involved in the validation process were really interested in the SECONOMICS project and their feedback about SECONOMICS scopes and methodologies were positive. An approach encompassing security, economics and societal aspects in an integrated way that analyze and balance risk, costs and passenger acceptance of airport security measures has been considered as promising and very useful for decision and policy makers in the aviation domain. Dependence on data that are difficult to estimate and gather, and generalization/application to different scenarios were considered among the main possible risks of SECONOMICS.

According to the feedback collected during the intermediate Falconara and the final Anadolu validation workshops, the modular and customizable modeling approach has been considered as one of the main strengths of the SECONOMICS framework. The modular approach allows the models to take into account different type of airports and traffic levels.

The probabilistic reasoning was considered a positive choice since it was recognized that the real word is hardly deterministic. However, someone pointed out that if the probabilistic distribution is unrealistic the model will fail or lead to low performances.

Perceived Effectiveness (User acceptability)

Already on the basis of introductory presentation of SECONOMICS approach and objectives, intermediate and final workshop attendees set very high expectancies over the need to have a socio-economics analysis methodology (73%) and to find the SECONOMICS approach useful in carrying out their own job. According to Eurocontrols and ENAC representative members, SECONOMICS will ease system modeling and analysis, communication and information sharing with different airport stakeholders (ranging from managers, politicians and regulators to front-end operators and passengers associations) and will effectively support decision making for policy makers and airport security managers.

According to participants in the Anadolu Workshop, main concerns are related to the real applicability and effectiveness of the models and tools presented. One weakness was recognized in the fact that the basic assumptions made can limit the effectiveness of the outcomes. The others relate to the target users of the models: it was pointed out that it should be clarified who is going to be the final decision maker.

Perceived Efficacy (User acceptability)

While someone found the model quite simple, easy to understand and to implement, most of the people found it hard to understand especially for operational people because they will have difficulties in agreeing with some decisions taken in the model. In addition, they pointed out that it requires experience and knowledge to be applied successfully.

Compliance and applicability (Domain suitability)

On the one hand, generalization of the models might be difficult since the Airport Security domain already has its own existing regulations, standard processes and widely adopted work-practice. But on the other hand, the Airport Security domain could accept SECONOMICS solutions because of potential and innovation of the approach with regard to the provision of decision supporting tools and guidelines that integrate Risk Assessment, advanced Cost Benefit Analysis and Social aspects.

Coverage (Domain suitability)

The models do not consider managerial issues as well as the possibility of technology investments to face new emerging threats.

Several suggestions were also proposed on how improving the model. The most important one is probably that of proposing more scenarios of applications with proposed solutions in order to give a better opportunity to evaluate the model.

Summarising, preliminary feedback and discussion were in general positive and promising, with some concerns with respect to possibly high costs of the SECONOMICS tools and guidelines, their complete compliance with existing regulations at an European level and the effort needed in the modeling phase (great expertise required).

In order to foster its adoption, the proposed solution should be cost-effective and easy to use. A possible exploitation model could be to include as additional consultancy service the support for the modeling and quantitative analysis part.

In addition, the results need to be explained and enhanced with how-to use guidelines&recommendations.

SECONOMICS consortium should take into account this feedback to customize its solutions for the Airport and Aviation domain and propose viable business models.

Table 4 highlights on all the main strengths, weaknesses, suggestions and concerns.

Table 4: Strengths, weaknesses, suggestions and concerns about the SECONOMICS framework

STRENGTHS	WEAKNESSES
- Points out views from different perspectives - Trying to calculate detailed variables and costs - Probability distribution (world is not deterministic, usually probabilistic) - Simplicity (easy to understand, easy to implement) - Considers both Defender and Attacker from their perspectives - Increase security - With low cost safety and security precautions some unpredictable situations can be avoided - Reduce the chance of being attacked - Decision shifting from personal and political to scientific independent person - Evaluate different type of airports and traffic levels - Performing a not well known area of study - Since attacks are not known and not estimated, these costs will remain. Do we need to invest on these big investments?	- Hard to understand for operational people - Probability distribution (if unrealistic, model will fail or low performance) - Requires experience and knowledge to apply successfully – not easy to learn - New procedures to integrate into the system - Theoretically limited, has limitations - The assumptions taken for modelling can limit the model effectiveness - No procedures to cope with - No technology investments to face new threats - From an operational point of view it is difficult to understand some decisions taken in the models - More detailed info should be taken from experts - Managerial issues should been considered - I believe that technological experts can not be controlled
SUGGESTIONS	CONCERNS
- More visual examples can be provided - More example scenarios - Some solved problems - A lot of testing - Trend prediction for graphics - Extensive user training - Language support - More operational specific vision to be provided - Consider also threats coming from “inside” e.g. people working in the airport - International and national procedures should be investigated and help can be taken from experts	- Maybe the mathematical approach behind the model is not sufficient - Attacker may also develop his own method of analysis - Applicability - Who will be the decision maker? - Clarify that the risk is evaluated through the probability of successful attacks

4.3.2 Validation of the Airport Security scenarios

According to the feedback from the intermediate and final validation workshops, the proposed scenarios have been evaluated towards the actual collaborative decision making in airport security. 76% respondants of Validation Questionnaire thought that scenarios are well structured with respect to both content and completeness of information.

In particular, the cyberthreat scenario, originated as United States specific scenario, is currently applicable and valuable in Europe as well, since the member states still lack ad-hoc regulations on that.

Cyberthreat Scenario

The Cyberthreat scenario is very innovative and interesting for the involved Policy Makers. ACI Europe is carrying out an in-depth research about cyber-security in Airport and comparing IT security level of different airports (linked to their size and to the national regulations on the topic) and they are studying the European Cyber-Security Strategy to understand how to apply it to the Airport domain to further inform relevant Policy Makers in the Aviation domain for future Regulations on the topic (currently almost uncovered).

Impacts of this scenario need to be better specified since they could be even worse than the ones currently foreseen. According to the expert judges, the impacts of an IT attack need to put safety and security into relation.

A prologue describing the overall context of emerging threats could be useful. The major need is to prevent eventual impacts of future threat (like biothreats and powder and chemical substances attacks) and, in order to reach this aim, the definition of the security scenario may need to be specified through a live example tuned on new security measures and future emerging threats.

The Cyberthreat scenario could be enriched by including:

- Daily flight frequency; if there is one only flight, the handling management system malfunction does not provoke any serious impact,
- Other targets, such as the SCADA systems and the tower personnel turn management system.

Attack to the Tower Scenario

The scenario is well-defined and covers enough elements for the attack to the tower. The overall quality of the scenario is given by specific features like motivation of main actors and types of attacks and defenses

The scenario is very suitable and generalizable to many small airports (e.g. Rome Ciampino) but doesn't seem very suitable for large hubs since the access to the tower is protected.

According to the Policy Makers, the Attack to Tower Scenario seemed less relevant and less realistic. Its validity seems mostly related to the particular Airport.

Towards effective security regulations scenario

The Towards effective security regulations scenario is very relevant for all European Airports and for ACI Europe as association. ACI is currently working in collaboration with ECAC exactly in the direction of a more customized security-regulation for small airports. Final results coming from WP6 model are expected to be discussed together with the SECONOMICS consortium.

The experts involved in the focused interviews supported the investigation of the issues related to current aviation regulations and security policies about the one-size-fits-all security regulation model applied in different countries. Indeed, the interviews conducted at the AA validation workshop revealed that in certain situations the security measures mandated by standard regulations do not fit properly to the specific airport needs. Security regulatory rules and funding mechanisms expressly designed should determine the optimal security expenditures.

4.3.3 Validation of the Models and results

The comprehensive evaluation of the models is summarized below towards the validation objectives and criteria. It integrates the results of all the validation activities that have been carried out.

As a general evaluation on technical usability, according to Policy Makers, the SECONOMICS models are comprehensible to specialists that have to support airport operators and policy makers in model building and interpretation of the results. Models' domain suitability is affected by limited coverage of social aspects. Some specific values of the parameters need more validation/check and may vary a lot depending on different countries (e.g., labour costs of Airport personnel). Indeed the major concern of Policy Making stakeholders is the "customizability" of the models to different situations/contexts and their easy application/generalization to different problems/scenarios.

Cyberthreat Model

Longevity and application of the model to a wider context (Domain Suitability)

The overall domain suitability and longevity of the scenario is assured by the introduction of security measure Control Areas (CA). By addressing the different CA, the cyberthreat scenario covers the relevant case issues.

The model does not assure the appropriate coverage of the socio-economic security issues implied. In particular it does not assure coverage since social issues are not included. The model is not explicit in the integration between social and economic issues. The analysis could allow developing a socio-economical understanding of the airport security but social impact should be detailed.

There is a need to complete and consolidate the costs for the Attacker (e.g. phone calls, deliver mails, etc.) and to include aspects related to passenger behaviour, security staff decisions and impact of the attack.

As for the completeness of the needed knowledge and information, the analytic and predictive capacity of the model is limited to the specific case that has been defined.

In order to be effective in supporting socio-economic security decision in a wider context, the model must allow verifying the basic assumptions behind the development of the model. As far as the model is conceived, it can be effectively adopted as they are in all those situations in which the basic assumptions are embedded.

Alternatively the model needs to be adapted and tailored on the specific requirements of the study case. In such a case, the results are useful as well-defined to start with.

Results visualization (Technical Usability)

The model is presented in a simple way but results are not easy-to-understand. The results' prospect is not very clear or self explaining.

The model results need to be made more comprehensible by also specifying 'how to use' information. The results' tables are not easy-to-understand at all and not useful. Although the current infographic representation does improve the understandability of the results, the overall presentation of the model needs to be improved (e.g. by mean of self-standing brochure, presentation, interactive tool, etc.).

Technical and scientific soundness
Model is thought to reduce the complexity of the underlying security decision making process only in part (44% of respondants to the validation questionnaire agreed).

Effectiveness (User Acceptability)
The cyberthreat model provides useful knowledge on the cyberthreat domain, also possibly to be extended to airlines, cargo companies, carrier IT networks (e.g. safety issues management). In fact there's a lack of strong literature analysis and knowledge-base on cyberthreat and emerging threats.
According to the validation questionnaire result, more than 60% of respondents:

- Do not agree that the model would be easy to use,
- Do not agree they would feel very confident using the model,
- Do not agree that the model will be very cumbersome to use,
- Do not notice too much inconsistency,
- Find the model unnecessarily complex.

71% of respondants think that they would need the support of a technical person to be able to use this model.

The results are very useful for airport security managers since they point the Control Areas out for supporting security investment. The results may also support the definition of specific needs (which the most critical vulnerabilities are, which the already-in-place controls are, what their level of maturity is).
Especially in the case of the experienced hacker the results are effective and suitable. In the case of the novice hackers the results (optimal portfolio) do not seem sufficient to effectively cope with the attack.
The results are useful since they provide a logical framework able to support, at least in part, the decision-making process. The results should be improved by the development of reactive and predictive evaluations since the security decision depends on which countermeasures are already in place.
The results fail in supporting the selection of the countermeasures. They instead allow the prioritization among the different Control Areas.

Attack to Tower Model

Coverage (Domain Suitability)
1/3 of validation questionnaire respondents agreed in saying that the model doesn't cover a complete set of domain constructs, i.e. not all necessary concepts of the application domain are represented in the way of modeling.

Application of the model to a wider context (Domain Suitability)

The model is very focused and the scope is not too wide and ambitious. It can't be easily generalizable since it is too much case-specific and it is very hard to imagine how it might be considered a result at European level.
The basic assumptions from which the model stems for are not sufficiently clear. The model does require that the initial assumptions are evaluated and redefined at each time. If the perimeter of the model is not clearly defined, its efficacy could be reduced.
In particular, the estimated defender costs (i.e. on security measures) do not seem realistic and lack of relevant items, such as 'flight delay' costs.
The attacker costs also needs to be consolidated and validated, in particular, those ones related to the estimation of the cost of a life (i.e. killed terrorist, imprisoned terrorist, and killed passengers). The rationale behind the estimation of the cost of the attacker needs to be verified.
As for the inclusion of social issues, they are partially covered by the model since only the image costs are computed within the model. At the same time, the social aspects that are interesting for the airport management board have to be verified with the end users and included, i.e. in order to inform their investments. It does not imply either the human resources issues, like training and procedures.

In order to improve the impact of the model at European level, the south-eastern international airport case-specific costs have to be translated to other EU countries, since the defender costs, such as technical controls and personnel costs, may differ a lot.

Quality of the results and perceived effectiveness (User Acceptability)
The results may provide useful information for both improving the scenario and the model itself, although the basic assumptions behind the tuning of the model need to be verified. The results of the model can only partially support airport security decision making. The impact of the model is estimated to be very limited.

Models and results visualization (Technical Usability)
The presentation of the model has to be simplified and made easy-to-understand. According to 68% of respondants to the validation questionnaire, they would need the support of a technical person to be able to use this model.
Math formulas included into the text make the presentation difficult to understand. They are suggested to be moved to an appendix.
The results are easy-to-understand for researchers (e.g. mathematicians) as final users. Abstract representations, like the influence diagrams, are very difficult to be caught by security managers who basically need to understand the attackers and defenders strategies and actions.
The results of the model are not effectively represented: the selected portfolios are not immediately easy-to-understand and two cases (out of three) do not diverge too much to be reasonably developed as separate cases.

Towards Effective Airport Security Regulation model

Application of the model to a wider context (Domain Suitability)

Efficiency, costs and social acceptance of different adopted security measures have been analyzed with the stakeholders through a series of trade-offs providing insights about their preferences towards several security measures, both physical and technological. Additional interviews have been conducted in order to understand the existing relationships between different actors involved in security tasks in the same airport environment. The aim was to outline the structure of the security duties and responsibilities designed by the regulators.

Interview results highlighted that the relationship among different security actors (mainly private security company staff and police staff have been considered) can be framed into a principal/agent theory in relation to the strategic decisions determined by the regulations. Incentive strategies, insourcing and outsourcing decisions as well contractual relationship settings between airport and outsourcing services companies informed the main variables on which the models based on Game Theory have been evaluated.

Perceived Efficacy (User acceptability)

Half of respondents (52% of respondents) think that the model would improve the process of decision making and almost the totality of respondants think that would like to use this model very frequently (87% of respondents).

5. Future and Emergent Threats

Future and emerging threats is a prominent theme within the Airport Security case study. In Deliverables D1.3, Airport Requirements, the focus was to investigate the relation between new security measures and emerging threats led by the following research question: what is the balance between new security measures and emerging threats in terms of cost and technology, security gain and risk perception of passengers?

Throughout year 2 emerging threats in Airport security have been broken down into different views which looked at the impact, opportunity, threat actors & motives and means. Other issues related to future and emerging threats were personal perspectives, preparedness (e.g. training and procedure), exercise of authority and information sharing (e.g. skilled personnel responsible and communication path).

As anticipated in Section. 2.1 Consolidation of scenarios, WP1 developed a whole new scenario and model specifically addressing Cyberthreat – Emerging threats. IT security and airport security experts involved by Deep Blue are convinced that the future airport security will be massively impacted by cyberthreats and information security threat. In addition to this, with the continued fast paced IT innovation, the means cyberattackers will have in the future to attack the air transport infrastructure is continually increasing. Finally, an increasing range of cyber attackers with higher capabilities and motivation to attack airport and air transport is also expected in the near future.

Future and emergent threats have also been pointed out by the stakeholders involved in Airport Security validation, as one of the requirements toward which the robustness of the models should be demonstrated. In particular, biothreats and chemical warfare have been recognized as the most prominent future threats to foresee in further development of the scenarios.

6. Pan-european Coordination

The main objective of SECONOMICS is to develop innovative risk assessment techniques and tools that will support policy makers in security-related decisions by taking into account social and economic factors. This is particularly challenging when considering both logical and physical security aspects and different domains in a pan - European perspective.

All the three Airport Security scenarios (Section. 2.2) have been developed by mean of a Pan-European coordination comprising two kinds of activities:

- Scenario-specific SoA and regulations' review at European level (Section 2 of D1.3 Airport Security Requirements) and
- Presentation and discussion of the SECONOMICS results with stakeholders at European level.

As a major step for the second activity, the SECONOMICS project was to actively involve high-level policy makers in the validation procedure.
In particular, the Aviation security domain is a very regulated domain with a top-down approach. Regulations, mandatory procedures and internal rules to ensure Security standards compliance have to be respected. Therefore, convincing high-level policy makers and regulators, both at National and European level, of the effectiveness and usefulness of the SECONOMICS approach has been a primary goal.

To achieve this objective, DBL has organized the following three main activities with Aviation Security high-level policy makers with the aim to collect stakeholders' preliminary feedback and comments about the applicability and suitability of the SECONOMICS results in the Airport Domain:

- ENAC: On 13th May 2013, DBL presented the SECONOMICS project objectives and preliminary results to two members) of the Security and Safety Departments of the Italian Civil Aviation Authority, the “Ente Nazionale per l'Aviazione Civile” (ENAC). ENAC mission is to propose and approve national aviation legislations compliant with international standards and to ensure regulatory enforcement on different civil aviation stakeholders. On 17th September 2013 DBL and UNITN presented SECONOMICS to the “Board of Airport Directors”. The Board encompasses the ENAC Directors of the major Italian Airports and it holds bimonthly meetings by discussing policy and regulatory proposals to be presented and approved by competent Authorities.

- On 26th of September DBL presented, together with other Security-related projects, SECONOMICS to three members of the Eurocontrol Security Department. Eurocontrol, the European Organisation for the Safety of Air

Navigation, is an international organisation founded in 1960 and composed of Member States from the European Region, including the European Community which became a member in 2002. Eurocontrol main mission is to support its Member States to achieve safe, efficient and environmental-friendly air traffic operations across the European region and to deliver the "Single European Sky" of the 21st century. To achieve its mission, the EUROCONTROL Agency works closely with Member States, air navigation service providers (ANSPs), civil and military airspace users, airports, the aerospace industry, professional organisations, intergovernmental organisations and the European institutions. EUROCONTROL is involved in the SESAR Joint Undertaking (SJU), together with ECAC, ICAO and the European Commission with the aim to further improve Aviation security in Europe. Aviation Security has two main sub-components that are Airport Security and ATM Security. Recently both SESAR and Eurocontrol are also focusing particularly on the definition of a cyber-security strategy at pan-european level.

- On February 3rd 2013 DBL joined the Airport Council International - ACI Europe Security Managers in Brussels to present the SECONOMICS models and results for the Airport Case Study in detail. ACI represents the interests of over 450 airports in 44 European countries. ACI members account for over 90% of commercial air traffic in Europe. ACI membership is comprised of airport operators of all sizes, along with national airport associations, world business partners and educational establishments working together in an active association to ensure effective communication and advocacy with legislative, commercial, technical, environmental, passenger and other interests.

More will follow in Project Year 3.

7. Conclusions

The WP1 Model validation process described in this deliverable allowed us to evaluate the modeling approach, the scenarios, the models themselves and the results in a comprehensive and integrated way. The validation has been made possible by the application of a methodology defined ad-hoc for the validation of scenarios and models, integrating state-of-the-art validation methods, like the EOCVM and Participatory & User Centred Design approach and techniques.

Through the participatory approach adopted, Airport security stakeholders have been involved in presentation, discussion and iterative refinement of working and final versions of the models and the scenarios.
Possible risks and limitation that have been highlighted, as well as the most appreciated and valuable results of the project are described.

REFERENCES

[1] Shim, W., Massacci, F., de Gramatica, M., Tedeschi, A., Pollini, A. (2013) Evaluation of Airport Security Training Programs: Perspectives and Issues. SecATM 2013.

[2] Pollini, A., Tedeschi, A., Cano, J., (2013) Modeling an Emerging Terrorist Threat against Airport Security Scenario. EUROInform Conference, Rome, July 2013.

[3] Shim, W., Massacci, F., M., Tedeschi, A., Pollini, A. (2013) A Relative Cost-Benefit Approach for Evaluating Alternative Airport Security Policies. Poster presented at SESAR Innovation Days 2013.

[4] Cano, J., Rios Insua, D., Tedeschi, A., Turhan, U. (2013) Security Economics: A Multiobjective Adversarial Risk Analysis Approach to Airport Protection. Submitted to Annals of Operations Research (ANOR).

[5] MOODY, D.L. (2005): "Theoretical and Practical Issues in Evaluating the Quality of Conceptual Models: Current State and Future Directions", Data and Knowledge Engineering, v.55 n.3, p.243-276, December 2005

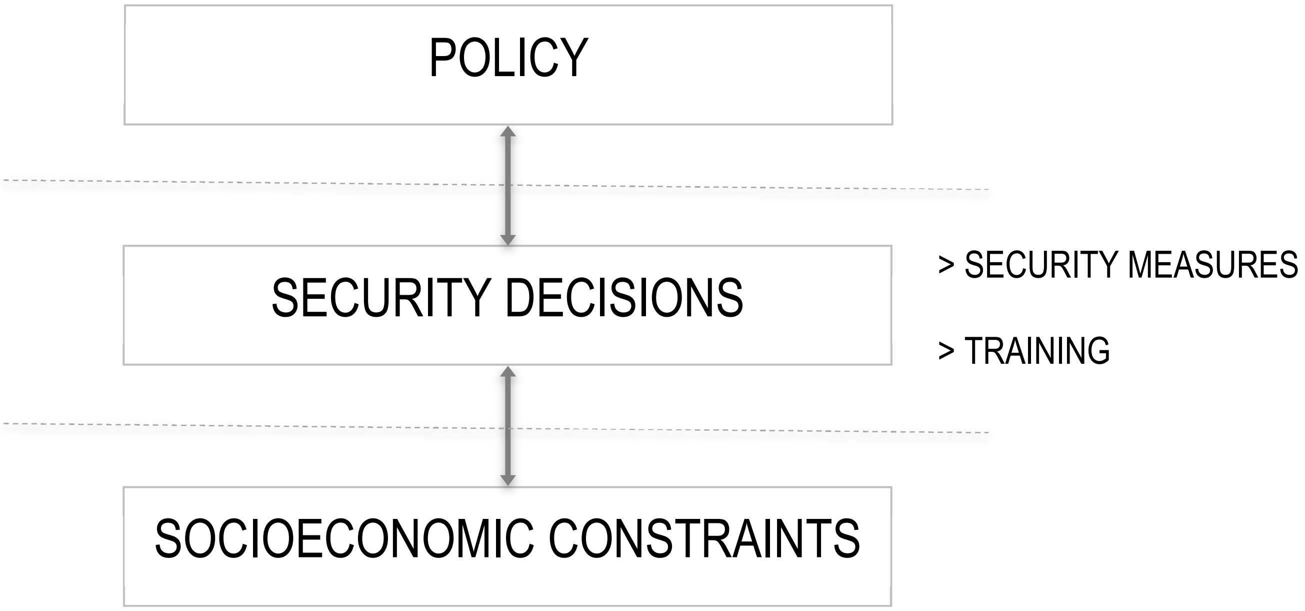
[6] F.D. Davis, (1989) Perceived usefulness, perceived ease of use and user acceptance of information technology, MIS Quarterly 13 (1989) 319–340.

[7] Venkatesh, V., Thong, J.Y.L, Xu, X. (2012) Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Q.* 36, 1 (March 2012), 157-178.

[8] EUROCONTROL (2005) European Operational Concept Validation Methodology (E-OCVM). Available at: https://www.eurocontrol.int/eec/public/standard_page/validation_ocvm.html

Annex 1 - Security Decision Questionnaire

From our previous communication, we would like to have an opportunity to ask you answer a list of questions below. These questions have been designed to collect general information about security decisions at your airport. In particular we are investigating the relation between security decisions and policies &regulation and between them and the socioeconomic constraints you have to face:



Questions are grouped into four categories:

- Section a: Personal and Organization Information
- Section b: Security Compliance
- Section c: Security Decision Making
- Section d: Security Expenditure

Please consider that your opinion will provide us with important information to accomplish research objectives at European Level and build useful tools for security airport decision making.

We appreciate your timely response to the questionnaire and your cooperation.

a. INFORMATION ABOUT YOU AND YOUR ORGANIZATION

1. How many employees does your airport have:

□ Between 50 and 100
□ Between 100 and 500
□ More than 500

2. How many employees in charge of security does your airport have:

□ Less than 50
□ Between 50 and 100
□ More than100

3. How many connections does your airport have:

□ Less than 10
□ Between 10 and 30
□ More than 30 (please indicate approximately the number): ____________________

4. Could you please indicate if your airport could be classified as:

□ HUB
□ SPOKE
□ I don't know

5. Could you please approximately indicate the average budget of your airport in previous years?

____
____

6. What is your position in your organisation?

□ Security Manager
□ Security Employee (please specify): ____________________________
□ Other, please specify: __________________________________

7. Are you involved in security related tasks?

□ Yes
□ No
□ If yes, please specify: ________________________

b. SECURITY COMPLIANCE

8. Which authority (airport, airline, government, etc) is responsible for regulating security policy?

____

9. How often is the security policy updated?

____

10. Be compliant to security regulations does impact on the effective airport security performance.
Please indicate which of the below listed events occurred as a consequence of security regulations compliance in your personal experience:

- ☐ Organization’s security was considerably improved
- ☐ Organization’s security was damaged
- ☐ Security became a higher business priority
- ☐ Security budget increased
- ☐ Additional staff were hired
- ☐ New security technology was deployed
- ☐ Other: ____________________________________

c. SECURITY DECISION MAKING

11. When making a decision related to security management, which are the most important parameters to take into consideration? Please rank the followings by priority (you can also assign the same priority to different items):

a) Executive and management priorities
b) Contacts with business partners
c) General Security Management standards
d) Sector-specific security regulations
e) Security and privacy laws
f) Other, please specify: ____

12. Which are the most useful sources of information when determining security needs and making a security-related decision? Please rank the followings by priority (you can also assign the same priority to different items):

a) Previous attacks on your airport
b) New reports of other attacks/incidents in other airports
c) Security breach notifications
d) Information shared with other organizations
e) Passenger surveys

f) Other, please specify: ____

13. What type of financial metrics for quantifying the costs and the benefits of security expenditures are used (check all that apply)?

a) Return on Investment (ROI)
b) Net present value (NPV)
c) Internal rate of return (IRR)
d) Please provide other metrics if needed: ____

d. SECURITY EXPENDITURE

14. Are you involved in the security expenditure decisional process? Please answer by choosing among the following statements:

☐ Yes, I am/was fully responsible for it
☐ Yes, I am/was partly responsible for it
☐ No, I am/ was not involved in it

15. What is approximately the percentage of the total budget spent on security?

a) Under 1%
b) 1% ~ Under 5%
c) 5% ~ Under 10%
d) 10% ~ Under 20%
e) Over 20%
f) I do not know

16. As a security expert what are the key issues to take into consideration when investing in security measures? Please rank the followings by priority (you can also assign the same priority to different items):

a) Security culture (e.g. optimization of security processes, security audits, airport security boards, others)
b) Security training program
c) Security procedures (e.g. passenger-baggage reconciliation, hand search, passenger profiling)
d) Security technologies (e.g. full body scanners, explosive trace detection, advanced imaging technology, behavior detection)
e) Security infrastructure (e.g. airport layout)
f) Others, please specify:____

Annex 2 - Template for gathering information on Airport Security cost structure

Structure

- The Airport Stakeholders
- Airport Security Commission
- Training, Research and Auditing Unit
- Operations

Costs Structure

- Human Resources
  - Agents (e.g. number of agents, shifts organization)
  - Monthly cost to the organization
  - Total cost to the organization

- Installations
  - Type of installation (e.g. new terminal, security watching towers, etc.)
  - Investment cost to the organization
  - Total cost to the organization

- Equipment
  - Type of equipment (e.g. camera, x-ray, WTMD, etc.)
  - Investment cost to the organization
  - Total cost to the organization

Annex 3 - Airport IT Infrastructure Questionnaire

QUESTIONS

1. From the information you already provided us with, we know that Anadolu Airport has between 100 and 500 employees in the airport and between 50 and 100 of those are in charge of security in the airport.
   Is it possible for you to provide us with an idea of the number of machines (PCs, servers, etc.) that are part of the overall airport IT network? And, approximately, how many machines are included in the VPNs in place at AA?
2. Since the AFTN, the Passport Control, the Operational Network, and the Police Networks use separated VPN connections over the ADSL line, is there any link among such networks?
3. There is an emergency line if ADSL fails? How does that work? Does DHMI manages it remotely? If yes how? Do they manage also the physical security of the equipment? If not, who? Is there a modem or any OOB system to connect to the AFTN?
4. Same questions for passport control network. Furthermore, which other systems are connected, directly, or indirectly to the passport control hosts or network equipment?
5. Camera network includes any wireless camera? Does it share any network equipment with other systems? Where are the connectors panels located, and how are the protected?
6. Are radios connected to other digital or network equipment? Do they allow for remote operation?
7. Which, if any, telephone line is digital? Which is the provider and equipment brand?
8. There is any modem module/RMU attached to any of the phone line outlets?
9. What services provided in the control tower, if any, are available to other networks/systems? What is the logical structure of the email service accessed from the tower? And vice-versa, what systems/networks are accessible from the IT systems in the tower? Where are the connection points? If different networks communicate, do they implement any type of segmentation? Is there a router to segment the network or also a firewall?
10. Does the “technical room” contain SCADA terminations? Is there any link connecting to other IT systems? Is maintenance operated locally or remotely? By who? What are the IT controls in place for the technical room?
11. Is the lights management system physically disconnected from other systems? How is maintenance performed? The technical personnel is part of which organization?
12. Does wifi give access to only a segment of the network or to all the network?

13. If possible, provide a network diagram of all the IT systems. Both logical and physical.
14. What is the backup solution for the airlines and for the police if the ADSL link fails?
15. Who does administrate and has the responsibility of the dedicated VPNs? Does each VPN managing company have its own IT administrator (e.g. Turkish National Police Officers, DHMI)? Does there exist one general IT administrator that is responsible for the VPNs?
16. Can the Navigation and Surveillance closed loop network be accessed by the airport IT networks?

IT Structure

17. Flight information network

18. Security network

19. IT Structure in Tower

20. CNS network

21. IT Structure of AA Terminal
    - Organizational Network
    - Police and Custom Network
    - Operational Network

Annex 4 - Cyberthreat Countermeasure Implementation Maturity Questionnaire

The objective of the questionnaire is to collect information useful for the determination of the level of maturity of information security defense measures relevant for the scenario identified in the model.

Such concept, the 'level of maturity', will be adopted instead of the 'effectiveness' label identified in the preliminary version of the cyberthreat model. The maturity level will include then the quality (1) and the completeness (2) of the implementation of each defense measure, and its value will be a function of the actual degree of implementation of the considered security measures in each control area. The level of maturity will be specific for each single airport / case.

By adopting 'effectiveness' we could generate ambiguity, since it might suggest that we are defining a way to prioritize the control area.
Instead we want to state that all the security measures are equally important and ought to be implemented all together to effectively raise the security of the system. In fact if all the measures would have been fully implemented, this would led to the ideal, although not reachable, 100% IT security.

The questions take into account the previously identified defense areas:

CA1 – Governance and People

1. Security governance
2. User awareness and training
3. Enforcement of measures on infraction
4. Background checks on employees and 3rd parties

CA2 – Policy and Processes

1. Information security policy
2. Data management policy
3. Computer and data use policy
4. Security processes and procedures

CA3 – Operations

1. Continuous monitoring of alerts related to system/application access, integrity monitoring, and network traffic
2. Periodic security risk analysis and vulnerability assessment
3. Periodic user recertification
4. Periodic update of critical software and configurations

CA4 – Technical controls

1. Network segmentation and firewalls
2. Antivirus,
3. IDS/IPS
4. VPN endpoints

CA5 – Attack response

1. Deploy emergency measures
2. Perform forensics
3. Deploy remediation measures
4. Update security areas

Questions:

1) Describe the governance organization of the security. Please include the following information: the final responsible for security and the responsible for the security budget allocation.
2) Is there an auditing office that reviews the security implementation?
3) Is the information security risk included in overall the risk assessment of the airport?
4) Is there a mandatory, periodic information security awareness and technical training for all employees? If yes, how often? If not, when was performed last?
5) Do you have in place internal regulations and clear actions for the management of unethical behavior and infractions? Are they always followed? Are they clearly communicated to, and signed off by employees before they are enabled to access organization assets?
6) Do you run background checks on employees? If yes, which type of information do you seek out and verify?
7) Do you perform a due diligence on third parties working for your organization and/or working on your premises? If yes, what does it include?
8) Do you have SLAs in place with service providers? Do you have security requirements for 3rd parties working with/for you? Do you have any binding contract on minimum security requirements with them?
9) Do you have an information security policy?
10) Do you have a data management policy or equivalent?
11) Do you have a set of IT and security policies covering all aspects of IT and information security?
12) Do you have a computer and data use policy? Is it signed off by employees before they are granted access to your systems?
13) Do you have well defined and formally documented processes in place? Do they cover all aspects of IT and IT security? Do they cover user provisioning and de-provisioning, access management and system administration?
14) Do you have well defined and documented procedures in place? Do they cover all aspects of IT security?
15) Do you have staff assigned to continuous, real-time, alert monitoring?
16) Do you perform information security risk analysis periodically? If yes how often, if not, when was the last time? The same for vulnerability assessment.
17) Do you have an integrated identity management solution? Do you perform periodically a user recertification? If yes, how often, if not and it is event driven, in which events?
18) Do you update your software? Operating system, applications, etc..? If yes, how often?

19) Please provide an estimate of the delay between the release of a security update for software in use in your systems and the time you update the systems in production.
20) Do you test software updates in a test environment before deploying them in the production environment? Does the test environment contain any sensitive data?
21) Do you back up critical configurations (e.g. firewalls, routers, OSs, specific applications)? If yes, how often?
22) What technical security measures are in place? Firewalls? SIEM? IDS? IPS? DLP solutions? Antivirus? Anti spam?
23) Are technical security solutions managed centrally? Are their logs aggregated, correlated and analyzed in a centralized manner?
24) Do external connections use VPN technology?
25) Does VPN or any other external connections use a two factors authentication?
26) Is the network segmented? Is the segmentation virtual or physical?
27) Is any eventual wifi network physically disconnected from the internal wired network?
28) Do you have a business continuity and/or an emergency plan for security breaches?
29) D you have a disaster recovery plan for cyber operations?
30) Do you have an incident response team for cyber events?
31) Do you have specific processes and procedures for IT staff to follow in case of a cyber security breach? Are they tested regularly? Is yes how often, if not, when was the last time?
32) Do you have in-house competences to perform forensics on IT systems?
33) Have you ever been breached? If yes when was the last time? And also, which were the root causes of the breach(es)? (e.g. unpatched systems, lack of monitoring, etc..)

Annex 5 - Cyberthereat focused interview script

Key Aspects of Emerging Threats with relation to your Airport

By starting with an overview of the Airport network infrastructures, we would like to enter the details of the emerging (mostly information/ cyber) threats that could have happened to each case.

By focusing on your Airport:

Measures & Policy

1. Which the airport security-critical network infrastructures are?
2. Do measures and actions guaranteeing information security measures exist?
3. Which are the national and european reference regulation for Airport information security?
4. Which are the mandatory regulation in the airport information security? Are there any differences between public and private entities?
5. How are information security policies implemented in your specific airport? What is the internal organizational structure of security? (E.g.: COO -> CISO -> Security Director, Sec. Manager, etc..)
6. Which are the events/ facts that have provoked an increasing number of information security measures?
7. What's the % of security budget on the total budget of the airport?
8. Is information security a board responsibility?
9. Is information security risk inputted in the overall airport risk assessment (together with financial risks, operational risks, etc..?)
10. Is information security risk audited?
11. do you have a remediation strategy in place?

Threats

12. Have the airport information / cyber-security ever been threatened?
If so, specify

12.1 the threat agent 12.2 the infrastructure 12.3 the vulnerability 12.4 the implicated risk 12.5 the impact 12.6 How did you find out about the breach? Was it before or after the impact? If after, how much was the cost of remediation?	**Threat agent:** e.g. adversary nation state, disgruntled employee, criminal ring, hacktivists, etc.. **Threat**: e.g.; spear phishing attack, DDoSs attack, specifically crafted malware, unauthorized access, etc.. **Threat vector**: e.g. Internet facing maintenance ports, SCADA networks, malware; **Vulnerability**: e.g. un-patched endpoint, slow user de-provisioning system, lack of defence in depth, lack of security monitoring; **Risk**: e.g. equivalent of a sudden and persistent ash cloud, switch back to

	manual procedures, loss of control or reliability of information systems; delay, cancellation or diversion of flights, critical services outage, loss of personal data, physical damage/incident; **Impact**: ...see model output? Economic, social, credibility, / for the airport, for the airline, for the country, etc..

Annex 6 - Screening technology questionnaire

Questionnaire on the introduction of screening technology for Airport Security
We focus on technological requirements for implementing the specific policy of inspecting passengers and their cabin baggage via various security measures. More specifically, we are performing a cost-benefit analysis of implementing current and newly proposed security policies, exploring issues of technological cost and performance.

Technologies used for screening cabin baggage are

1) hand search (HSB),
2) X-ray equipment (XR)
3) explosive detection systems equipment (EDS),

Technologies used for passenger screening are

1) hand search (HSC),
2) Walk-through metal detection equipment (WTMD),
3) Hand-Held Metal Detection equipment (HHMD),
4) Explosive Detection Dogs
5) Explosive Trace Detection equipment (ETD).

Legenda:
In the following sections, the subscripts A and NA indicate 'Alarm' and 'No Alarm', respectively, while the subscripts T and NT represent 'Threat' and 'No Threat', respectively. For illustrative purpose, we do not specify the technology used for screening. However, we will used a superscript, HSB, XR, EDS, HSC, WTMD, HHMD and ETD, on the estimates when necessary.

TIME

N1 = number of years of useful life for a baggage screening security device before technical obsolescence ________________
N2 = number of years of useful life for a baggage screening security device before it wears out due to being in operation ________________

COSTS

C_O = annual maintenance and repair costs (operational) for the screening device, including annual lease expenses (if any); this is independent of the volume of object inspected ________________
C_F = the purchase price of the screening device ________________
C_I = cost of operating the screening device, per object inspected

____

C_{FA} = cost of a false alarm= cost of falsely indicating a threat on a scanned object ________________
C_{TC} = cost of a true clear = cost of correctly indicating a non-threat on a scanned object ________________

C_{TA} = cost of a true alarm = cost of correctly detecting a threat on a scanned object _______________
C_{FC} = cost of a false clear = cost of not detecting a threat on a scanned object
____

VOLUMES

SCAP = number of checked objects a screening security device can screen per year (i.e., the screening capacity) _______________
SC = number of checked objects a screening security device can screen before wearing out due to being used _______________
S1 = number of selected (e.g., high risk) objects received per year at the airport _______________
S2 = number of non-selected (e.g., low risk) objects received per year at the airport _______________
α = proportion of selected objects checked at the airport _______________
ß = proportion of non-selected objects checked at the airport
____

PROBABILITY

P_T = Probability that a scanned object has a threat _______________
P_{FA} = $P_{A|NT}$ = Probability of a false alarm (a device falsely indicates a threat – false positive) _______________
P_{FC} = $P_{NA|T}$ = 1 – P_{TA} = Probability of a false clear (a device does not detect a threat – false negative) _______________
P_{TC} = $P_{NA|NT}$ = 1-P_{FA} = Probability of a true clear (a device does not alarm when there is no threat) _______________
P_{TA} = $P_{A|T}$ = Probability of a true alarm (a device correctly detects a threat)
____

Annex 7 - Airport Security Training Questionnaire

Approfondimento dello Scenario di Training in Airport Security[3]

Obiettivo: indagare come avviene l'implementazione effettiva di programmi di training in aeroporti di diversa dimensione e status, sia come singoli attori che come attori inseriti in una rete di aereoporti/ gestori.
In particolare vorremmo concentrarci sulle seguenti categorie di aereoporti, identificati sulla base dei dati ottenuti dalla raccolta dei questionari (vedi doc in allegato per i dati sugli aereoporti):

- Small-size International Airport (per cui abbiamo come esempi Falconara, Pescara e Esbjerg)
- Medium-size International Airport (per cui abbiamo Brno)

In questa fase ci riserviamo di approfondire l'Aereoporto Universitario di Anadolu, Turchia, come caso particolare da indagare nel dettaglio con il partner di progetto.

Focus: Immagini di ricevere una richiesta di progettazione e di implementazione di attività di:

1. Initial Training
2. Recurrent Training
3. Additional Training (es. Human Factors, Cyberthreats)

Dai seguenti attori:

a) un Small-size International Airport (es. Falconara),
b) un Medium-size International Airport (es. in un contesto italiano potrebbe essere Bologna)
c) un grande Hub Intercontinentale (es. Fiumicino).

Domande:

1. Potrebbe descrivere come queste 3 organizzazioni implementano e gestiscono le attività di training delle varie categorie?

2. Le attività di training 1. 2. e 3. sono obbligatorie per tutte le tipologie di aeroporti considerate? Potrebbe darci il riferimento specifico alla normativa che definisce questo aspetto?

3. Quali sono le quote percentuali nelle attività di training 1. 2. e 3. per:
- training aula
- CBT
- e-learning
- on-the-job

[3] The Airport Security Training Questionnaire is available only in italian since it has been administered to national experts.

4. Quali sono le differenze tra 'formazione pratica' e 'on-the-job'? In quali modalità sono gestite le simulazioni (es. quella per screeners)?

5. Nel caso specifico dei piccoli aeroporti come è operazionalizzato il training? Posseggono i gestori dei piccoli aeroporti le risorse per rispondere alle normative sulla sicurezza?

6. I piccoli aeroporti/ gestori si appoggiano ai grandi gestori/aeroporti? Hanno in alternativa la possibilità di federarsi con altri gestori piccoli?

7. Può verificarsi il caso in cui training è implementato in una 'rete' formata da aeroporti/ gestori con diverse dimensioni e capacità (es. un aeroporto grande che offre servizi di training per aeroporti più piccoli)? Eventualmente quali potrebbero essere i vantaggi di tale modello?

8. Nel caso in cui il training sia implementato congiuntamente da attori diversi, qual'è la distribuzione dei tasks e dei ruoli tra i diversi attori? Quali le modalità privilegiate (frontale, CBT, e-learning, etc.)? Quale la ripartizione dei costi?

9. Com'è implementato il training nel caso di un gestore con più aeroporti (es. ADR con Fiumicino e Ciampino)?

10. Com'è implementato il training nel caso del singolo aeroporto rispetto alla pluralità di destinatari: i fornitori si riferiscono al training del gestore (es. il responsabile della sicurezza del catering) oppure realizzano attività specifiche per le loro competenze?

11. Esistono training sulla sicurezza specifici per fornitore? Es. tutti i catering seguono un training definito ad hoc.

12. Oltre a ADR e SEA quali sono gli operatori che gestiscono più aeroporti in Italia?

13. Quali sono i modelli di implementazione del training delle altre nazioni europee? es. Spagna.

Annex 8 - Policy Makers Evaluation Questionnaire[4]

a. In riferimento alla presentazione del progetto SECONOMICS, ritiene che debbano essere inclusi nella ricerca ulteriori prospettive e tematiche, attualmente non contemplate?

b. Per quanto riguarda la valutazione del rischio economico, quali sono gli aspetti più importanti che ritiene debbano essere approfonditi nella ricerca?

c. Per quanto riguarda la valutazione del rischio psicosociale, quali sono gli aspetti più importanti che ritiene debbano essere approfonditi nella ricerca?

d. Ritiene che debbano essere incluse ulteriori prospettive quali ad es. gli aspetti politici e la sicurezza ambientale nella presa di decisione in materia di sicurezza? Se si, quali?

e. Nella sua opinione quali sono i potenziali utilizzatori del tool che svilupperà il progetto SECONOMICS? E con quale impatto?

[4] The Policy Makers Evaluation Questionnaire is available only in italian since it has been administered to ENAC Board of Airport Directors.

Annex 9 - Validation Support Questionnaire

Instructions for using this questionnaire (please read carefully):

1) Before starting filling the questionnaire, please read through the questions to get a rough overview about the criteria.
2) If you collaborate with several people for the airport decision making, try to negotiate a “group opinion” about the SECONOMICS Model.
3) The questionnaire has two scales for each criterion (statement): Please indicate for each criterion on the left scale whether the criterion is fulfilled. And indicate on the right scale how important this criterion is to you in general. On page 6, you can note identified problems issues with the model
4) You can fill in the questionnaire at any time after the presentation of the models.
5) After completing the questionnaire, please scan it and send it to: alessandro.pollini@dblue.it or alessandra.tedeschi@dblue.it

Thank you!

Which **version** of the model did you use for your evaluation? □ Version September 2013 Other:
How many people were involved in the validation activities and in filling in this questionnaire? (number of people)

USER ACCEPTABILITY					
PERCEIVED EFFICACY (Perceived ease of use and perceived usefulness)	How much do you agree or disagree with the sentence?				
	Strongly agree	Rather agree	Very important	Rather disagree	Strongly disagree
I think that the model would improve the process of decision making.	□	□		□	□
I found that the output of model is of quality.	□	□	□	□	□
I thought the model would be easy to use.	□	□		□	□
I think that there are conditions that would facilitate the usage of the model.	□	□		□	□
I think that I would need the support of a technical person to be able to use this model.	□	□		□	□
I think that the output of the model would be task relevant.	□	□		□	□
I think that the adoption of the model would impact on the task.	□	□		□	□
I think I would feel very confident using the model.	□	□		□	□
I needed to learn a lot of things before I could get going with this model.	□	□	□	□	□
I think that I would like to use this model frequently.	□	□		□	□
I found the model very cumbersome to use.	□	□	□	□	□

I found the model unnecessarily complex.	□	□	□	□	□
I found the various functions in this model were well integrated.	□	□	□	□	□
I thought there was too much inconsistency in this model.	□	□		□	□

	Is the criterion fulfilled?					How important is the criterion to you?		
	Strongly agree	Rather agree	Difficul t to say	Rather disagree	Strongly disagree	Very important	Somewhat important	Not important
TECHNICAL AND SCIENTIFIC SOUNDNESS								
Reducing complexity: The modelling reduces the complexity of the underlying security decision making process.	□	□	□	□	□	□	□	□
Increasing knowledge: The model contributes to increase the user’s security-specific knowledge.	□	□	□	□	□	□	□	□
Scalability: The model is suitable for creating very large models of the case study domain.	□	□	□	□	□	□	□	□
Predictability: The model brings to predictable results.	□	□	□	□	□	□	□	□
Automation: The model is supported by effective automated computations.	□	□	□	□	□	□	□	□

DOMAIN SUITABILITY

	Is the criterion fulfilled?					How important is the criterion to you?		
	Strongly agree	Rather agree	Difficult to say	Rather disagree	Strongly disagree	Very important	Somewhat important	Not impor tant
Applicability								
The models can be applied on the airport case study for modelling the functional and security requirements characterizing the case study.	□	□	□	□	□	□	□	□
Human effort								
The modelling of changing requirements in the case study can be conducted with less effort than by using state of the art techniques.	□	□	□	□	□	□	□	□
Domain scoping								
The model has an appropriate scope for the airport domain. It is neither too broad, which results in a less specific and less expressive modelling language, nor too narrow.	□	□	□	□	□	□	□	□
Coverage								
The defined set of socio-technical systems is representable in the model.	□	□	□	□	□	□	□	□
The defined set of security requirements is representable in the model.	□	□	□	□	□	□	□	□
Analyzability								
The model is analyzable by using suitable reasoning techniques.	□	□	□	□	□	□	□	□

TECHNICAL USABILITY

	Is the criterion fulfilled?					How important is the criterion to you?		
	Strongly agree	Rather agree	Difficult to say	Rather disagree	Strongly disagree	Very important	Somewhat important	Not important
Comprehensibility								
The model covers a complete set of domain constructs, i.e. all necessary concepts of the application domain are represented in the way of modelling.	□	□	□	□	□	□	□	□
Various readers of the model who didn’t participate in building the model (e.g. colleagues, customers, managers…) accurately interpret the model (result).	□	□	□	□	□	□	□	□
Memorability								
The model concepts are easy to learn/recall from memory.	□	□	□	□	□	□	□	□

When you **rather or strongly disagreed** with the fulfilment of criteria, what were the reasons?
Please make a **list of problem issues** for the model

Annex 10 - Falconara Workshop Plan

VALIDATION ACTIVITIES	PHASES
SLOT 1. Scenario-based Simulation Aiming to elicit decision making processes as baseline for Models evaluation. 'What if' simulation of 3 cases: - Tower attack - Emerging threats - Implementation of security measures (i.e. the Introduction of the 3D Body Scanner)	***1* Problem setting** Presentation of the problem ***2* Collaborative Inquiry** Group activity aimed at addressing the problem and take the decision. The decision taking process is documented. ***3* Presentation and sharing of results** Each group does present the analysis and the decision-making process at the other groups.
SLOT 2. Visit to the airport Aiming to direct observation of airport sectors and facilities.	General overview of the airport infrastructures and externalities. Security infrastructure: admission rights and duties, IT security and physical security.
SLOT 3. Presentation and Dissemination to the ENAV Board of Airport Directors	
SLOT 4. Focus Group Aiming at presenting and discussing the models' structure and the computational mechanisms.	***1* Presentation of the models:** Each model is presented through focus on: input structure, main parameters and components, outputs, descriptive capacity, interactions, causal relations, computational effort, predictive capacity. ***2* Focused questions on:** Domain suitability, User acceptability and Technical Usability ***3* Discussion**
SLOT 5. Presentation of the tool Aiming at gathering feedback on the quality of model output, data visualization and functionality of the tool.	***1* Presentation and discussion of the visualization tool** Aiming at eliciting which information the stakeholders would need to get from the tool and in which shape.

Annex 11 - Online Focused Survey[5]

Acceptance of Security Measures by Airport Passengers

1. When did you last travel by plane?
Within □ last month □ last three month □ last six month □last year □ longer time ago □ never

2. Please specify your age
□ < 20 □ 21-30 □31-40 □41-50 □51-60 □ > 61

3. Gender
□ Female □ Male

4. Citizenship

5. Religion (in order to measure cultural differences)
□Islam □ Christianity □ Hinduism □ Buddhism □ Judaism □Other …..................

6. Including this flight, how many times have you taken international flight trips in the last two years?
□ 2 or less □3-4 □5-6 □7-8 □9-10 □ more than 10 times

7. What reasons do you usually travel by air for?
□ Business □ Holidays □ Education □ Family visit □ other

8. Please indicate the following procedures that are important for you during security check. You can indicate more than one.

□ CCTV (Close Circuit Television System/Camera System) monitoring
□ Hand search
□ Walk through metal detector
□ X-Ray Screening
□ Interaction with Security personnel
□ Full body screening
□ None

[5] The online survey represents an adaptation of the Istanbul Ataturk International Airport passenger survey developed by Dr. Nalan Ergün, Birsen Yörük Açıkel, Dr. Uğur Turhan, Anadolu University, The Faculty of Aeronautics and Astronautics.

9. Which of the following security procedures disturb you. You can indicate more than one.

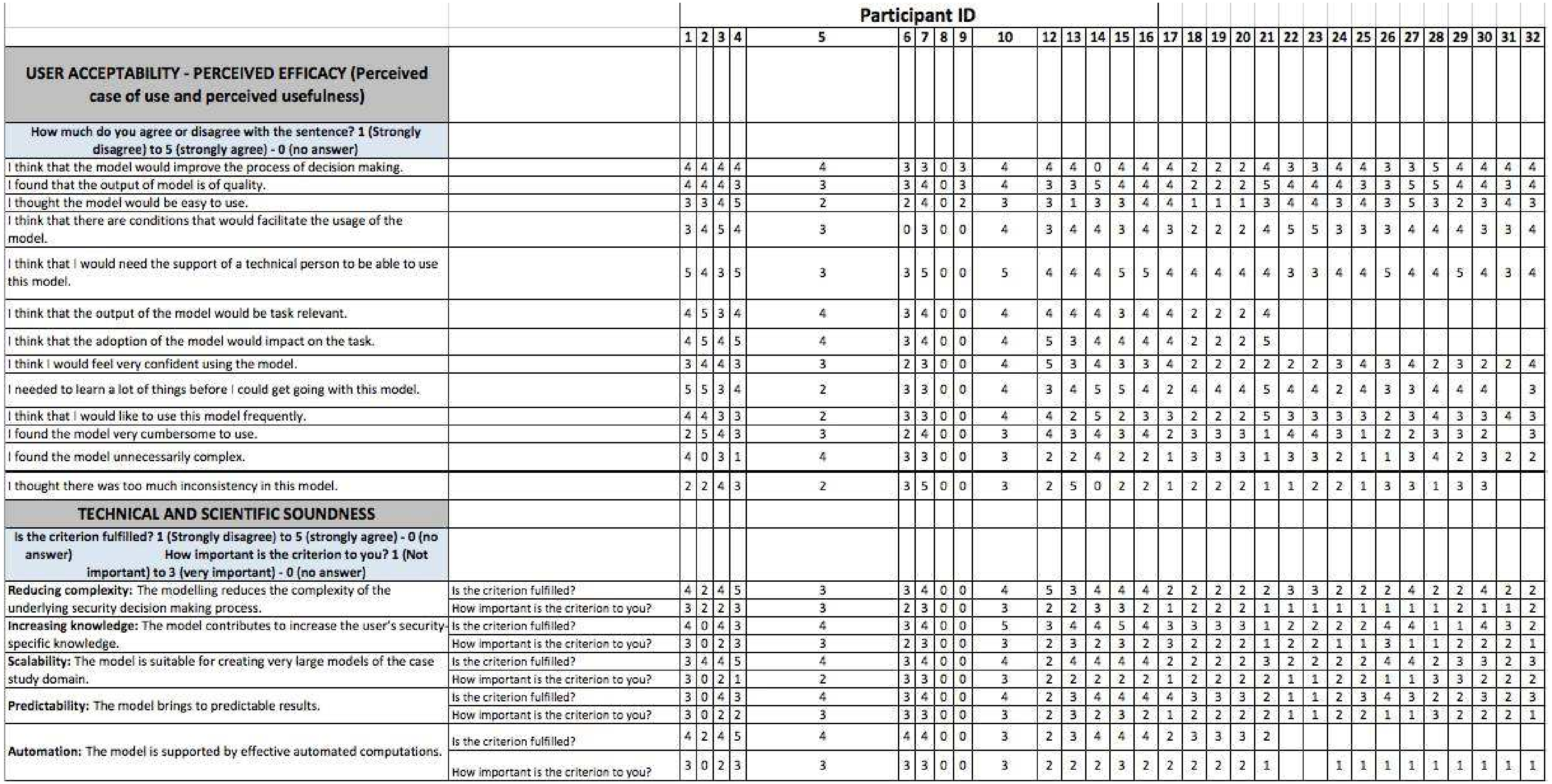
□ CCTV (Close Circuit Television System/Camera System) monitoring
□ Hand search
□ Walk-through metal detector
□ X-Ray Screening
□ Interaction with Security personnel
□ Full body screening
□ None

10. Please, express your agreement/disagreement with the following statements

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
1. Security devices do not threaten my health.					
2. Due to increased security measures at airports, I would prefer to use different means of transport.					
3. I encounter different treatment during security procedures due to my nationality.					
4. Security procedures at airports are sufficient to guarantee people safety.					
5. Security procedures lead to delays.					
6. Being randomly chosen for detailed security screening does not disturb me.					
7. I trust security personnel and security procedures.					
8. Due to my beliefs, I am subjected to additional security screening.					
9. Equipment enables security personnel to do their jobs professionally.					
10. I believe that security procedures ensure my safety when flying.					
11. Technological development is very important to ensure the reliability of security screening.					

Annex 12 - Validation Questionnaire - Full tables of results

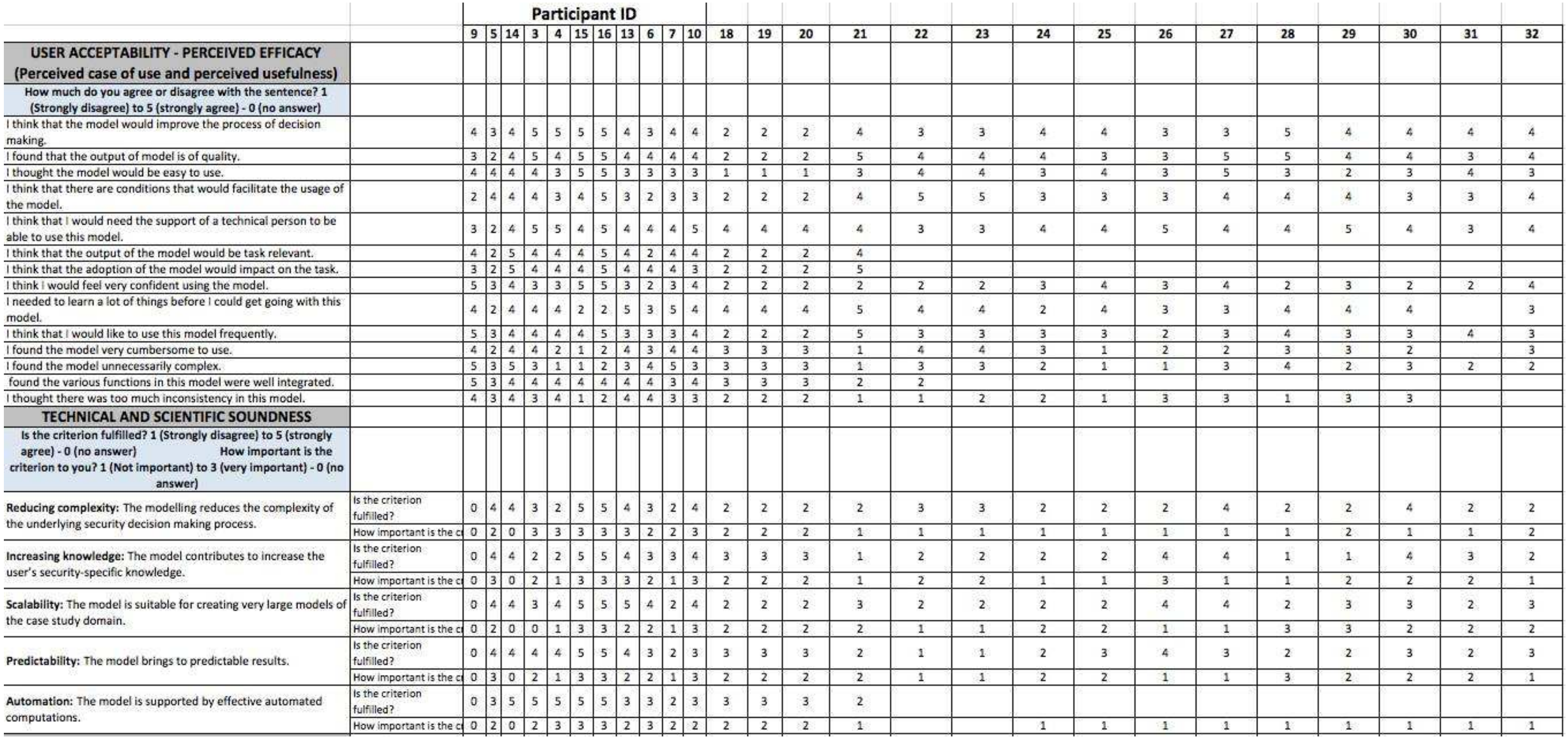
Cyberthreat Model



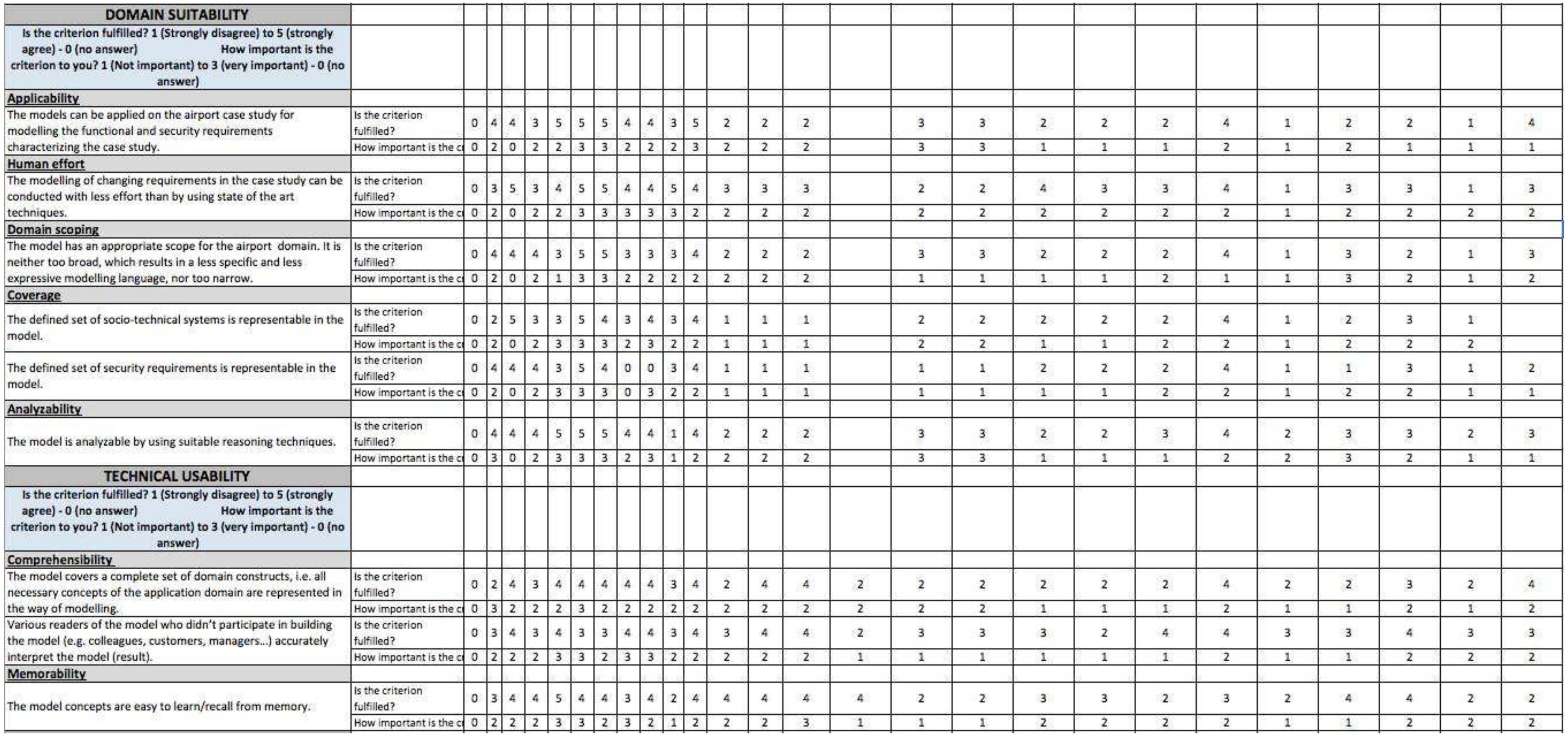
		Participant ID																														
		1	2	3	4	5	6	7	8	9	10	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
USER ACCEPTABILITY - PERCEIVED EFFICACY (Perceived case of use and perceived usefulness)																																
How much do you agree or disagree with the sentence? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer)																																
I think that the model would improve the process of decision making.		4	4	4	4	4	3	3	0	3	4	4	4	0	4	4	4	2	2	2	4	3	3	4	4	3	3	5	4	4	4	4
I found that the output of model is of quality.		4	4	4	3	3	3	4	0	3	4	3	3	5	4	4	4	2	2	2	5	4	4	4	3	3	5	5	4	4	3	4
I thought the model would be easy to use.		3	3	4	5	2	2	4	0	2	3	3	1	3	3	4	4	1	1	1	3	4	4	3	4	3	5	3	2	3	4	3
I think that there are conditions that would facilitate the usage of the model.		3	4	5	4	3	0	3	0	0	4	3	4	4	3	4	3	2	2	2	4	5	5	3	3	3	4	4	4	3	3	4
I think that I would need the support of a technical person to be able to use this model.		5	4	3	5	3	3	5	0	0	5	4	4	4	5	5	4	4	4	4	4	3	3	4	4	5	4	4	5	4	3	4
I think that the output of the model would be task relevant.		4	5	3	4	4	3	4	0	0	4	4	4	4	3	4	4	2	2	2	4											
I think that the adoption of the model would impact on the task.		4	5	4	5	4	3	4	0	0	4	5	3	4	4	4	4	2	2	2	5											
I think I would feel very confident using the model.		3	4	4	3	3	2	3	0	0	4	5	3	4	3	3	4	2	2	2	2	2	2	3	4	3	4	2	3	2	2	4
I needed to learn a lot of things before I could get going with this model.		5	5	3	4	2	3	3	0	0	4	3	4	5	5	4	2	4	4	4	5	4	4	2	4	3	3	4	4	4		3
I think that I would like to use this model frequently.		4	4	3	3	2	3	3	0	0	4	4	2	5	2	3	3	2	2	2	5	3	3	3	3	2	3	4	3	3	4	3
I found the model very cumbersome to use.		2	5	4	3	3	2	4	0	0	3	4	3	4	3	4	2	3	3	3	1	4	4	3	1	2	2	3	3	2		3
I found the model unnecessarily complex.		4	0	3	1	4	3	3	0	0	3	2	2	4	2	2	1	3	3	3	1	3	3	2	1	1	3	4	2	3	2	2
I thought there was too much inconsistency in this model.		2	2	4	3	2	3	5	0	0	3	2	5	0	2	2	1	2	2	2	1	1	2	2	1	3	3	1	3	3		
TECHNICAL AND SCIENTIFIC SOUNDNESS																																
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																																
Reducing complexity: The modelling reduces the complexity of the underlying security decision making process.	Is the criterion fulfilled?	4	2	4	5	3	3	4	0	0	4	5	3	4	4	4	2	2	2	2	2	3	3	2	2	2	4	2	2	4	2	2
	How important is the criterion to you?	3	2	2	3	3	2	3	0	0	3	2	2	3	3	2	1	2	2	2	1	1	1	1	1	1	1	1	2	1	1	2
Increasing knowledge: The model contributes to increase the user's security-specific knowledge.	Is the criterion fulfilled?	4	0	4	3	4	3	4	0	0	5	3	4	4	5	4	3	3	3	3	1	2	2	2	2	4	4	1	1	4	3	2
	How important is the criterion to you?	3	0	2	3	3	2	3	0	0	3	2	3	2	3	2	3	2	2	2	1	2	2	1	1	3	1	1	2	2	2	1
Scalability: The model is suitable for creating very large models of the case study domain.	Is the criterion fulfilled?	3	4	4	5	4	3	4	0	0	4	2	4	4	4	4	2	2	2	2	3	2	2	2	2	4	4	2	3	3	2	3
	How important is the criterion to you?	3	0	2	1	2	3	3	0	0	3	2	2	2	2	2	1	2	2	2	2	1	1	2	2	1	1	3	3	2	2	2
Predictability: The model brings to predictable results.	Is the criterion fulfilled?	3	0	4	3	4	3	4	0	0	4	2	3	4	4	4	4	3	3	3	2	1	1	2	3	4	3	2	2	3	2	3
	How important is the criterion to you?	3	0	2	2	3	3	3	0	0	3	2	3	2	3	2	1	2	2	2	2	1	1	2	2	1	1	3	2	2	2	1
Automation: The model is supported by effective automated computations.	Is the criterion fulfilled?	4	2	4	5	4	4	4	0	0	3	2	3	4	4	4	2	3	3	3	2											
	How important is the criterion to you?	3	0	2	3	3	3	3	0	0	3	2	2	2	3	2	2	2	2	2	1			1	1	1	1	1	1	1	1	1

DOMAIN SUITABILITY																																
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																																
Applicability																																
The models can be applied on the airport case study for modelling the functional and security requirements characterizing the case study.	Is the criterion fulfilled?	4	0	4	4	4	4	4	0	0	4	2	4	4	4	4		2	2	2		3	3	2	2	2	4	1	2	2	1	4
	How important is the criterion to you?	3	0	2	2	2	2	2	0	0	3	2	3	3	2	2		2	2	2		3	3	1	1	1	2	1	2	1	1	1
Human effort																																
The modelling of changing requirements in the case study can be conducted with less effort than by using state of the art techniques.	Is the criterion fulfilled?	0	0	4	4	5	4	4	0	0	4	2	3	3	5	4		3	3	3		2	2	4	3	3	4	1	3	3	1	3
	How important is the criterion to you?	0	0	2	3	3	3	2	0	0	2	2	2	2	3	2		2	2	2		2	2	2	2	2	2	1	2	2	2	2
Domain scoping																																
The model has an appropriate scope for the airport domain. It is neither too broad, which results in a less specific and less expressive modelling	Is the criterion fulfilled?	4	0	4	4	5	3	4	0	0	4	2	4	3	4	4		2	2	2		3	3	2	2	2	4	1	3	2	1	3
	How important is the criterion to you?	0	0	2	2	2	2	2	0	0	2	2	3	4	3	2		2	2	2		1	1	1	1	2	1	1	3	2	1	2
Coverage																																
The defined set of socio-technical systems is representable in the model.	Is the criterion fulfilled?	5	0	4	3	3	3	4	0	0	3	3	0	4	4	4		1	1	1		2	2	2	2	2	4	1	2	3	1	
	How important is the criterion to you?	3	0	2	2	2	3	2	0	0	2	2	0	0	3	2		1	1	1		2	2	1	1	2	2	1	2	2	2	
The defined set of security requirements is representable in the model.	Is the criterion fulfilled?	3	0	4	4	3	3	3	0	0	3	4	4	4	4	4		1	1	1		1	1	2	2	2	4	1	1	3	1	2
	How important is the criterion to you?	3	0	2	2	2	2	2	0	0	2	2	2	2	2	2		1	1	1		1	1	1	1	2	2	1	2	2	1	1
Analyzability																																
The model is analyzable by using suitable reasoning techniques.	Is the criterion fulfilled?	0	0	4	4	4	4	3	0	0	3	4	5	4	4	4		2	2	2		3	3	2	2	3	4	2	3	3	2	3
	How important is the criterion to you?	3	0	2	3	2	3	2	0	0	2	2	3	3	2	2		2	2	2		3	3	1	1	1	2	2	3	2	1	1
TECHNICAL USABILITY																																
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																																
Comprehensibility																																
The model covers a complete set of domain constructs, i.e. all necessary concepts of the application domain are represented in the way of modelling.	Is the criterion fulfilled?	3	0	4	0	2	3	3	0	0	3	5	4	4	4	4	2	2	4	4	2	2	2	2	2	2	4	2	2	3	2	4
	How important is the criterion to you?	3	0	2	0	2	2	2	0	0	2	3	3	2	2	2	1	2	2	2	2	2	2	1	1	1	2	1	1	2	1	2
Various readers of the model who didn't participate in building the model (e.g. colleagues, customers, managers…) accurately interpret the model	Is the criterion fulfilled?	3	0	4	0	4	3	3	0	0	3	5	4	4	4	4	2	3	4	4	2	3	3	3	2	4	4	3	3	4	3	3
	How important is the criterion to you?	3	0	2	0	1	3	2	0	0	2	3	2	2	2	2	1	2	2	2	1	1	1	1	1	1	2	1	1	2	2	2
Memorability																																
The model concepts are easy to learn/recall from memory.	Is the criterion fulfilled?	4	0	4	0	3	2	3	0	0	4	5	2	4	4	4	3	4	4	4	4	2	2	3	3	2	3	2	4	4	2	2
	How important is the criterion to you?	3	0	2	0	2	3	2	0	0	3	3	3	2	3	2	2	2	2	3	1	1	1	2	2	2	2	1	1	2	2	2
COMMENTS																																
When you **rather or strongly disagreed** with the fulfilment of criteria, what were the reasons? Please make a list of problem issues for the model		0	0	0	0	Model can be perfect but it is all about the applicability. Whatever you can do is limited by the awareness of the operators and technical staff	0	0	0	0	Model is simple but reuires experienced staff apply	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

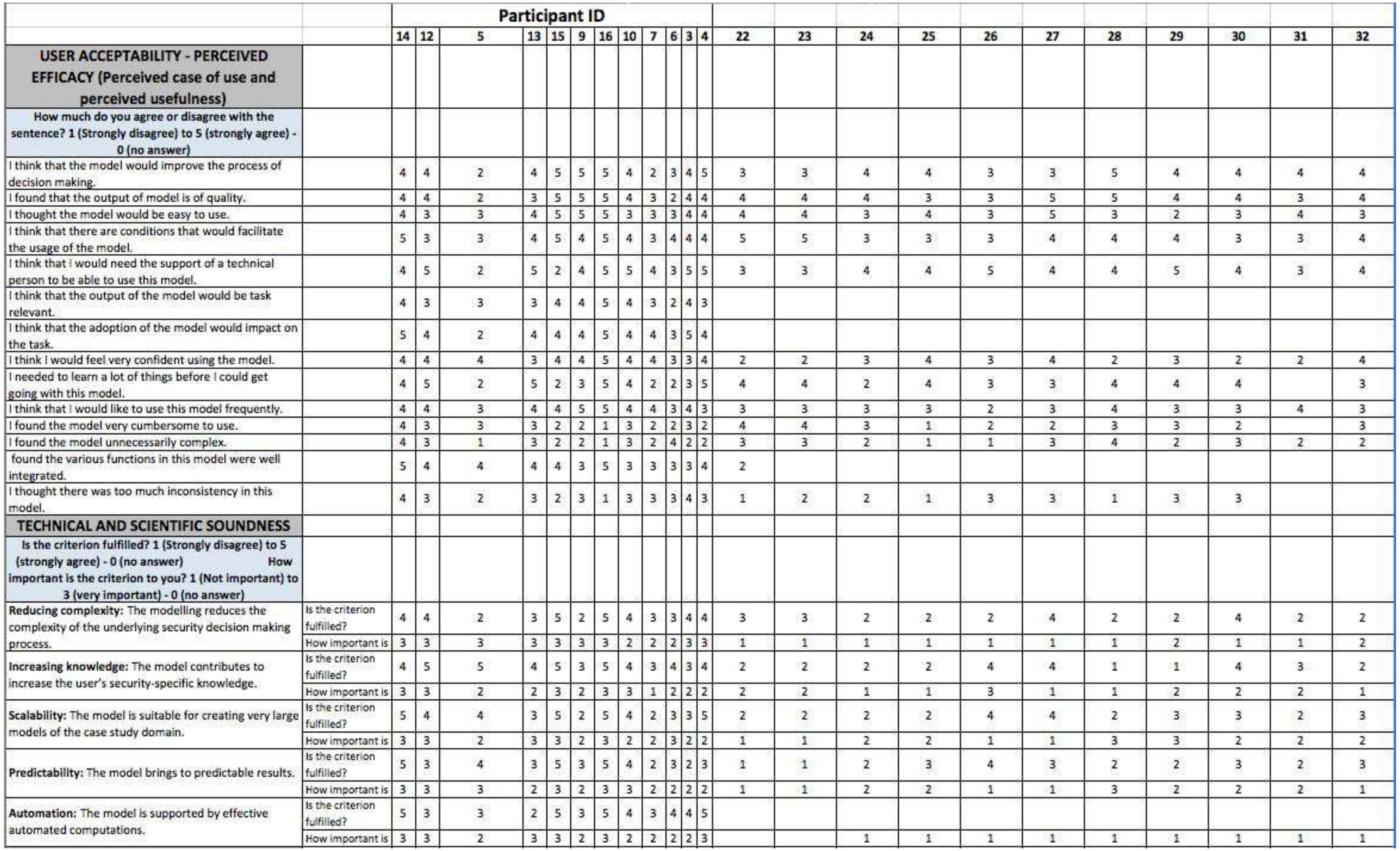
Attack to Tower Model



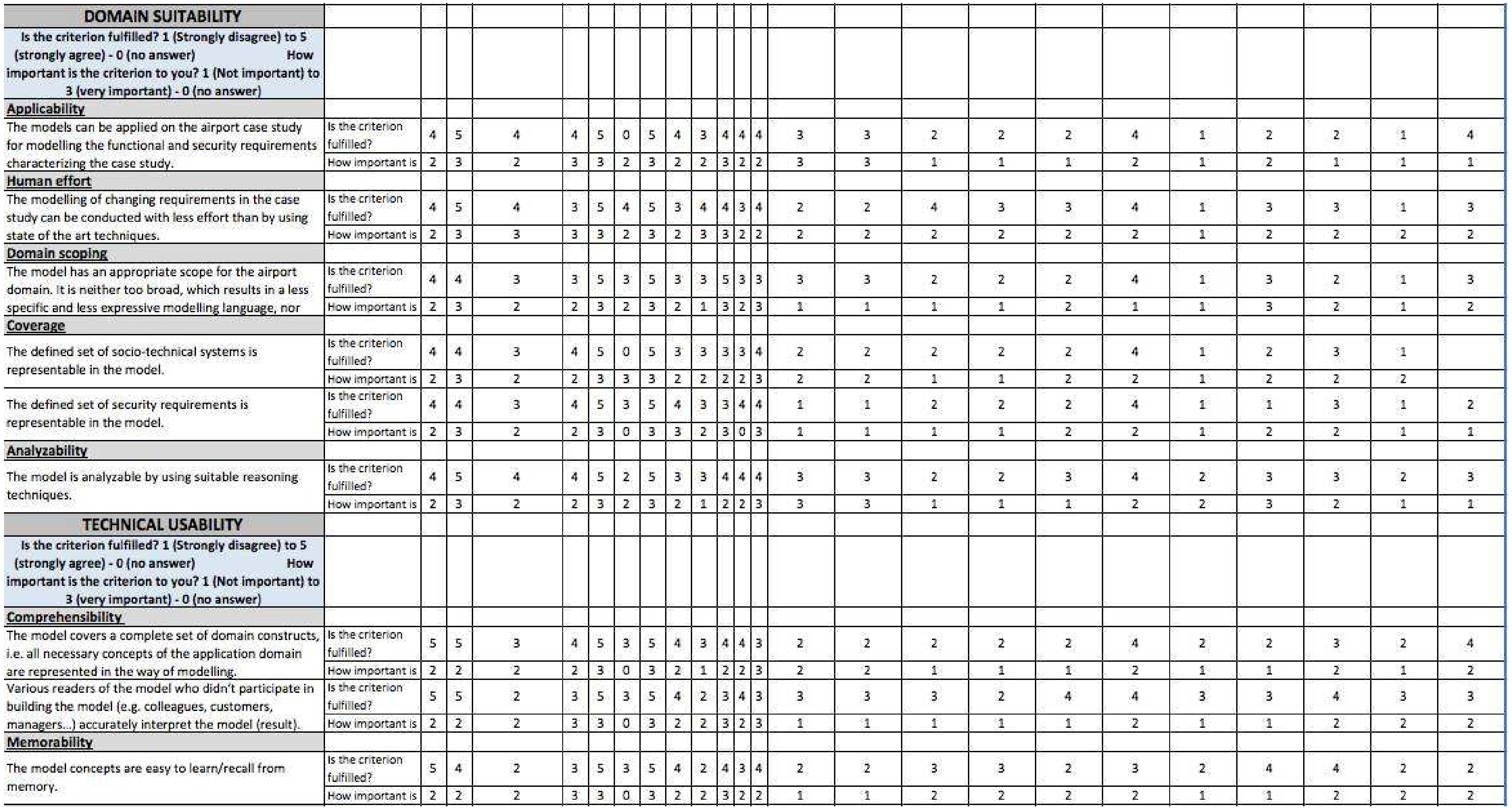
		Participant ID																									
		9	5	14	3	4	15	16	13	6	7	10	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
USER ACCEPTABILITY - PERCEIVED EFFICACY (Perceived case of use and perceived usefulness)																											
How much do you agree or disagree with the sentence? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer)																											
I think that the model would improve the process of decision making.		4	3	4	5	5	5	5	4	3	4	4	2	2	2	4	3	3	4	4	3	3	5	4	4	4	4
I found that the output of model is of quality.		3	2	4	5	4	5	5	4	4	4	4	2	2	2	5	4	4	4	3	3	5	5	4	4	3	4
I thought the model would be easy to use.		4	4	4	4	3	5	5	3	3	3	3	1	1	1	3	4	4	3	4	3	5	3	2	3	4	3
I think that there are conditions that would facilitate the usage of the model.		2	4	4	4	3	4	5	3	2	3	3	2	2	2	4	5	5	3	3	3	4	4	4	3	3	4
I think that I would need the support of a technical person to be able to use this model.		3	2	4	5	5	4	5	4	4	4	5	4	4	4	4	3	3	4	4	5	4	4	5	4	3	4
I think that the output of the model would be task relevant.		4	2	5	4	4	4	5	4	2	4	4	2	2	2	4											
I think that the adoption of the model would impact on the task.		3	2	5	4	4	4	5	4	4	4	3	2	2	2	5											
I think I would feel very confident using the model.		5	3	4	3	3	5	5	3	2	3	4	2	2	2	2	2	2	3	4	3	4	2	3	2	2	4
I needed to learn a lot of things before I could get going with this model.		4	2	4	4	4	2	2	5	3	5	4	4	4	4	5	4	4	2	4	3	3	4	4	4		3
I think that I would like to use this model frequently.		5	3	4	4	4	4	5	3	3	3	4	2	2	2	5	3	3	3	3	2	3	4	3	3	4	3
I found the model very cumbersome to use.		4	2	4	4	2	1	2	4	3	4	4	3	3	3	1	4	4	3	1	2	2	3	3	2		3
I found the model unnecessarily complex.		5	3	5	3	1	1	2	3	4	5	3	3	3	3	1	3	3	2	1	1	3	4	2	3	2	2
found the various functions in this model were well integrated.		5	3	4	4	4	4	4	4	4	3	4	3	3	3	2	2										
I thought there was too much inconsistency in this model.		4	3	4	3	4	1	2	4	4	3	3	2	2	2	1	1	2	2	1	3	3	1	3	3		
TECHNICAL AND SCIENTIFIC SOUNDNESS																											
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																											
Reducing complexity: The modelling reduces the complexity of the underlying security decision making process.	Is the criterion fulfilled?	0	4	4	3	2	5	5	4	3	2	4	2	2	2	2	3	3	2	2	2	4	2	2	4	2	2
	How important is the cı	0	2	0	3	3	3	3	3	2	2	3	2	2	2	1	1	1	1	1	1	1	1	2	1	1	2
Increasing knowledge: The model contributes to increase the user's security-specific knowledge.	Is the criterion fulfilled?	0	4	4	2	2	5	5	4	3	3	4	3	3	3	1	2	2	2	2	4	4	1	1	4	3	2
	How important is the cı	0	3	0	2	1	3	3	3	2	1	3	2	2	2	1	2	2	1	1	3	1	1	2	2	2	1
Scalability: The model is suitable for creating very large models of the case study domain.	Is the criterion fulfilled?	0	4	4	3	4	5	5	5	4	2	4	2	2	2	3	2	2	2	2	4	4	2	3	3	2	3
	How important is the cı	0	2	0	0	1	3	3	2	2	1	3	2	2	2	2	1	1	2	2	1	1	3	3	2	2	2
Predictability: The model brings to predictable results.	Is the criterion fulfilled?	0	4	4	4	4	5	5	4	3	2	3	3	3	3	2	1	1	2	3	4	3	2	2	3	2	3
	How important is the cı	0	3	0	2	1	3	3	2	2	1	3	2	2	2	2	1	1	2	2	1	1	3	2	2	2	1
Automation: The model is supported by effective automated computations.	Is the criterion fulfilled?	0	3	5	5	5	5	5	3	3	2	3	3	3	3	2											
	How important is the cı	0	2	0	2	3	3	3	2	3	2	2	2	2	2	1			1	1	1	1	1	1	1	1	1



DOMAIN SUITABILITY																											
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																											
Applicability																											
The models can be applied on the airport case study for modelling the functional and security requirements characterizing the case study.	Is the criterion fulfilled?	0	4	4	3	5	5	5	4	4	3	5	2	2	2		3	3	2	2	2	4	1	2	2	1	4
	How important is the cr	0	2	0	2	2	3	3	2	2	2	3	2	2	2		3	3	1	1	1	2	1	2	1	1	1
Human effort																											
The modelling of changing requirements in the case study can be conducted with less effort than by using state of the art techniques.	Is the criterion fulfilled?	0	3	5	3	4	5	5	4	4	5	4	3	3	3		2	2	4	3	3	4	1	3	3	1	3
	How important is the cr	0	2	0	2	2	3	3	3	3	3	2	2	2	2		2	2	2	2	2	2	1	2	2	2	2
Domain scoping																											
The model has an appropriate scope for the airport domain. It is neither too broad, which results in a less specific and less expressive modelling language, nor too narrow.	Is the criterion fulfilled?	0	4	4	4	3	5	5	3	3	3	4	2	2	2		3	3	2	2	2	4	1	3	2	1	3
	How important is the cr	0	2	0	2	1	3	3	2	2	2	2	2	2	2		1	1	1	1	2	1	1	3	2	1	2
Coverage																											
The defined set of socio-technical systems is representable in the model.	Is the criterion fulfilled?	0	2	5	3	3	5	4	3	4	3	4	1	1	1		2	2	2	2	2	4	1	2	3	1	
	How important is the cr	0	2	0	2	3	3	3	2	3	2	2	1	1	1		2	2	1	1	2	2	1	2	2	2	
The defined set of security requirements is representable in the model.	Is the criterion fulfilled?	0	4	4	4	3	5	4	0	0	3	4	1	1	1		1	1	2	2	2	4	1	1	3	1	2
	How important is the cr	0	2	0	2	3	3	3	0	3	2	2	1	1	1		1	1	1	1	2	2	1	2	2	1	1
Analyzability																											
The model is analyzable by using suitable reasoning techniques.	Is the criterion fulfilled?	0	4	4	4	5	5	5	4	4	1	4	2	2	2		3	3	2	2	3	4	2	3	3	2	3
	How important is the cr	0	3	0	2	3	3	3	2	3	1	2	2	2	2		3	3	1	1	1	2	2	3	2	1	1
TECHNICAL USABILITY																											
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																											
Comprehensibility																											
The model covers a complete set of domain constructs, i.e. all necessary concepts of the application domain are represented in the way of modelling.	Is the criterion fulfilled?	0	2	4	3	4	4	4	4	4	3	4	2	4	4	2	2	2	2	2	2	4	2	2	3	2	4
	How important is the cr	0	3	2	2	2	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	2	1	1	2	1	2
Various readers of the model who didn't participate in building the model (e.g. colleagues, customers, managers...) accurately interpret the model (result).	Is the criterion fulfilled?	0	3	4	3	4	3	3	4	4	3	4	3	4	4	2	3	3	3	2	4	4	3	3	4	3	3
	How important is the cr	0	2	2	2	3	3	2	3	3	2	2	2	2	2	1	1	1	1	1	1	2	1	1	2	2	2
Memorability																											
The model concepts are easy to learn/recall from memory.	Is the criterion fulfilled?	0	3	4	4	5	4	4	3	4	2	4	4	4	4	4	2	2	3	3	2	3	2	4	4	2	2
	How important is the cr	0	2	2	2	3	3	2	3	2	1	2	2	2	3	1	1	1	2	2	2	2	1	1	2	2	2



		Participant ID																						
		14	12	5	13	15	9	16	10	7	6	3	4	22	23	24	25	26	27	28	29	30	31	32
USER ACCEPTABILITY - PERCEIVED EFFICACY (Perceived case of use and perceived usefulness)																								
How much do you agree or disagree with the sentence? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer)																								
I think that the model would improve the process of decision making.		4	4	2	4	5	5	5	4	2	3	4	5	3	3	4	4	3	3	5	4	4	4	4
I found that the output of model is of quality.		4	4	2	3	5	5	5	4	3	2	4	4	4	4	4	3	3	5	5	4	4	3	4
I thought the model would be easy to use.		4	3	3	4	5	5	5	3	3	3	4	4	4	4	3	4	3	5	3	2	3	4	3
I think that there are conditions that would facilitate the usage of the model.		5	3	3	4	5	4	5	4	3	4	4	4	5	5	3	3	3	4	4	4	3	3	4
I think that I would need the support of a technical person to be able to use this model.		4	5	2	5	2	4	5	5	4	3	5	5	3	3	4	4	5	4	4	5	4	3	4
I think that the output of the model would be task relevant.		4	3	3	3	4	4	5	4	3	2	4	3											
I think that the adoption of the model would impact on the task.		5	4	2	4	4	4	5	4	4	3	5	4											
I think I would feel very confident using the model.		4	4	4	3	4	4	5	4	4	3	3	4	2	2	3	4	3	4	2	3	2	2	4
I needed to learn a lot of things before I could get going with this model.		4	5	2	5	2	3	5	4	2	2	3	5	4	4	2	4	3	3	4	4	4		3
I think that I would like to use this model frequently.		4	4	3	4	4	5	5	4	4	3	4	3	3	3	3	3	2	3	4	3	3	4	3
I found the model very cumbersome to use.		4	3	3	3	2	2	1	3	2	2	3	2	4	4	3	1	2	2	3	3	2		3
I found the model unnecessarily complex.		4	3	1	3	2	2	1	3	2	4	2	2	3	3	2	1	1	3	4	2	3	2	2
found the various functions in this model were well integrated.		5	4	4	4	4	3	5	3	3	3	3	4	2										
I thought there was too much inconsistency in this model.		4	3	2	3	2	3	1	3	3	3	4	3	1	2	2	1	3	3	1	3	3		
TECHNICAL AND SCIENTIFIC SOUNDNESS																								
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																								
Reducing complexity: The modelling reduces the complexity of the underlying security decision making process.	Is the criterion fulfilled?	4	4	2	3	5	2	5	4	3	3	4	4	3	3	2	2	2	4	2	2	4	2	2
	How important is	3	3	3	3	3	3	3	2	2	2	3	3	1	1	1	1	1	1	1	2	1	1	2
Increasing knowledge: The model contributes to increase the user's security-specific knowledge.	Is the criterion fulfilled?	4	5	5	4	5	3	5	4	3	4	3	4	2	2	2	2	4	4	1	1	4	3	2
	How important is	3	3	2	2	3	2	3	3	1	2	2	2	2	2	1	1	3	1	1	2	2	2	1
Scalability: The model is suitable for creating very large models of the case study domain.	Is the criterion fulfilled?	5	4	4	3	5	2	5	4	2	3	3	5	2	2	2	2	4	4	2	3	3	2	3
	How important is	3	3	2	3	3	2	3	2	2	3	2	2	1	1	2	2	1	1	3	3	2	2	2
Predictability: The model brings to predictable results.	Is the criterion fulfilled?	5	3	4	3	5	3	5	4	2	3	2	3	1	1	2	3	4	3	2	2	3	2	3
	How important is	3	3	3	2	3	2	3	3	2	2	2	2	1	1	2	2	1	1	3	2	2	2	1
Automation: The model is supported by effective automated computations.	Is the criterion fulfilled?	5	3	3	2	5	3	5	4	3	4	4	5											
	How important is	3	3	2	3	3	2	3	2	2	2	2	3			1	1	1	1	1	1	1	1	1



DOMAIN SUITABILITY																								
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																								
Applicability																								
The models can be applied on the airport case study for modelling the functional and security requirements characterizing the case study.	Is the criterion fulfilled?	4	5	4	4	5	0	5	4	3	4	4	4	3	3	2	2	2	4	1	2	2	1	4
	How important is	2	3	2	3	3	2	3	2	2	3	2	2	3	3	1	1	1	2	1	2	1	1	1
Human effort																								
The modelling of changing requirements in the case study can be conducted with less effort than by using state of the art techniques.	Is the criterion fulfilled?	4	5	4	3	5	4	5	3	4	4	3	4	2	2	4	3	3	4	1	3	3	1	3
	How important is	2	3	3	3	3	2	3	2	3	3	2	2	2	2	2	2	2	2	1	2	2	2	2
Domain scoping																								
The model has an appropriate scope for the airport domain. It is neither too broad, which results in a less specific and less expressive modelling language, nor	Is the criterion fulfilled?	4	4	3	3	5	3	5	3	3	5	3	3	3	3	2	2	2	4	1	3	2	1	3
	How important is	2	3	2	2	3	2	3	2	1	3	2	3	1	1	1	1	2	1	1	3	2	1	2
Coverage																								
The defined set of socio-technical systems is representable in the model.	Is the criterion fulfilled?	4	4	3	4	5	0	5	3	3	3	3	4	2	2	2	2	2	4	1	2	3	1	
	How important is	2	3	2	2	3	3	3	2	2	2	2	3	2	2	1	1	2	2	1	2	2	2	
The defined set of security requirements is representable in the model.	Is the criterion fulfilled?	4	4	3	4	5	3	5	4	3	3	4	4	1	1	2	2	2	4	1	1	3	1	2
	How important is	2	3	2	2	3	0	3	3	2	3	0	3	1	1	1	1	2	2	1	2	2	1	1
Analyzability																								
The model is analyzable by using suitable reasoning techniques.	Is the criterion fulfilled?	4	5	4	4	5	2	5	3	3	4	4	4	3	3	2	2	3	4	2	3	3	2	3
	How important is	2	3	2	2	3	2	3	2	1	2	2	3	3	3	1	1	1	2	2	3	2	1	1
TECHNICAL USABILITY																								
Is the criterion fulfilled? 1 (Strongly disagree) to 5 (strongly agree) - 0 (no answer) How important is the criterion to you? 1 (Not important) to 3 (very important) - 0 (no answer)																								
Comprehensibility																								
The model covers a complete set of domain constructs, i.e. all necessary concepts of the application domain are represented in the way of modelling.	Is the criterion fulfilled?	5	5	3	4	5	3	5	4	3	4	4	3	2	2	2	2	2	4	2	2	3	2	4
	How important is	2	2	2	2	3	0	3	2	1	2	2	3	2	2	1	1	1	2	1	1	2	1	2
Various readers of the model who didn't participate in building the model (e.g. colleagues, customers, managers...) accurately interpret the model (result).	Is the criterion fulfilled?	5	5	2	3	5	3	5	4	2	3	4	3	3	3	3	2	4	4	3	3	4	3	3
	How important is	2	2	2	3	3	0	3	2	2	3	2	3	1	1	1	1	1	2	1	1	2	2	2
Memorability																								
The model concepts are easy to learn/recall from memory.	Is the criterion fulfilled?	5	4	2	3	5	3	5	4	2	4	3	4	2	2	3	3	2	3	2	4	4	2	2
	How important is	2	2	2	3	3	0	3	2	2	3	2	2	1	1	2	2	2	2	1	1	2	2	2