PROJECT FINAL REPORT

Grant Agreement number: 285663

Project acronym: INNOSEC

Project title: INNOvation Management Models for SECurity Organisations

Funding Scheme: Collaborative Project

Date of latest version of Annex I against which the assessment will be made:

Period covered: from 01/02/2012 to 31/01/2014

Name, title and organisation of the scientific representative of the project's coordinator[1]:

Mrs. Amaia Sopelana

Fundación Tecnalia Research & Innovation

Tel: +34 946 400 450

Fax:

E-mail: amaia.sopelana@tecnalia.com

Project website[2] address: http://www.innosec-project.eu

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

[2] The home page of the website should contain the generic European flag and the FP7 logo which are available in electronic format at the Europa website (logo of the European flag: http://europa.eu/abc/symbols/emblem/index_en.htm logo of the 7th FP: http://ec.europa.eu/research/fp7/index_en.cfm?pg=logos). The area of activity of the project should also be mentioned.

Table of contents

1. Final publishable summary report 1

1.1 Executive summary 1

1.2 The INNOSEC project and objectives 1

1.3 Main S & T results/foregrounds 4

1.4 Potential impact and the main dissemination activities and exploitation of results 17

1.5 INNOSEC details: contact details and address of the project website 19

2. Use and dissemination of foreground 20

2.1 Section A (public) 20

Abbreviations

SO	Security Organisation
IM	Innovation Model
IP	Innovation Practice

1. Final publishable summary report

This report corresponds to the Final Report of the INNOSEC project. This document aims at including general information of the project's objectives and the research approach that has been followed by the consortium as well as the results achieved during the whole lifecycle of the project, two years. It also covers a list of the dissemination activities that have been developed during that period. And lastly, the future plans for exploitation.

1.1 Executive summary

The INNOSEC project has addressed the need of European Security Organisations (SOs) of implementing, effectively and efficiently, an innovation management model. The project has produced a unique modular model, together with an implementation roadmap and a web-based supporting tool, for implementing and improving innovation management in public and private security end-users. Titled as 'INNOSEC model', it represents the response to security sector demands of an innovation management model that was adaptable to the features of SOs providing with tools for evaluation and instructions for decision-making according to their organisational capacities and needs.

The 'INNOSEC model' is unique because it is devoted to security organisations, it is simple and efficient to use, it is composed by easily understandable modules which can be ranked in preference by the organization, allows SOs to evaluate the current situation (as-is) and the desired (to-be) maturity level of innovativeness, it is technology independent and flexible regardless organization type, size and culture, and ready to be implemented with or without external support.

INNOSEC model enables SOs to go beyond the simple procurement process, enhancing the ability to identify, assess and test innovation, streamlining the innovation process from ideation stage going through selecting and designing stage towards implementation stage (of the new service or a new technology), and reinforcing cooperation with peer organizations and technology and service providers. All in all, INNOSEC strengthens public-private dialogue for the access and absorption of innovation.

The European co-operation project coordinated by Tecnalia was performed by a selected team of research and technology centres that are experts in technology innovation, technology transfer and security sector research. The user-driven approach was ensured by three case studies provided by Security Organizations (project's partners) that have served to derive requirements upon the model, roadmap and web-tool being developed and to test the solutions developed as organisational demonstrators. The partners are coming from United Kingdom, Germany, Spain, Austria, Finland, Netherlands and Sweden. Additionally, several associated security organizations, external to the consortium, contributed with experiences, insights and invaluable recommendations.

1.2 The INNOSEC project and objectives

Framework of today's security organisations exhibits fundamental weaknesses for managing an innovation system based on, among others, networked activities, as a key factor within these type of organisations. Generally speaking, INNOSEC project was challenged with implementing and sustaining innovation management for security organisations. Since they are immerse in the uncertainty and

dynamism of a global knowledge-based environment, increasing their innovation capacity immediately could be able to translate into increasing efficiency and effectiveness in the provision of security as a service for the European citizens.

Therefore, the objective of developing a modular model for innovation and innovation management was based on providing the security organisations the opportunity to adapt its modules that could be more convenient in terms of their current innovation requirements and situation related to the coordination with other stakeholders to deliver effective and efficient security services to the society.

The modular model has not been built from scratch. The multiple security organisations currently have basic innovation management systems, most of them relying on service systems (provision of hardware, software, and consultancy, in general) provided in the market by a big number of suppliers, sometimes not explicitly specialised in security applications. Then, security organisations have been forced to develop their innovation initiatives upon several building blocks not designed under their own requirements for its usage. Besides, for them, most of the operational missions are conducted with time-pressure and with difficulties to gather and analyse relevant data to conveniently formulate citizens or customers' requirements, especially for the medium and long terms, which causes disequilibrium toward the offer side (offer push).

To achieve the aforementioned objective, the research methodology of INNOSEC project was orientated towards the development of the following elements:

1) A modular innovation model for innovation management representing an integral framework of five modules that can be implemented independently (including guidelines for the use of them) to support the creation and/or management of:
    a. Innovation Strategy
    b. Innovation Process: Ideation, Selecting and Designing, Implementation
    c. Innovation Culture including readiness of people for innovation and learning processes.
2) An implementation roadmap for INNOSEC model, to guide security companies towards successful organisational change strategies which enhance innovation capacities.
3) A web-based support tool (supported by project the web-site) which assists security organisations in putting in practice the guidelines and the modules of the INNOSEC model.

The results of the project enabled the three security organisations participating in the project to streamline their current innovation process and capacities. Recently, some exploitation and dissemination activities of the ‘INNOSEC model’ have allowed other European security organisations to benefit from the results of the research project.

INNOSEC model was conceptualized expecting to address some research challenges (see Figure 1) that are listed below.

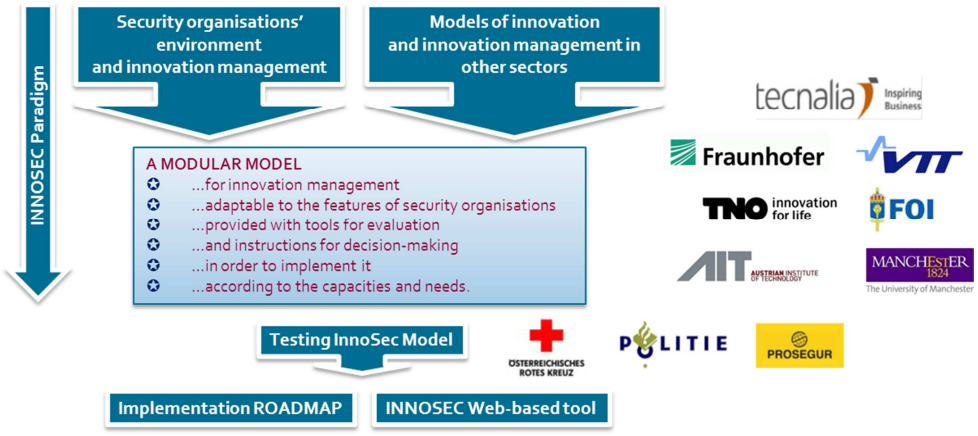

Figure 1: INNOSEC project overview

The first research challenge concerned to understand, from a multidisciplinary viewpoint, how security organisations interpret most critical needs of change, how they address innovation management to accomplish the requirements from uncertain environmental changes, how their structural and cultural organisational conditions facilitate or impede successful innovation initiatives. The research activities were thus focused on analysing the operating environment and its impact on the innovation management of SOs, on identifying security organisations' current practices of innovation management in selected segments of the security sector and how they interact with their specific environments. Finally, key issues arising from the analysis were synthesised and lessons for the development of the innovation model were drawn.

To identify and characterise relevant new models of innovation management constituted the second research challenge. Hence, the project addressed the analysis of innovation management practices in non-security sectors and the development of a typology of these innovation models and practices with respect to their suitability for different types of embedding organisational environments. The selection of those non-security sectors was based on a set of criteria that ensured a high degree of comparability with the security sector (for instance, the mixed public-private character of organisations, the service character of the outputs delivered by the organisations in the sector, the advanced nature of the innovation practices in the sector, the fast pace of change and turbulence in the environment of the organisations of the sector, or a high-degree of inter-organisational networking in innovation).

The third challenge was to develop a supporting model for innovation management in security organisations, under the consideration of organisational responsiveness issues, to meet the real needs of citizens' security topics, fostering a networked innovation landscape, and consequently avoiding inadequate innovation initiatives. Based on the outcomes from previous specifications described, the consortium proposed to develop a first version of a modular innovation model which helps SOs in innovation management in each of the phases of the overall process:

- providing them with the best adaptation of tools for the identification of innovation opportunities and available technology for the innovation design (including foresight methods for the development of technology and operation environment, road mapping, scenario techniques etc.);

- helping them in networked R&D and search of new business models in the development of innovation; and,

- giving them support in the definition of the organisational conditions for the implementation of innovations and new technologies (such as the promotion of innovation culture, the creation of dynamic capabilities that foster explorative initiatives with the adequate design of structural conditions to improve the adaptation capability of security organisations as end-users).

The user-driven approach was, therefore, unavoidable and a fourth challenge came from the necessity of customising and testing of the first version of the modular Innovation Model in the SOs of the project with the main objective of refining it. The testing process allowed the consortium's security organisations to familiarise with the innovation model and to partially or totally implement its modules into the innovation procedures. As a complementary element for testing the model, the project was aimed at providing an organisational learning landscape in which the insights and knowledge were shared, transferred and elaborated in a collaborative way with security organisations. All this was proposed to promote the adaptation of the model in their organisational characteristics and finally to refine the first version of the 'INNOSEC model'.

To develop an appropriate implementation roadmap which could guide security companies towards successful implementation of INNOSEC model was the fifth challenge of the project. In order to address this challenge, the proposed research approach was based on activities developed previously in order to identify and elaborate the implementation building blocks of 'INNOSEC model'. The modularity of the model was especially amenable to such building block approach. However, successful implementation requires also building blocks that address human-centred and motivational aspects of implementation in a more holistic way. Aspects such as tools (ICT solutions), use of new technologies for ICT-solutions (e.g. web 2.0), organisational change, training and education and legislative and institutional measures were going to be considered.

Lastly, the sixth aim was the development of a prototype of a web-based tool (supported by project the web-site) to provide support to SOs in putting in practice the guidelines and the modules of the 'INNOSEC model' according to their organizational characteristics. The supporting tool was aimed at stimulating SOs to acquire knowledge and experience applying the 'INNOSEC model' and its associated modules.

1.3 Main S & T results/foregrounds

Based on the aforementioned challenges, the main results of the project, from a general perspective, were:

'INNOSEC model': modular model for innovation management in security organisations

The INNOSEC innovation model consists of five modules with a Guideline for the use of the model. The modules are: Innovation Strategy, Ideation, Selecting and Designing, Implementation, and People, Culture and Learning (Figure 2). The Innovation Strategy module deals with strategic level of innovation management and it helps a security organisation to formulate the long-term innovation direction and goals of the organisation. Ideation, Selecting and Designing, and Implementation are the process phase modules in the INNOSEC model. The Ideation module aims to present a systematic approach for identifying and introducing new innovations in the security sector. The Selecting and Designing module helps a security organisation to take immature ideas from the Ideation to refine and evaluate them, and design them so

that they can be efficiently and effectively implemented. The Implementation module gives guidance to the implementation of new technology into existing security service and to the development and implementation of new security services into organisational processes. The module People, Culture and Learning aims to explain why innovation belongs to everybody, what kind of leadership and management is needed, how to develop culture of continuous innovation, and how to support organisational learning and change management.

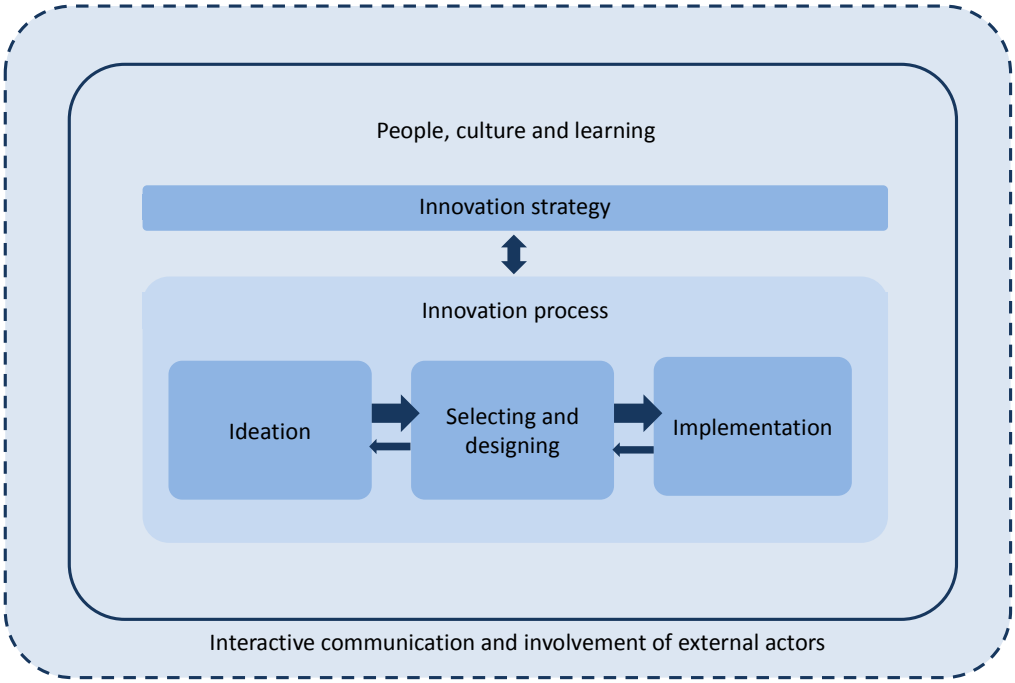

Figure 2: Overview of INNOSEC model and modules (*source: Deliverable 4.3*)

The idea and paradigm behind the modular model is to give flexibility for the security organisations to implement INNOSEC results of innovation management and respect for current practices in general management and operation. A security organisation may choose to implement the whole model or just the modules it finds feasible for them. Nonetheless, the consortium underlines the fact that the model described here is comprehensive and generic, while its actual implementation will in most cases require some customisation and adaptation.

The modules and its elements are described as follows:

Module: Innovation strategy

An innovation strategy refers to the part of an organisation's strategy that deals with the growth of the organisation through the development of new products, services, processes or business models, i.e. innovation. It is a long-term plan of action on how to use the development of new products, services, processes or business models to achieve the organisation's objectives/ missions.

The innovation strategy is typically a part of the organisational strategy. It helps to formulate the innovation goals of the organisation and provide an overall coherence for the innovation activities of the organisation. The innovation strategy within our model consists of three elements (Figure 3): (i) the

framework for innovation strategy; (ii) the innovation strategy process; and (iii) the innovation strategy content.

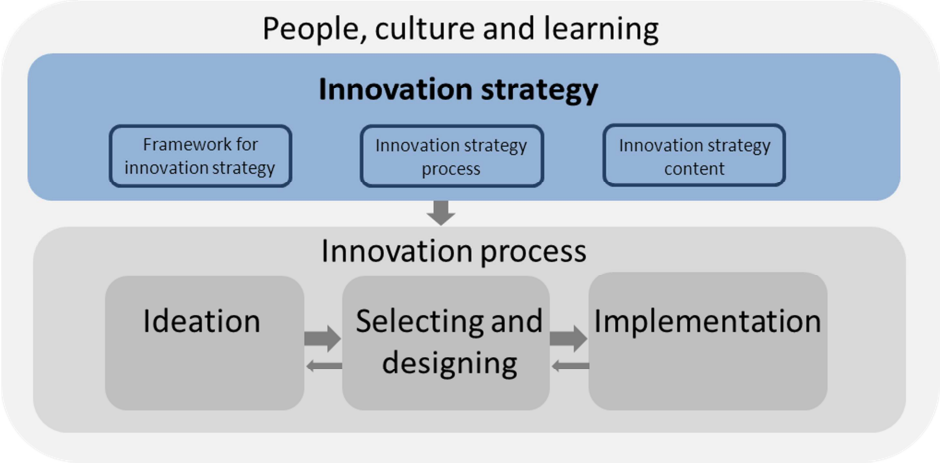

Figure 3: Elements of Innovation Strategy module (*source: Deliverable 4.3*)

Module: Ideation

Ideation is the first process phase module in the INNOSEC model. It consists of three elements (Figure 4): searching; idea generation; and idea management. It aims to present a systematic approach for identifying and introducing new innovations in the security sector through a distinct and proper search strategy incorporating market and environment monitoring to enable identification of new ideas and technologies that are relevant to the organisation (and aligned to its strategy).

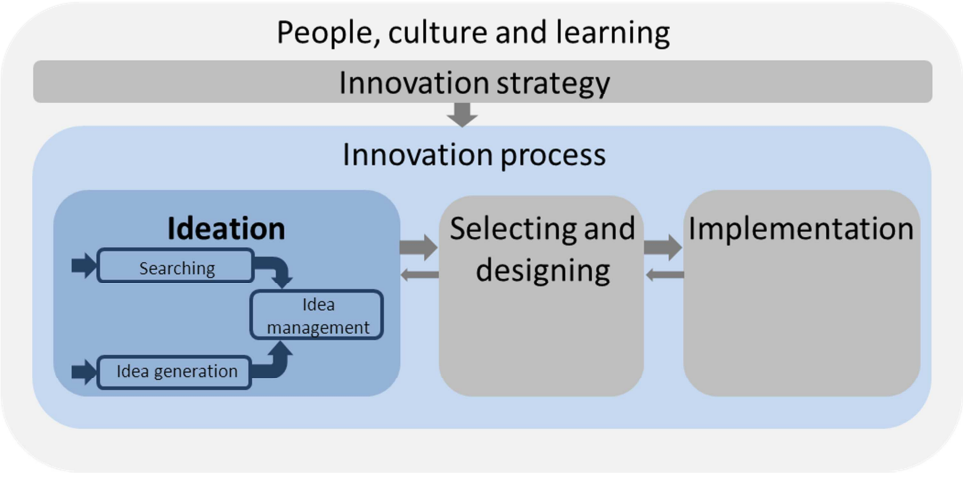

Figure 4: Elements of Ideation module (*source: Deliverable 4.3*)

Module: Selecting and designing

Selecting and designing is a central module of the INNOSEC model which has (interactive) relationships between all the other modules of the model. The main purpose of this module is to take immature ideas from the ideation module to refine and evaluate them, and design them so that they can be efficiently and effectively implemented in the following module.

This module has three elements (Figure 5) to support the strategic decision-making to turn ideas into solutions: Evaluation and selection, Concept development, and Experimentation.

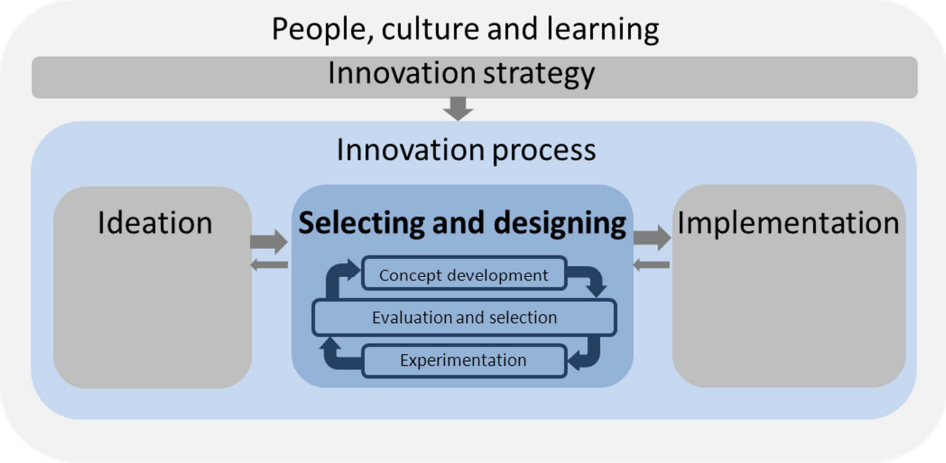

Figure 5: Elements of Selecting & Designing module (*source: Deliverable 4.3*)

Module: Implementation

Implementation is the final stage of the innovation process. The goal of this stage is to implement new technology into existing security service, or to develop and implement new security services into organisational processes.

It has four elements (Figure 6): development project guideline; Technology adoption; Service development; and New service operationalization. The first element promotes the use of project management to develop the implementation process. Project management processes have been found useful in helping to manage and control development and change and is highly recommended to provide structure and guide innovation management in a systematic way. However, project management may not be suitable for all organisations; while highly recommended, it is crucial that organisations choose a process that is suitable for them. The second element is for cases where existing external technology will be adopted into existing service of security with only minor changes in the process, organisation or the actual service. The last two elements are for innovation work that targets completely new service of security or work where major changes will be done for the process, organisation or the actual service of security. There may be iterative interaction between the Implementation module and the Selecting and Designing module in some work of innovation.

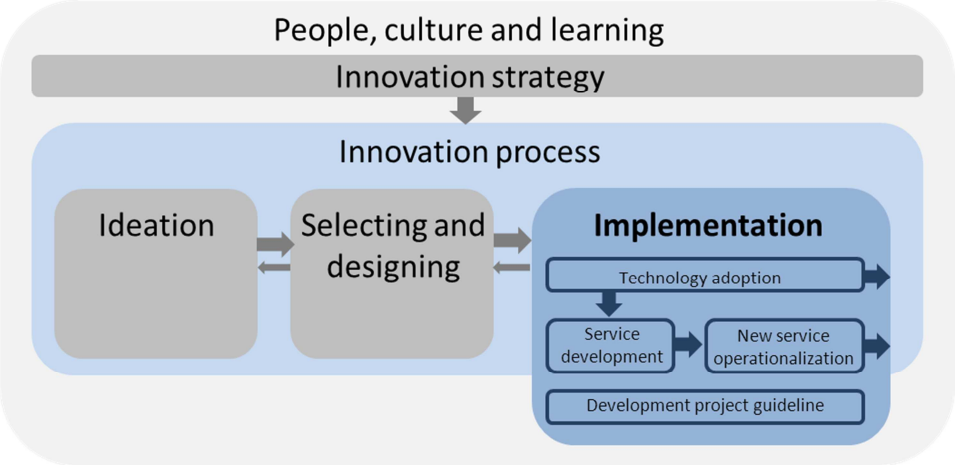

Figure 6: Elements of Implementation module (*source: Deliverable 4.3*)

Module: People, culture and learning

The purpose of this module is to explain why innovation belongs to everybody, what kind of leadership and management is needed, how to develop culture of continuous innovation, and how to support organisational learning. The module has five elements (Figure 7) to consider: Employees and innovation tasks; Leadership and management; Culture of continuous innovation; Learning; and Change management. It considers how to shape the culture of the organisation to be more innovation-oriented overall but also cuts across all the other modules.

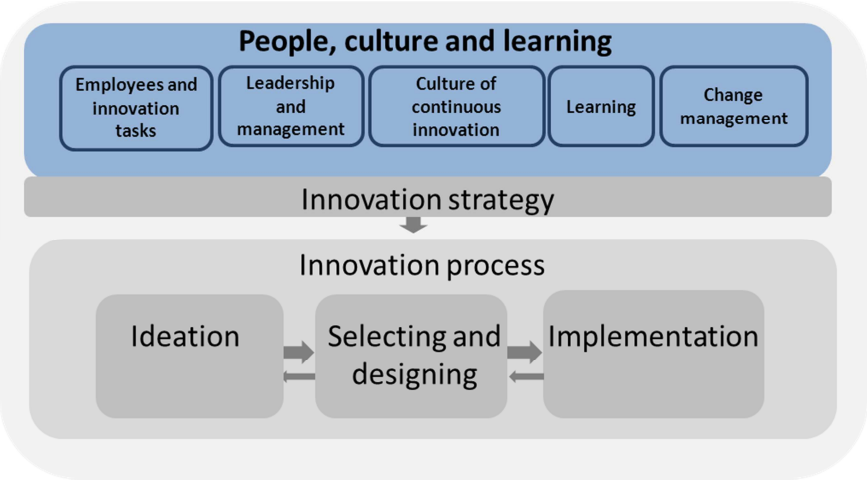

Figure 7: Elements of Implementation module (*source: Deliverable 4.3*)

INNOSEC implementation roadmap

An important result in the project was the variation among Security Organisations and their specificities were compared to the standard commercial organisations for which innovation models have previously been developed. This insight led to the construction of a **typology for Security Organisations**, which was tested at a user-oriented conference and modified based on these findings. The SO typology can be derived from the following characteristics with their states:

Characteristic 1: Degree of procedural freedom of Security Organisation

This characteristic describes whether or not SO's are at liberty to choose the procedures they follow in their activities.

1. Complete/Dominant external restrictions (e.g., aviation security, nuclear industry)
2. Partial external restrictions (e.g., policing, department store, emergency medicine)
3. Almost complete freedom

Characteristic 2: Security focus of organisation at large

This characteristic surfaces the fact that security activities vary in importance for the organisation. Of course some organisations are totally dedicated to security, and among those that are not, the strategic importance of security may vary a lot.

1. Security specific (police, security company)
2. Security vital (airport, nuclear power plant, coast guard)
3. Security peripheral (department store)

Characteristic 3: Customer vs. industrial security focus of Security Organisation

This characteristic relates to whether the SO has to deal with the public or not

1. The Security Organisation operates in an environment with large numbers of customers or other representatives of the public present
2. The Security Organisation operates in an environment with normally only dedicated personnel present

Characteristic 4: Rate of change in technological and threat environment for Security Organisation

This characteristic describes whether the SO operates in a stable or fast-changing environment.

1. Disruptive changes prevalent
2. Continuous and fast changes
3. Mainly stable but with significant areas changing fast
4. Stable environment

Characteristic 5: Business focus of organisation at large

This characteristic illustrates whether the SO is set in a profit-oriented context or not.

1. For-profit (security company, department store, nuclear power plant)
2. Non-for-profit (police)

Characteristic 6: Size of Security Organisation

The size of the SO is obviously of importance for its innovative ambitions.

1. Security budget < 0.3 M€
2. Security budget 0.3- 3 M€
3. Security budget 3-30 M€
4. Security budget > 30 M€

Characteristic 7: Organisational diversity of Security Organisation

Diversity vs. uniformity of staff regarding education and position has importance for innovation processes.

1. Diverse operational staff
2. Uniform operational staff

The Implementation Roadmap consists of the three tiers: why?, what?, and how?

The why? tier is about purpose. What good should an Innovation Model (IM) bring to an organisation? Should it, e.g., assure competitiveness in the market place, help the SO keep ahead of a dynamic threat, help convince regulators or customers accept novel security solutions? And of course combinations of these and other purposes are possible.

The what? tier, viz. what parts of the IM to deploy; it is closely related to why?. For example, in order to keep ahead of a dynamic threat, foresight activities could be a good idea.

How?, finally, is what instruments to deploy to establish or upgrade an IM practice as indicated at the what? tier.

For guidance at all three tiers an SO typology was developed. It is – of course – not our idea that a cell in the typology should totally determine what INNOSEC model implementation to choose. But at why? tier the typology is intended to highlight important differences in purpose between SO's, which should be expected to strongly influence the what? tier.

The insights on specificities and variations led to the realisation that successful implementation of the Innovation Model required further detail. Therefore its five modules and 18 elements were broken down to 36 Innovation Practices, with the number of Practices per element ranging from one to five. Also, for each Innovation Practice three capability levels above rudimentary were carved out based on the typology to enable Security Organisation to assess their present status and tailor the Innovation Model to their needs.

Finally a continuous implementation process was developed. Also this is a development during the work process, going from a perspective of implementation of the Innovation Model as a one-shot process to one where the Capability needs assessment tool based on the Innovation Practices is used to monitor and regularly evaluate and reassess the need for innovation capabilities.

The implementation process for the INNOSEC Model is described by the following steps. As indicated in Figure 8 the steps are cyclical, such that Monitoring and evaluation on, e.g., a yearly basis leads to reassessing the module selection. It is of course possible to iterate between steps. This means that different time horizons for implementation activities are considered in a unified process.

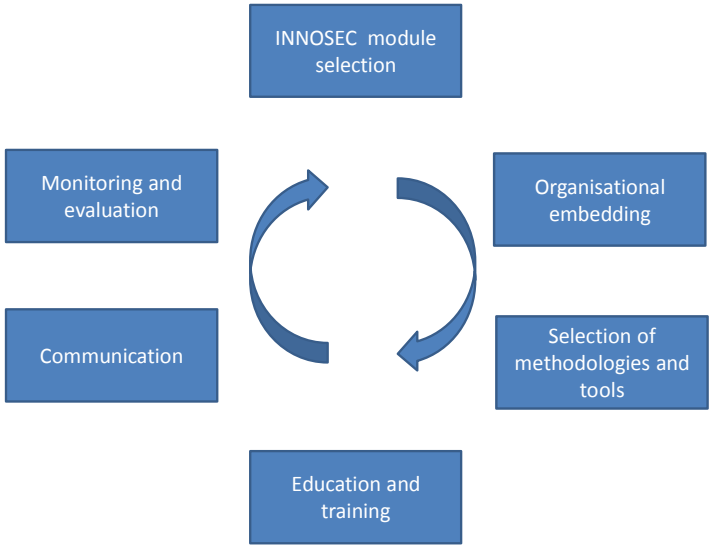

Figure 8: The INNOSEC implementation process (*source: Deliverable 5.2*)

Innosec module selection

This step along with Monitoring and evaluation represent the why? and what? levels, with the other steps building up how?. It is often appropriate to iterate between module selection and the how? steps before making the decision on selection.

Organizational embedding

The next step in the cyclic implementation process is the organizational embedding of the selected modules. It should be clear who is responsible for the implementation of a specific module and though what lines of communications the interaction between the separate modules will take place. It is of crucial importance that the innovation modules are formally embedded in the organization so innovation processes are managed.

Selection of methodologies and tools

Next step is the selection of the methodologies and tools that the organization will use in the selected modules. There are many innovation management methodologies and tools. The INNOSEC Model gives valuable guidelines on possible methodologies and tools, but in the selection the specific needs and, very important, the organizational culture plays an important role.

An important decision that also should be made in this phase is whether the organization will use a specific methodology or tool by itself, or if it will hire an external consultant for specific innovation management methodologies.

The selection of the methodologies and tooling is the responsibility of the manager that is responsible for each specific module. In this decision process they should coordinate with other innovation managers and with top management so that the selected methodologies reflect the organizations innovation strategy and innovation culture.

Education and training

Especially for methodologies that are executed internally, so without the use of external consultants, the organizations need skilled people to use these methodologies and tools. For this, methodology- and tool-specific educations are required. These trainings may be required for few specific persons, but it is also possible that for the implementation of a specific widely used tool, a generic training is required for a broader audience.

Communication

Innovation and innovative ideas can pop up throughout the organization. It is therefore crucial that innovation strategy, procedures, responsibilities, lines of communications and methodologies and tools are communicated not only to managers but to everyone in the organization. It is the responsibility of top management that a communication plan for innovation is written and executed.

Monitoring and Evaluation

The INNOSEC Innovation Model is not a static model. The performance of the innovation processes, methodologies and tools that are used should be monitored and evaluated on a regular basis. The INNOSEC Capability needs assessment tool can be used for this. This process may lead to the selection of new INNOSEC modules or to the improvement or alteration of methodologies and tools that are used.

INNOSEC web-based tool

The INNOSEC project delivered a working web-based support prototype that facilitates security organisations to gain an understanding of the INNOSEC model, its modules and some guidance for implementing it. By using the web-tool, R&D managers or any business area's manager will be able to learn about the implementation of the INNOSEC model (or individual modules) following a phased approach. More specifically, the web-tool aims to:

1) help security organisations to find a solid justification regarding the necessity of an innovation management model;

2) obtain a precise evaluation of the maturity level of the organisation with regards to innovation management practices that the INNOSEC modules address and subsequently, to make decisions about potential implementation;

3) define an implementation roadmap for the modules that have been chosen to be implemented in the organisation.

Once the registration has been successfully carried out, a welcome page appears "Welcome to INNOSEC (INNOvation Management Models for SECurity Organizations)" showing three sections (Figure 9) which provides the user valuable material:

- HANDBOOK (to understand the model), the INNOSEC model is provided in a pdf format
- ACCESS TRAINING MATERIAL, to access training material
- WEBTOOL, to start learning about the model and its modules for managing innovation

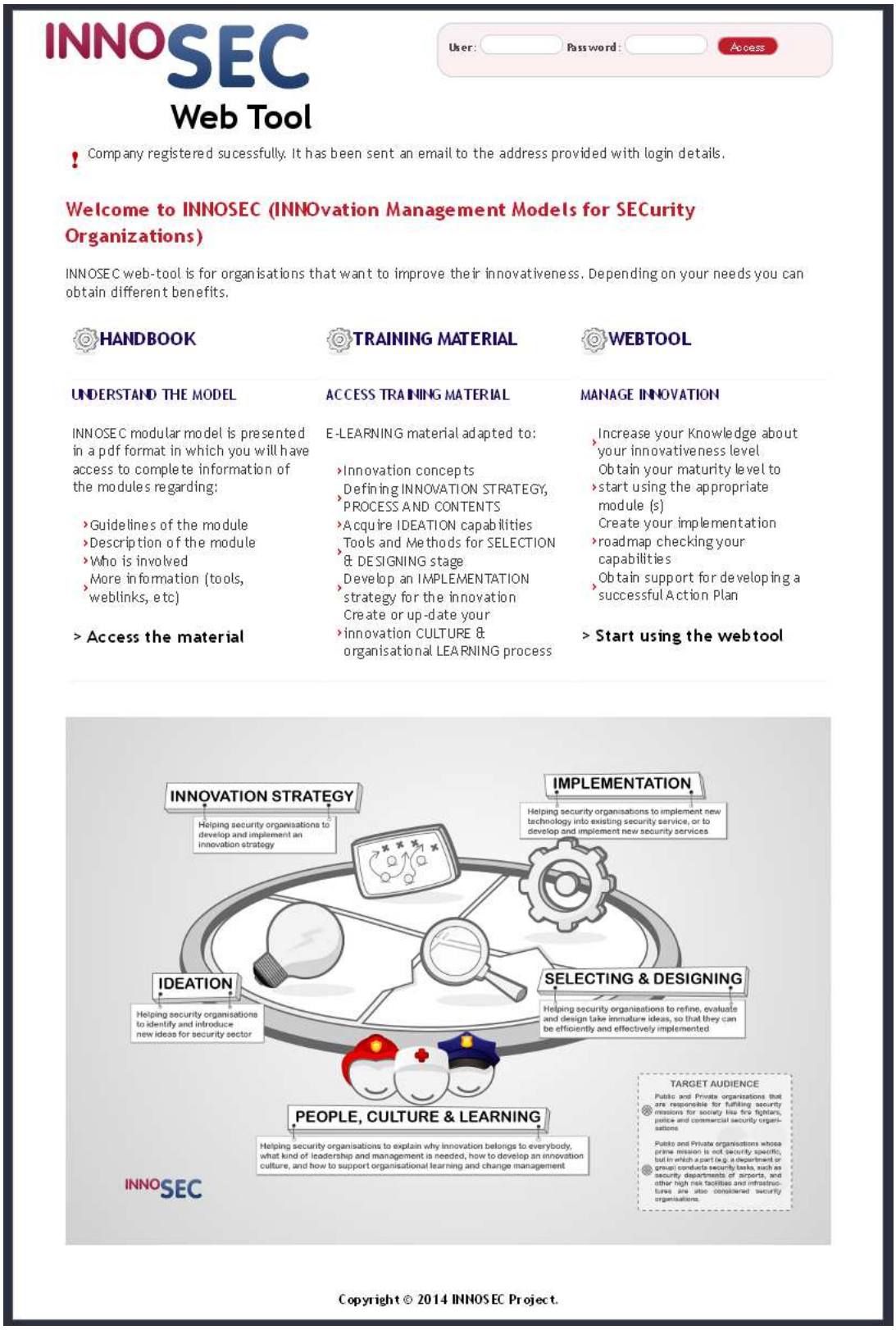

Figure 9: INNOSEC Web-tool welcome page (*source: Deliverable 6.9*)

The tool is user-centred which means that it is conceived with the objective of providing relevant information for decision making, through user-friendly interfaces. The functionalities of the web-tool have been structured following the PDCA approach. In the following figure (Figure 10) the proposed steps to be followed by the user are graphically drawn:

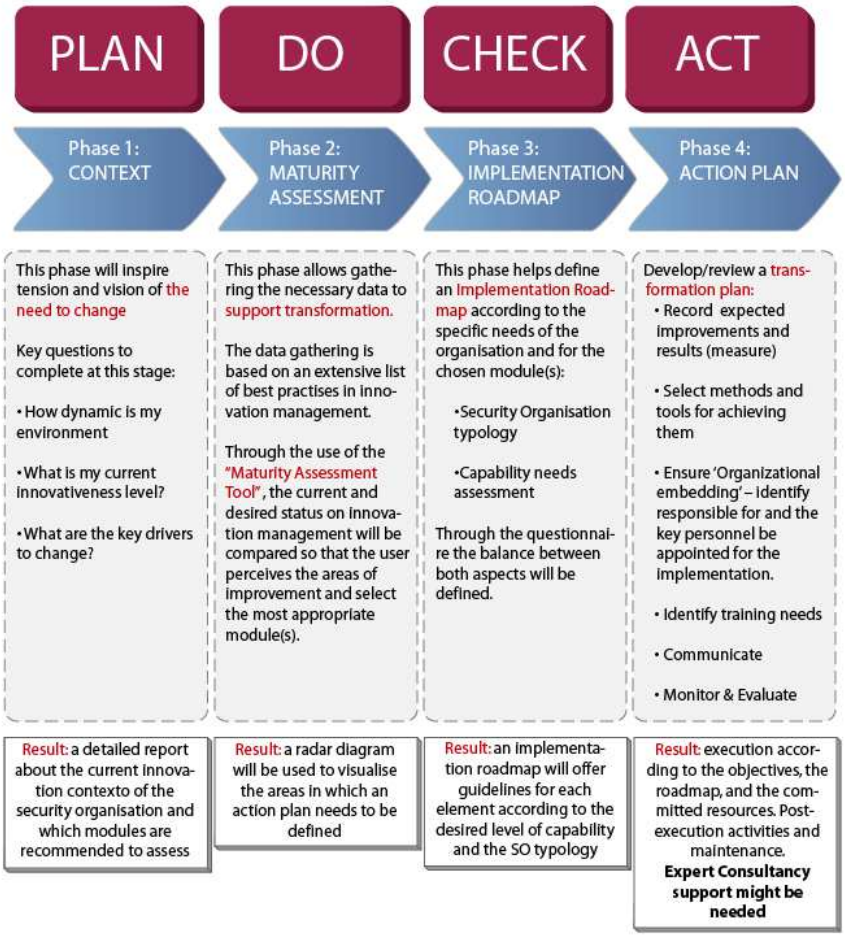

Figure 10: Overview of INNOSEC web-tool functionalities (*source: Deliverable 6.9*)

CONTEXT

The first phase (PLAN) addresses the necessity of the organisation regarding innovation management. In four steps, the security organisation will be able to obtain a detailed report which determines the organisation's ability to deal with changes in environment and the actions needed to optimize its level of innovativeness.

In this first phase of the process, it is aimed to provide a well-founded justification for implementing an innovation management model, that is, why should the security organisation implement INNOSEC model?

This phase will inspire tension and vision on the need to change. The context's evaluation is questionnaire-based and covers the following dimensions of innovation management:

- Manager's perception about the dynamism and complexity of the environment of the security sector in which the organisation operates
- The level of innovativeness of the organisation from the innovation process perspective as well as from the adaptive capacity of the security organisation
- The R&D strategy of the organisation.

The web-based tool offers, at the end of this first phase, the possibility to graphically visualize the results generated and the possibility to obtain a report in a pdf. format which delineates the appropriateness and necessity for an Innovation Model and provides recommendations about which module(s) the organisation may focus their efforts, if further implemented. The overall vision of the results in this report will lead the respondent towards the next phase: THE MATURITY ASSESSMENT.

MATURITY ASSESSMENT

Once the innovation management context has been evaluated, the Maturity Assessment tool is provided in the second phase (DO) to measure a security organisation's innovation management maturity level in the selected module(s). The Maturity Assessment offers to security organisations:

- a diagnosis of the current (AS-IS) and expected (TO-BE) status of the security organisation with regards to best practices in innovation management in the selected module(s) and,
- prioritize the obtained gaps by the relevance score provided by the respondent, that is, each innovation practise may be scored according to how important it is for the security organisation at the moment of doing the assessment.

For the development of the questionnaire that supports the assessment 36 Innovation Practices have been identified and grouped by the elements of the five modules of the INNOSEC model: Innovation Strategy (3 elements), Ideation (3), Selection (3), Implementation (4) and People, Culture and Learning (5).

After exercising the maturity assessment, a diagram allows the respondent to visualise the critical areas in which the manager(s) need to focus their attention for further improvement. The web-based tool offers, at the end of this second phase, the possibility to obtain a report in a pdf. format which delineates the main gaps in innovation management to be covered. The web-based tool will lead the respondent towards the next phase: THE IMPLEMENTATION ROADMAP.

IMPLEMENTATION ROADMAP

In the previous phase, a prioritisation of relevant maturity gaps has been possible, selecting the most relevant modules to be implemented in the security organisation. This phase (CHECK) helps security organisation to define an Implementation Roadmap according to its specific needs and addressing the chosen module(s).

The Implementation Roadmap consists of the three tiers:

- The 'why?' tier is about purpose. What good will the INNOSEC innovation model bring to an organisation?

Will it, e.g., assure competitiveness in the market place, help the SO stay ahead of a dynamic threat, help convince regulators or customers to accept novel security solutions? Combinations of these and other purposes are also possible.

- The 'what?' tier, viz. What parts of the INNOSEC innovation model should be deployed?

For example, in order to keep ahead of a dynamic threat, foresight activities could be a good idea.

- The 'How?' tier identifies what instruments to deploy to establish or upgrade an innovation practice as indicated at the 'what?' tier.

Within this phase and for guidance at all three tiers the SO typology is defined firstly. Secondly, a capability assessment is presented (which is questionnaire-based). Four levels of capability have been defined per each of the elements of the INNOSEC innovation model:

1. Rudimentary
2. Can be achieved ad hoc with considerable risks for quality deficit, time delay and cost overrun problems
3. Can be achieved according to a good practice approach with limited risks for quality deficit, time delay and cost overrun problems
4. Can be achieved according to a best practice approach with low and predictable risks for quality deficit, time delay and cost overrun problems.

A Capability Needs Assessment tailored for SOs specifically is provided and its aim is to help the users in the selection of proper implementation instrument that the INNOSEC Model provides.

The web-based tool offers, at the end of this third phase, the possibility to obtain a report in a pdf. format with a detailed implementation roadmap that offers guidelines for each element according to the desired level of capability and the SO typology. The overall vision of the results in this report will lead the respondent towards the next phase: THE ACTION PLAN.

ACTION PLAN

At this stage (ACT), the improvement process is finally put into action. In order to achieve the habits and behaviour to change, there has to be a high level of understanding, organisation and communication beforehand.

Assuming that the previous phases have been performed effectively, this phase aims to develop or review a transformation plan, which includes:

- Record expected improvements and results (measure)
- Select methods and tools for achieving them
- Ensure 'Organizational embedding' – identify responsible for and key personnel be appointed for the implementation.
- Identify training needs
- Communicate
- Monitor & Evaluate

At this stage, ensuring that the performance measurements are still relevant and effective is the objective. Consider the behaviours that are changing due to this process and focus on understanding the habits that are forming due to these changes.

The execution plan will be defined according to the objectives, the roadmap, and the committed resources as well as post-execution activities. In this phase, expert consultancy will be needed to provide specific support for change management.

1.4 Potential impact and the main dissemination activities and exploitation of results

The implementation of INNOSEC model expects to have a decisive impact on the innovativeness level of European (public and private) security organisations in several aspects:

- They will be able to **forecast the possibilities of accessing to strategies and to implement innovation management systems** in the security field: The INNOSEC understanding of innovation management, emphasises how organisations monitor technological developments in their external operating environment and how they identify available technological and innovation opportunities, how they select, adopt and adapt such technologies and, finally, how they feedback and interact with providers of innovations within a learning process.
- They will **expand the model throughout the whole value chain**, including SME technology providers and suppliers, to reinforce the cooperation between them. With the INNOSEC model, security organisations can develop networked innovation. Such a networked innovation gives additional external resources for the security organisation to solve present and anticipated challenges in their security environment. Since networked innovation would mean additional challenges for the security operators that they should manage, the modular INNOSEC model offers practical tools for the security organisations to manage the additional challenges related to innovation with external partners.
- They will be able to **balance the need to react to innovation opportunities with the efficiency to develop appropriate solutions** (new technology, new business models) in line with innovation capabilities and responsiveness of the security organisations. This would cause greater efficiency in the organisations and the release of resources for other tasks.

INNOSEC tried to cover a higher portion of European security organisations. Primarily, three security organisations (two public and one private security organisations) actively participated in the development of project's results inside the consortium. Research was orientated to identify, in addition to project partners' requirements, additional insights from 11 security organisations that voluntarily participated. Complementarily, the Advisory Board, represented by six security organisations, contributed to the project results' development providing the consortium with their requirements and vision concerning the different stages of the project, and intermediate and final results. INNOSEC consortium has gathered their feedback and integrated these recommendations in all project outcomes. Besides, the Advisory Board has actively participated in networking activities that were organised for exchange of best practices between the security organisations in Europe. Furthermore, external experts in innovation management and in the security field also attended the networking activities. All in all, they contributed to the emergence of jointly identified needs and similar procedures based on a common ground, while respecting cultural and organisational diversity.

Posterior wide scale application of the new model would allow a considerable leap forward to the European security sector in terms the creation of an integrated security innovation system in Europe. Subtopics like system governance, system relationships with existing nodes and entities, the representativeness of the components, especially the ones corresponding to the society itself would have also paramount importance. Obviously, the complexity of the approach and the big impact of expected

results make impossible to approach the project on a local or national basis but on the contrary it has to be developed under a transnational pattern.

As far as dissemination activities are concerned, since the beginning the project, many dissemination activities have been performed by the project partners, under the coordination of the WP6 leader:

- Three papers presented in International Conferences:
  - Future Security 2012 (7th Security Research conference in Bonn, Germany, September 2012) and Future Security 2013 (8th Future Security Conference 2013, Berlin, Germany, September 2013). The Future Security Conference is organized by the Fraunhofer Group for Defence and Security and takes a holistic view on security. It provides insight into technological breakthrough as well as societal aspects of security. The participants of the conference were decision makers and public authorities (e.g. Federal Ministry of Defence, Federal Ministry of Education and Research, Federal Criminal Police Office) as well as industry and scientists.
  - 'R&D management conference' - presentation of publication on "Capacity building and competencies for innovation management in security organisations" June, 2013, Manchester. Type of audience: R&D experts, innovation experts.
- INNOSEC project has been shown in six dissemination events (special sessions, workshops, seminars) some of them organised by project consortium.
  - INSEC project Workshop during **Sectech 2013**, Oslo. Audience: Police forces, security experts, technology and consultancy providers (European level)
  - **National Congress of Emergencies Organizations** (Spanish), May 2013, San Sebastian, Spain. Audience: Emergency services, first-responders, fire fighters.
  - Workshop organized by INSEC during the **MILIPOL**, November 2013, Paris, France. Audience: Security organizations, technology providers, consultancy in Security (European level). Participation at MILIPOL Conference in the **Talk-Show "Innovation in Security Organization"**, November 2013, Paris, France. Audience: Scientific community, Industry, policy makers (European level) http://www.archimedes-eu.eu/videos/video.php?&video=milipol_innovation_management .
  - **Final Conference "The INNOSEC project- results and experience of partner security organisations",** January 2014, San Sebastian, Spain. Audience: Security organisations (local and national Spanish companies)
  - **Workshop at Interpol organized by INSEC project**, February 2014. Audience: Lyon, France, Police forces (European level).
  - **Roundtable organized by ARCHIMEDES project**, February 2014, Aix-en-Provence, France. Security organizations, experts in innovation management (European level)
- One International Publication, Chapter "Innovation management in security organisations" in **"Research highlights in safety and security", VTT Research highlights 10, Espoo, 2013**. Audience; multiple choices in the fields of safety and security
- The INNOSEC project has been published in some press releases of the project partners' organisations.

1.5 INNOSEC details: contact details and address of the project website

	INNOSEC
Title	INNOvation Management Models for SECurity Organizations
Research area	SEC-2011.7.5-1: Innovation and research within security organisations
Call ID	FP7- SEC-2011- Collaborative Project
Project ID	285663
Duration	24 months (01/02/2012 - 31/01/2014)
Project Coordinator:	Amaia Sopelana Fundación Tecnalia Research & Innovation Parque Tecnológico de Bizkaia, calle Geldo, Edificio 700 E-48160, Derio, Spain- www.tecnalia.com Tel: +34 946 400 450 amaia.sopelana@tecnalia-com
Project website:	www.innosec-project.eu
Project partners:	

Beneficiary name		Country
FUNDACION TECNALIA RESEARCH & INNOVATION	**TECNALIA**	Spain
FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V	**FRAUNHOFER**	Germany
TEKNOLOGIAN TUTKIMUSKESKUS VTT	**VTT**	Finland
TOTALFORSVARETS FORSKNINGSINSTITUT	**FOI**	Sweden
AIT Austrian Institute of Technology GmbH	**AIT**	Austria
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK	**TNO**	Netherlands
THE UNIVERSITY OF MANCHESTER	**UNIMAN**	United Kingdom
OSTERREICHISCHES ROTES KREUZ ORK	**ARC**	Austria
PROSEGUR COMPANIA DE SEGURIDAD SA	**PROSEGUR**	Spain
Politieregio Zaanstreek-Waterland	**POLITIEREGIO**	Netherlands

2. Use and dissemination of foreground

2.1 Section A (public)

The dissemination of the INNOSEC project's concepts includes papers on scientific conferences, public presentations of the results and the creation and management of a web site and the respective forum (wiki). The web site is used to give prompt visibility to the project development and results. There is also a forum used for discussions. The dissemination activities have mainly taken place from the beginning of second year of the project, once tangible results could be disseminated and those activities have intensified as the final stage of the project has been getting closer.

The activities devoted to raising public participation and awareness, as well as to the activities related to the exchange of experiences, have been carried out by the respective national partners, led by dissemination leader, through National and International Conferences worldwide, workshops and other specific focussed events. The project partners have also presented project results on relevant exhibitions where they have participated. The main dissemination activities are:

Web site

A web site started to be available during the first year of the project. It presents, through tailored material, the project and its results. All the public material, such as public deliverables, publications etc. are available through it. It also hosts the access to the web-tool of INNOSEC model that facilitates security organisations, after a formal registration, the access to its main functionalities (context evaluation, maturity assessment, training material, etc.). A forum, called the INNOSEC Collaboration Network, has been created. The final aim of this work is to create a self-sustained community around the innovation management concepts in security that will use, spread and further develop the INNOSEC concepts.

Conference publications, Workshops and Special Sessions

The technical and scientific dissemination of the project was addressed through several papers dedicated to the results of this project, which have been presented at international conferences (such as Future Security Conference). In addition to scientific and technical dissemination, the project mainly intended to target the security organisations who can be interested in the INNOSEC model and modules. For this reason, the attendance of project partners to various workshops and roundtables has been of paramount importance. With these activities partners have shared with potential customers the status of the INNOSEC results and have obtained their feedback in order to improve them. A big effort has been made by different partners and workshops have had great success. Other general dissemination has been obtained through flyers and brochures distributed in selected events.

The following tables compiled the dissemination activities along the project lifecycle (two years).

TEMPLATE A2: LIST OF DISSEMINATION ACTIVITIES								
NO.	**Type of activities[3]**	**Main leader**	**Title**	**Date/Period**	**Place**	**Type of audience[4]**	**Size of audience**	**Countries addressed**
	Poster presentation	FRAUNHOFER	"Innovation in Security Organisations- Introducing the INNOSEC Project" in Future Security conference	September 2012	Bonn	Technology providers, system integrators, security organizations	>200	International
	Presentation and Workshop	TECNALIA, VTT, FRAUNHOFER	INSEC Workshop during Sectech 2013	March 2013	Oslo	Police forces, security experts, technology and consultancy providers	15	International
	Presentation and Workshop	ARC		January, March 2013	Vienna	Head and researcher of innovation department, ARC headquarters	5	National
	Presentation	TECNALIA	National Congress of Emergencies Organizations	May 2013	San Sebastian,	Emergency services, first-responders, fire fighters	50	National

[3] A drop down list allows choosing the dissemination activity: publications, conferences, workshops, web, press releases, flyers, articles published in the popular press, videos, media briefings, presentations, exhibitions, thesis, interviews, films, TV clips, posters, Other.

[4] A drop down list allows choosing the type of public: Scientific Community (higher education, Research), Industry, Civil Society, Policy makers, Medias, Other ('multiple choices' is possible).

					Spain			
	Publication	Fraunhofer	Overview of INNOSEC in Fraunhofer Annuary 2012	May 2013	Munich	Technology providers, SO	>100	National
	Presentation and Interviews	ARC		May, August 2013	Vienna	QM Manager and staff of blood donation centre	4	National
	Presentation at Conference	UNIMAN	R&D management conference- presentation of publication on "Capacity building and competencies for innovation management in security organisations"	June, 2013	Manchester	R&D experts, innovation experts	>100	International
	Presentation and Workshop, Interview	ARC		June, July 2013	Baden	CEO and Head of departments, local branch of ARC	5	National
	Press Release	ProSegur	Dissemination in web and social networks	August, 2013	Madrid	SO	>100	National
	Future Security Conference 2013	FRAUNHOFER	The INNOSEC Project	September 2013	Berlin, Germany	Technology providers, system integrators, security organizations	>200	International
	Presentation, Flyers	ARC		October, December 2013	Sierning	Heads Emergency medical services, regional branches	12	National

	Workshop	TECNALIA	Organized by INSEC during the MILIPOL	November 2013	Paris, France	Security organizations, technology providers, consultancy in Security	20	International
	MILIPOL Conference	AIT	Talk-Show “innovation in security organization”	November 2013	Paris, France	Scientific community; Industry; policy makers		International
	Publication	VTT	Chapter “Innovation management in security organisations” in “Research highlights in safety and security”, VTT Research highlights 10, Espoo, 2013	November 2013	Finland	Multiple choices in the fields of safety and security		International
	Workshop	ARC		January 2014	Vienna	ARC Headquarters heads of departments	8	National
	Final Conference	TECNALIA	The INNOSEC project- results and experience of partner security organisations	January 2014	San Sebastian, Spain	Security organisations		Spain
	Workshop	TECNALIA	Workshop at Interpol organized by INSEC	February 2014	Lyon, France	Police forces	15	International
	Workshop	TECNALIA	Roundtable organized by ARCHIMEDES	February 2014	Aix-en-Provence,	Security organizations, experts in innovation	12	International

					France	management		