SUPPORTED UNDER:
SEVENTH FRAMEWORK PROGRAMME

PROJECT FULL TITLE: **F**acilitate **I**ndustry and **R**esearch in **E**urope
GRANT AGREEMENT N. 318762

DELIVERABLE D2.1

DELIVERABLE D2.1-FIRE RESEARCH AND INNOVATION ANALYSIS METHODOLOGY

Due Date: 30 11 2012
Main Author: Neil Adams, Richard Chisnall, Chris Pickering, Brian Whicher
Contributors: All partners
Dissemination: Public

Document Control Sheet

Project Number	318762	
Project Acronym	FIRE	
Work-package:	WP2-Develop Pan EU ICT Security Cluster Research Network and Strategy	
Version 1	27/10/2012	*First draft*
Version 2	28/11/2012	*Final version*

Classification

This report is:

Draft	
Final	x
Confidential	
Restricted	
Public	

Partners Owning	ADS
Main Editor	ADS
Partners Contributed	All

Table of contents

1 EXECUTIVE SUMMARY

This paper presents a structured framework for collecting and analysing Trustworthy ICT research and innovation (R&I) capabilities and activities in the regions represented by the partners in the Facilitate Industry and Research in Europe (FIRE) project. This is Deliverable D2.1 from Task 2.2 of the FIRE project. A methodology has been developed that combines key individual organisation data and builds on that with regional-level information to provide qualitative and quantitative data that can be analysed to produce an IT security research agenda for each of the regions, and then a joint pan-Cluster research agenda across the regions. The output of this task will be used in Task 2.3 where the cluster information will be collected and analysed using a common structure, which in turn will be used in Task 4.3 by the consortium to identify areas for pan-cluster cooperation and programmes and develop the pan-cluster research agenda.

2 INTRODUCTION

The aim of this paper is to produce a structured framework for collecting and analysing Trustworthy ICT research and innovation (R&I) capabilities and activities in the regions represented by the partners in the Facilitate Industry and Research in Europe (FIRE) project. This is Deliverable D2.1 from Task 2.2 of the FIRE project. The output of this task will be used in Task 2.3 where the cluster information will be collected and analysed, which in turn will be used in Task 4.3 by the consortium to identify areas for pan-cluster cooperation and programmes and develop the pan-cluster research agenda.

3 CONTEXT

In the ICT context, trustworthiness as defined by the EC refers to ICT "that is secure, reliable and resilient to attacks and operational failures; guarantees quality of service; protects user data; ensures privacy and provides usable and trusted tools to support the user in his security management"[1].

The problems that the FIRE project is trying to solve are listed below:

- The EU has world-leading research in Trustworthy ICT but this does not translate into economic competitiveness and world-leading companies.
- Policy makers at EC, national and regional level want companies to grow and are looking for ways they can help in policy and programme terms.
- Organisations, particularly Industry, may be very sensitive about sharing information, especially information on security activities: the fact that a company is even working on an idea can be something they do not wish to share.
- Industry can find it difficult to know who in academia to go to with their problems – where are the experts and what do they do?
- Academia can find it difficult to link to companies to exploit their research
- Both Industry and Academia sometimes struggle to find collaborators for technology development
- Since there is no overview of EU-wide R&D capabilities there is a suspicion that there is duplication but there are also gaps in EU capability that are not being addressed.

4 AIM

To develop a joint strategy and research agenda, a common framework is needed for collecting and analysing data and information (both quantitative and qualitative) on Trustworthy ICT capabilities and activities across the regions. The regions here are defined as the country of the partner together with their wider areas of responsibility, as agreed in the DoW. The framework must support the following goals:

1. Data and information collected for the regions by the partners must capture the key R&D and commercial IT security organisations in their regions, and analyse their collective strengths, weaknesses, opportunities, and threats.
2. Data and information collected for the regions by the partners must be structured in such a way that it allows synergies and gaps between capabilities and activities across the regions to be identified. Common standards for assessing the relative strengths of organisations (and regions) must be agreed and used to allow objective comparison of capabilities and activities between regions and across organisations, and ensure that results can be readily compared.

[1] EC Workshop on measurability of trustworthiness, Brussels 03/09.

3. It is necessary to understand who the main IT Security customers (users) are and what they need from IT security research and IT security solutions.
4. Data and information collected for the regions by the partners must provide suitable information to allow a pan-Cluster Trustworthy ICT research agenda to be produced.
5. The Pan-Cluster Research Agenda should support policy makers (e.g. UK – Home Office, Dept of Business, Innovation & Skills, Technology Strategy Board, Engineering and Physical Sciences Research Council), enabling them to (i) understand capabilities in Academia and Industry to baseline the capabilities, (ii) support policy, programme and investment decisions, and (iii) to understand the geographic location and strength of capabilities to support national policy development.

5 APPROACH

The information required from each region (as defined above) consists of three elements:

1. Information on key organisations undertaking R&D, both research institutes and industry, including their focus areas, capabilities and strengths.
2. Information on key industry players and industrial capacity, together with industry needs.
3. Top-level regional information, e.g. an overview of regional R&D intensity, major capabilities, activities and initiatives.

Items 1 and 2 will only pick out key organisations, but this information, when combined with the regional information in Item 3, will give the right level of information to identify trans-cluster synergies and gaps.

Each cluster will collect data on its own country and neighbouring markets, as follows:

- AMETIC: Spain, Italy, Portugal
- LSEC: Belgium, Luxemburg, Netherlands, France
- ADS: UK, Ireland
- IFIS: Germany, Austria, Switzerland
- NSMC: Czech Republic, Slovak Republic, Slovenia, Poland
- CYBER: Estonia, Baltic States, Scandinavia (including Denmark)

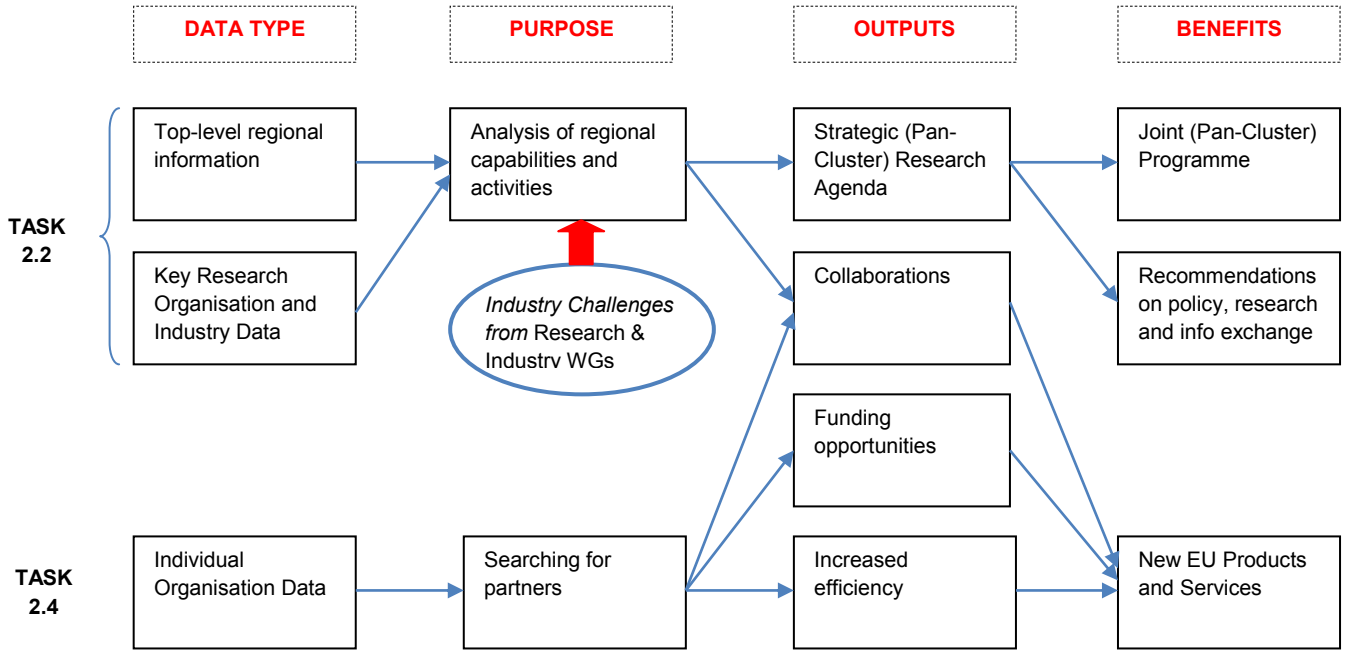
It is recommended that the partners begin the information collection process in their own local region/country, before extending to the wider designated regions, as there are significant differences in some regions, e.g. Spain as the partner region has many differences to Portugal and Italy.

It is proposed that in Year 1 (for the work leading to a draft joint research agenda in Month 12) the partners focus on collecting data for their countries, and that in Year 2 that the partners then consider activities in neighbouring countries when updating their view on regional priorities to support the final joint research agenda in Month 24.

The database being developed in Task 2.4 has a different objective to that being developed here, viz. to enable users and researchers to search for partners. Hence the database is being structured in such a way that users can ask questions that identify research organisations relevant to their business needs. However, the data collection process for key individual organisations (item 1 above) could use the database to collect some of the information. More details of the data required for the analysis are given below.

A flowchart to clarify how the data will be used is shown in Figure 1, showing the purpose, outputs and resulting benefits. This report focuses on Task 2.2 while details of the database (task 2.4) will be dealt with elsewhere.

Figure 1 – Data Purpose, Outputs and Benefits



6 FRAMEWORK FOR COLLECTING DATA ON KEY INDIVIDUAL ORGANISATIONS

A significance test will need to be applied to identify key organisations when collecting data on individual organisations and their activities, to ensure that the data is useful for the regional and pan-cluster analysis. Data should be collected on 'significant' organisations working in the field, carrying out 'significant' research or delivering 'significant' projects and services. For example, for the UK and Ireland, data on all companies including individual sole-traders and research institutions where there is just one researcher working in the field, would not be useful. The partners will need to define and agree the significance level for data collection on individual organisations, and then aim to ensure a high data collection rate for those organisations. For companies this threshold might be in terms of turnover, their position in the market, or their level of R&D, and for research organisations it might be in terms of the number of current research projects, the number of researchers or their national or international ranking.

In the UK the Engineering and Physical Sciences Research Council (EPSRC), that funds most academic research in Trustworthy ICT, and the Government Communications Headquarters (GCHQ), have jointly set up a Scheme to recognise UK Academic Centres of Excellence in Cyber Security

Research (ACEs-CSR)[2]. The research areas that are within scope for these centres are classified as below (with sub-topics not given here):

i. Cryptography, key management and related protocols
ii. Information risk management
iii. Systems engineering and security analysis
iv. Information assurance methodologies
v. Operational assurance techniques
vi. Research into security of strategic technologies and products
vii. Science of cyber security and human factors
viii. Building trusted and trustworthy systems.

The Scheme describes detailed criteria that will be applied for research organisations to achieve accreditation as an ACE-CSR. These are listed below as an example, and more details are available[2].

1. 'Description of the Applicant', including details of the research environment and strategy and vision. To ensure critical mass, there should be a minimum of 5 permanent members of staff who demonstrate a track record of, and potential for future, working together in the areas of the proposed ACE-CSR. There should be a well-funded research environment that is well equipped and supported by the Institution.

2. Track Record and Esteem Indicators of Members of Staff.

3. Peer-Reviewed Publications.

4. Doctoral Level Students Programme. During the last 5 years, at least 10 successful doctoral theses should have been produced and at least ten doctoral students should have started.

5. External Research Funding and Impact of Projects.

This approach will be developed and agreed with the partners to identify 'significant' research organisations in cyber security. This will need to include their national/ international ranking. Ideas for defining the significance threshold for IT security companies are also under development.

For key individual organisations it is suggested that the following types of information will be required, as detailed in Appendix A for IT security research organisations (public and private sector) and Appendix B for IT Security companies developing products and services:

1. Organisation level data (e.g. name, contact details, location)
2. Activity level data (specifically descriptions of current research expertise or research interests, and business activities)

7 FRAMEWORK FOR COLLECTION AND ANALYSIS OF REGIONAL CAPABILITIES AND ACTIVITIES

The information to be collected at regional level must enable trans-cluster synergies and gaps to be identified and allow a joint pan-cluster research agenda to be produced (Tasks 2.5 and 4.3). ENISA has produced a useful starting point that describes what national cyber security strategies should

[2] EPSRC Scheme to recognise Academic Centres of Excellence in Cyber Security Research - Invitation for proposals dated 14 August 2012

consider[3], and a useful example has been published presenting the national cyber security research agenda for the Netherlands[4]. These documents identify key factors that must be considered in the joint research agenda.

A research agenda will be produced for each region by the partners, covering the following elements. Suggested questions to capture the required information are listed below: it will not be possible to answer all in detail, but the regional outputs should be sufficient to support cross-Cluster strategy development.

It is proposed that in Year 1 (for the work leading to a draft joint research agenda in Month 12) the partners focus on collecting data for their countries, and that in Year 2 that the partners then consider activities in neighbouring countries when updating their view on regional priorities to support the final joint research agenda in Month 24.

A) VISION FOR THE FUTURE

What are the region's aspirations in IT Security (capturing national, regional, public and private stakeholder views), and what part does the FIRE partner aim to play in this?

B) CURRENT SITUATION

1. ENVIRONMENT (CONTEXT)

What are the significant influences/ change factors affecting IT security?

- Political
- Economic
- Socio-cultural
- Technological
- Legislation
- Environmental

2. IT SECURITY CUSTOMERS

Who are the regional IT Security customers and what do they need from IT security research and IT security solutions?

- Energy
- Finance
- Health
- Mobile Communications
- Government

3. IT SECURITY INDUSTRY CAPABILITY

3.1 Which are the significant IT security companies in the region (at least the top 5 to 10 based on turnover, position in the market, and market share), what are their products/ services, and what are their research interests and needs?

[3] ENISA May 2012 – National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace
[4] Herbert Bos, Sandro Etalle, Erik Poll 2012 – National Cyber Security Research Agenda – Trust and Security for our Digital Life

3.2 Describe the markets, trends, relationships and resource issues for the region (in Year 1 partners look at market size etc in their countries, and then in Year 2 additionally consider market size etc in neighbouring countries)

- Markets – Market size, Market growth, Products and Services
- Industry Trends – Competition, New Technology, Entry barriers, Exit barriers
- Relationships – Suppliers, Customers, Distributors
- Resources – Finance, Skills, Capital equipment, Other

3.3 What is the overall level of IT Security R&D expenditure in the business sector?

3.4 What IT Security investment support is provided by the venture capital sector?

4. IT SECURITY RESEARCH CAPABILITY

Identify the significant organisations involved in IT Security research in each region (at least the top 5 to 10 based on national or international ranking, the number of researchers, or the number of research projects) and where they are located, their research strengths, and their research activities with application areas and commercialisation activities.

5. NATIONAL INITIATIVES AND PROGRAMMES

5.1 What are the national programmes/initiatives (R&D, training, education etc) for developing capabilities in IT security and addressing IT security issues, including resilience?

5.2 What are the national critical information infrastructures (CIIs) and what is being done nationally to develop or improve preparedness, response and recovery plans and measures for protecting such CIIs?

5.3 What mechanisms are used to allow public and private stakeholders to discuss and agree on policy, regulatory and other issues such as research and innovation?

5.4 What initiatives are being carried out by security 'clusters' of companies, research organisations and policy makers/ funding agencies to improve cooperation and enhance competitiveness (e.g. ICT Clusters, ICT networks such as the UK Cybersecurity Knowledge Transfer Network), and what examples of best practice are there?

6. POLICY AND REGULATORY ISSUES

6.1 What are the roles and responsibilities and rights of the private and public sector in providing cyber security and trust in ICT, e.g. mandatory reporting of incidents?

6.2 What are the governance and legal frameworks for IT security, including policies and regulatory measures to provide cyber security and trust in ICT e.g. legal framework for fighting cyber-crime?

6.3 What is the national approach to risk management, e.g. trusted information sharing and national registries of risk?

6.4 What International co-operation agreements and activities are in place with EU and non-EU states?

7. STRENGTHS, WEAKNESSES, OPPORTUNITIES AND THREATS IN IT SECURITY

7.1 Strengths and Weaknesses of the Region's IT security capability and competitiveness

7.2 Opportunities and threats from forces, issues, trends and events outside the Region

8. COMPETITION AND COMPETITIVE ADVANTAGE

8.1 Where does the region have competitive advantage in IT security?

8.2 What activities, capabilities and resources give the region competitive advantage in IT security?

C) RESEARCH AGENDA AND ACTION PLAN (TO BE DEVELOPED BY THE PARTNERS FOR THEIR REGIONS)

Analysing the current situation, identify the key issues that the region needs to address to enhance its IT security capability and competitiveness, and identify the IT security research priorities for the region.

- Priorities should be based on addressing threats and weaknesses and exploiting strengths and opportunities.

Develop a future IT security research roadmap for the region.

- Define the desired outcomes (goals) to address the key issues, and the specific measurable results to be achieved to achieve those outcomes (objectives), with timescales.

Identify the actions required to deliver the IT security research roadmap, with timescales.

- This should include policy and programme recommendations for key stakeholders, to enable the roadmap to be implemented.

Draft regional research agendas will be presented at workshops to other partners, end users and other key stakeholders and independent experts, to refine the regional strategies and identify opportunities for cooperation. The results of these workshops will be used to develop the pan-Cluster research agenda.

8 DATA COLLECTION PROCESS

The information required for the analysis will need to be collected by the partners and their associated Regional Cluster Organisations. While they may know some of the key research organisations and major industry players well, others may be known only by reputation. Therefore public sources are likely to be an important source for location of this information.

The process by which the project partners will collect this information, using partner data sources, open sources, external stakeholder data and possibly direct input of data by individual organisations themselves, will need to be tailored to the individual regional circumstances. Suggested external stakeholders that may help with the information provision are shown below, with examples from the UK/Ireland in italics after the type of organisation:

a. Partner Cluster organisation or association: e.g. *ADS affiliated groups SITC (Security Innovation Technology Consortium), CPAG (Cyber Protection and Assurance Group), DIG (Digital Intelligence Group), SEFG (Security Export Focus Group), SRN (Security and Resilience Network)*

- → Future strategy
- → Industry members (especially SMEs) and product areas
- → Industry expenditure and market size
- → Industry challenges and research needs
- → Key members to contact

b. Research funding agencies*: EPSRC (Engineering & Physical Sciences Research Council), TSB (Technology Strategy Board), Science Foundation Ireland*

- → Future strategy
- → Major academic research institutes and projects
- → Key capability areas
- → Major academic-industry collaborative projects and participants

c. Major research institutions: *UK GCHQ-accredited Academic Cyber Security Centres of Excellence, Waterford Institute of Technology, University College Dublin.*

- → Key capability areas
- → Industrial collaborators
- → Major projects

d. Business support networks: *ICT (Cyber Security) Knowledge Transfer Network, UKTI and INTELLECT*

- → Public Sector contacts
- → Major industry players and contacts
- → Industry members (especially SMEs) and product areas
- → Industry expenditure and market size
- → Industry challenges and research needs
- → Key members to contact

e. Member State Government Departments: *BIS (Dept for Business, Innovation and Skills) and GCHQ (Government Communications Headquarters)*

- → Future strategy
- → Public Sector contacts
- → Major industry players and contacts

f. National Contact Points: *UK FP7 ICT and Security NCPs, Irish FP7 ICT and Security NCPs*

→ Major collaborative projects and participants

9 PAN-CLUSTER STRATEGIC RESEARCH AGENDA

Following the production of the regional research agendas above, a collaborative research agenda will be produced jointly by the consortium, containing the following elements:

A) VISION FOR THE FUTURE

What are the aspirations of the regions working together in IT Security (capturing EU, national, regional, public and private stakeholder views), represented by the partners?

B) CURRENT SITUATION

1) ENVIRONMENT (CONTEXT)

What are the significant trans-national influences/ change factors affecting IT security?

- Political
- Economic
- Socio-cultural
- Technological
- Legislation
- Environmental

2) IT SECURITY CUSTOMERS

Who are the main IT Security customers and what do they need from IT security research and IT security solutions that could be provided via trans-national providers?

- Energy
- Finance
- Health
- Mobile Communications
- Government

3) IT SECURITY INDUSTRY CAPABILITY

3.1 Identify Industry capability synergies and gaps across the regions, opportunities for cooperation, and recommendations.

4) IT SECURITY RESEARCH CAPABILITY

4.1 Identify Research capability synergies and gaps across the regions, opportunities for cooperation, and recommendations.

4.2 Assess the commercial impact of IT security research across the regions and how this can be improved.

4.3 Identify opportunities for Industry and Academic cooperation across the regions, and recommendations.

5) NATIONAL AND LOCAL INITIATIVES AND PROGRAMMES

Identify synergies and gaps across the regions, best practice across the regions, opportunities for cooperation, and recommendations at EU and MS level.

6) POLICY AND REGULATORY ISSUES

6.1 How do the policy and regulatory frameworks across the regions compare, and what are the cases of best practice?

6.2 What International co-operation agreements and activities are in place with EU and non EU states covering the regions?

7) STRENGTHS, WEAKNESSES, OPPORTUNITIES AND THREATS IN IT SECURITY

7.1 Strengths and Weaknesses of the Partner Regions (working together)

7.2 Opportunities and threats from forces, issues, trends and events outside the Partner Regions

8) COMPETITION AND COMPETITIVE ADVANTAGE

8.1 Where do the partner regions have collective competitive advantages in IT security?

8.2 What activities, capabilities and resources give the partner regions collective competitive advantages in IT security?

C) JOINT RESEARCH AGENDA AND ACTION PLAN (TO BE DEVELOPED BY THE CONSORTIUM)

Analysing the current situation, identify the key issues that the partner regions need to jointly address to enhance IT security capability and competitiveness, and agree joint IT security research priorities.

- Priorities should be based on addressing threats and weaknesses and exploiting strengths and opportunities.

Develop a future joint IT security research roadmap.

- Define the desired outcomes (goals) to address the key issues, and the specific measurable results to be achieved to achieve those outcomes (objectives), with timescales.

Identify the actions required to deliver the joint IT security research roadmap, with timescales.

- This should include policy and programme recommendations for key stakeholders, to enable the roadmap to be implemented.

10 CONCLUSIONS

A methodology has been developed that combines key individual organisation data and builds on that with regional-level information to provide qualitative and quantitative data that can be analysed to produce a regional IT security research agenda for each of the partner regions using a common structure. This will provide the basis for joint development of the pan-cluster research agenda by the consortium.

11 APPENDIX A – Individual IT Security research organisation information for regional research analysis

The following types of data will be needed for selected significant organisations to **allow comparison and aggregation of individual IT Security research organisation data**. Additional data, such as individual researchers and their key publications will be needed in the database for partner searching, but this is not addressed here.

ORGANISATION LEVEL DATA (1):

1. University or Company Name

2. Department or Business Unit

    2.1 Department or Business Unit Name

    2.2 Numbers of staff involved in IT Security R&D (with level of experience if possible)

    2.3 Address and Contact Details (includes web address)

    2.4 Location (Latitude and Longitude)

3. Strength of Research Capability

    This could be defined in various ways, but should use assessment systems already in use regionally, nationally, or internationally e.g. UK Academic Centres of Excellence in Cyber Security, international QS ranking system.

ACTIVITY LEVEL DATA (2):

4. Research activities

    4.1 Research topics (using categories in agreed drop-down list - example categories from UK Academic Centres of Excellence for Cyber Security Research, used by GCHQ and EPSRC, are given in Appendix C).

    4.2 Additional free text data including key phrases highlighting areas of expertise as identified by the group (e.g. names of groups, topics of interest, targeted applications, etc) from websites, abstracts, etc.

5. Research project data (optional but may be useful for the analysis to indicate where a critical mass of activity is taking place)

    5.1 Trustworthy ICT Research Projects

5.1.1 Funding Agency

5.1.2 Start Date

5.1.3 End Date

5.1.4 Value

5.1.5 Title

5.1.6 Collaborating partners

6. Commercialisation activities

6.1 Targeted markets and applications of current research

6.1.1 Description

6.1.2 Key words describing the Expected Applications of current research (applications not skills) from the 'K-Matrix Taxonomy'

6.2 Products and services (for industrial organisations)

6.3 Major industry partners and collaborations (for research institutes and universities)

6.4 Other, e.g. Spin-Outs

12 APPENDIX B – Individual IT Security Company information for regional Industry analysis

The following types of data will be needed for selected significant companies to **allow comparison and aggregation of individual IT Security Company data**.

ORGANISATION LEVEL DATA (1):

1. Company

    1.1 Company Name

    1.2 Department or Business Unit Name (if appropriate) e.g. Cyber Security Business Unit

    1.3 Number of employees

    1.4 Turnover (€/year)

    1.5 R&D Budget or R&D % Turnover (if applicable)

    1.6 Number or percentage of staff involved in R&D (if applicable)

    1.7 Address and Contact Details (includes web address)

    1.8 Location (Latitude and Longitude)

ACTIVITY LEVEL DATA (2):

2. Business activities

    2.1 Markets

    2.2 Products and services

        2.2.1 Description

        2.2.2 Key words describing the applications of the products and services from the 'K-Matrix Taxonomy'

    2.3 Major research partners and collaborations

    2.4 Other, e.g. Spin-Outs

3. Research interests and needs

    3.1 Research topics of interest (using categories in agreed drop-down list - example categories from UK Academic Centres of Excellence for Cyber Security Research, used by GCHQ and EPSRC, are given in Appendix C).

    3.2 Additional free text data including key phrases highlighting research interests and needs identified by the company.

13 APPENDIX C - Research Categories of the UK Academic Centres of Excellence in Cyber Security Research

This appendix contains material from the 'EPSRC Scheme to recognise Academic Centres of Excellence in Cyber Security Research - Invitation for proposals' dated 14 August 2012.

This Appendix provides a summary of the research areas that are within scope for Academic Centres of Excellence in Cyber Security Research. To be in scope, research in these areas must substantively address security, not merely using it as an example, nor having a sole focus elsewhere, such as, by way of example, on safety.

Cryptography, key management and related protocols

• cryptographic research

• quantum cryptography

• key management

• applied cryptography

• authentication protocols

• provable security

Information risk management

• technical threat assessment

• information risk assessment and analysis methods

• asset valuation and business impact

• information risk reduction and mitigation

• managing information risk and governance

Systems engineering and security analysis

• research into methodologies for engineering end to end systems

• high assurance software

• access control

• electromagnetic security

• side channel attacks and countermeasures

• embedded security

• system on chip, FPGA and ASIC design of cryptographic algorithms

• anti-tamper

• secure sanitisation

• reverse engineering

• hardware development techniques – for example, the use of COTS in secure products

Information assurance methodologies

• techniques for gaining confidence in software/hardware implementations of security controls

• measuring the effectiveness of combining different security controls in a system

• large-scale analysis of complex systems for design and implementation faults

• static and dynamic analysis of products and systems

• combining and targeting assurance techniques to make risk decisions

• translating assurance outputs into risk management decisions

Operational assurance techniques

• vulnerability discovery techniques

• intrusion analysis techniques

• active mitigation

• forensics

• malware analysis

• real-time situational awareness

• converting situational awareness or attack information into an assessment of the impact on the business

• vulnerability analysis

• intrusion tolerance techniques

• incident handling and response

• detection and prevention of e-crime

• threat mitigation

Research into the security of strategic technologies and products

• computing platforms, for example

  o virtualisation and trusted platforms

  o sandboxing and kernel/user Interaction

  o secure architectures

• communications technologies and architectures, for example:

  o security of mobile devices

  o cloud security

  o security of smart grid and smart metering

• data and service architectures

• databases and information stores

• infrastructure components and protocols

• web technologies

• identity management

• steganalysis

Science of cyber security and human factors

• security measurement and economics

• risk decision making

• analysing attacks

• security design

• human factors – developing techniques to allow proper risk management of human factors within the enterprise

Building trusted and trustworthy systems

• rigorous, formal methods for the development of secure systems

• research into the development of systems that are dependable/resilient/survivable in the presence of cyber threats/attacks

• research addressing privacy and trust issues in networked distributed systems

- research addressing security issues in cross domain working
- security in service-based approaches
- security as a service

14 APPENDIX D – Pilot exercise for validation of the database

Objective

One of the FIRE deliverables from WP2 is a database that allows “users” to enter information and so that they and others may ask questions that address their business needs. While this is **not** directly related to the Analysis Methodology addressed here, it has been necessary to consider its development during the methodology development. The database may be used to collect some of the information required for the pan-cluster analysis as described earlier.

The first stage of the database development is a risk reduction pilot to:

- Refine the likely question types
- Determine the practicality of acquiring and maintaining the underlying data
- Explore the shortcomings, if any, of the initial assumptions
- Understand better the practicality and trade-offs involved in implementing an “ideal” solution.

The pilot may also be useful in identifying relevant data for the analysis.

Database Users

The users are likely to include:

- Regional Cluster Coordinators (trade organisations)
- Industrial members of the Clusters
- Academic institutions who may or may not be Cluster members
- Those involved in oversight for policy or other reasons, e.g. European Commission.

The main purposes of the database are:

For Industry

- To find Academic research partners with suitable R&D expertise
- To find Industry partners with relevant products/ services/ skills

For Academia

- To find Industry partners for exploitation
- To find Academic research partners working in related areas for cooperation

Questions - Finding collaborators

This needs a pragmatic approach to balance the large volumes of data with the desired simplicity of maintaining the database and in framing questions. It is anticipated that the data will be available, in different formats, across organisations in each of the Member States. The aim of the database is to provide matchmaking ability, so that potential collaborating organisations may be identified. It is the first stage in a process involving business judgements, not the sole mechanism.

For the risk-reduction exercise, it is proposed that typical questions may contain one or more of the following elements (in any order):

- What organisations are working in the field of ….?
- How good are they?
- How big are they?
- Who should I contact?
- How close are they?
- Have they evidence that they can handle security-sensitive information?
- Have they evidence that they can establish a satisfactory commercial arrangement (IP exploitation, etc.)?
- How successful are they at forming industrial links?
- With whom do they have a relationship already?

Data Collection Process

Latency (keeping the data up to date) is a key issue. It is therefore proposed that the data to be entered should be data that will remain relatively fixed for 12 months or more. For example details of substantive research projects lasting 1-3 years should be collected but short research projects only lasting a month should not.

For individual organisations it is suggested that the following types of information will be required:

1. Organisation level data, (e.g. name, contact details, location)
2. Activity level data (specifically descriptions of current research expertise captured in research interests, publications and projects, and economic activity)

In both cases care will be required to ensure that that data are:

- Adequately detailed to support the type of enquiry that users may pose
- Not so large and complex that maintenance becomes difficult and costly
- Extensible, to allow, for example, new categories of activity to be captured without having to redesign the data structures.

The process by which the project partners will collect these data, using partner data sources, open sources, external stakeholder data and also direct input of data by individual organisations themselves is described in Table 1 and Figure 2. The pilot will validate the first version of the database and suggest adding and/or removing fields to make the database more user-friendly and effective for the dual purposes above.

Ideally one would wish that all organisations in the database will enter their own data in a defined format. However this has a number of disadvantages:

- It is not easily extensible as research definitions change
- Different organisation will allocate different priorities to entering the data (leading to unreliable and incomplete results)
- Consistency: different organisations will take different views of what data it is appropriate to add, and will describe things differently, using different terms and acronyms for similar things.
- The information will need maintaining and updating and the originators are unlikely to wish to undertake that task.

The data entry is therefore likely to fall to the Regional Cluster Organisations at least for the first iteration. While they may know some of these organisations well, others may be known only by reputation. Therefore public sources are likely to be a key source for location of this information. Keeping the data sought to a minimum may significantly improve the quality and currency of the database.

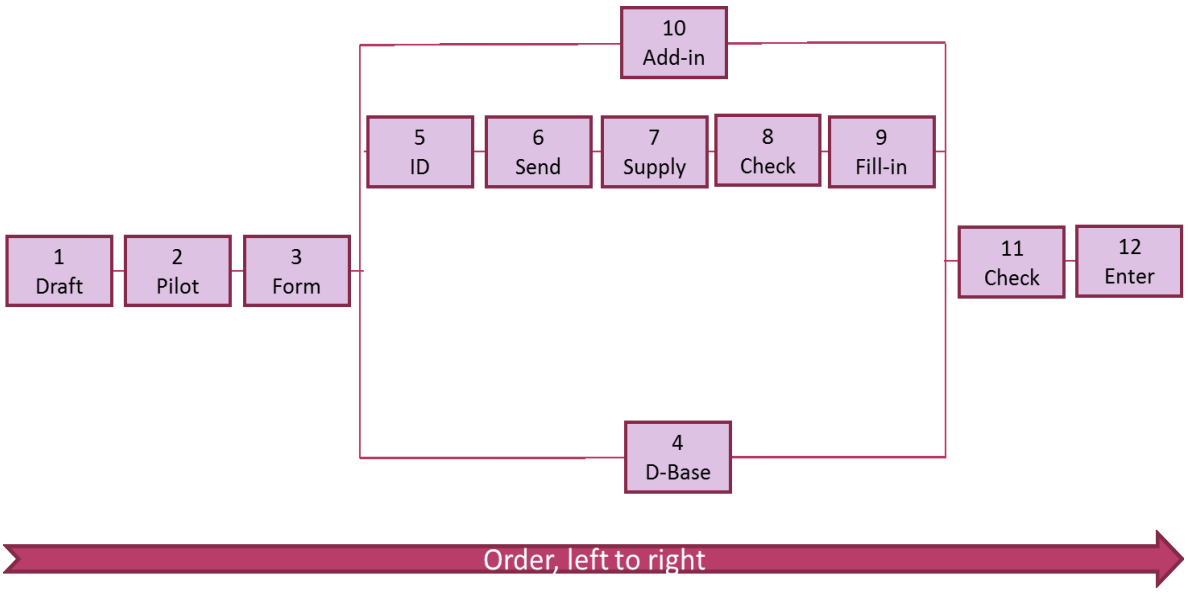


Figure 2 – Data Collection Process

Table 1 – Information Capture Approach

No.	Who	What
1	Partners	Agree draft structure for database
2	Partners	Design and implement risk reduction pilot with limited R&D data reviewed by potential users
3	LSEC	Design database form and guidance to capture data on individual organisation R&D capabilities and activities
4	LSEC	Design database structure – tables, standard queries and reports
5	Partners	Identify major players (institutes, companies, associations, funding agencies) to target to provide information
6	Partners	Send request for information on R&D capabilities and activities to third party organisations in partner clusters (e.g. LSEC to LSEC members) and other relevant networks (e.g. ADS to Cyber Security KTN members)
7	3rd Parties	Produce information for use in database and provide data to project partners
8	Partners	Check data returned by third party organisations for completeness
9	Partners	Fill in incomplete data (in third-party organisation Returns)
10	Partners	Add missing data forms (on behalf of third-party organisations)
11	Partners	Check data for accuracy prior to sending data to LSEC
12	LSEC	Populate database

An example of how the process could work for the UK activity led by ADS is shown in Figure 3.

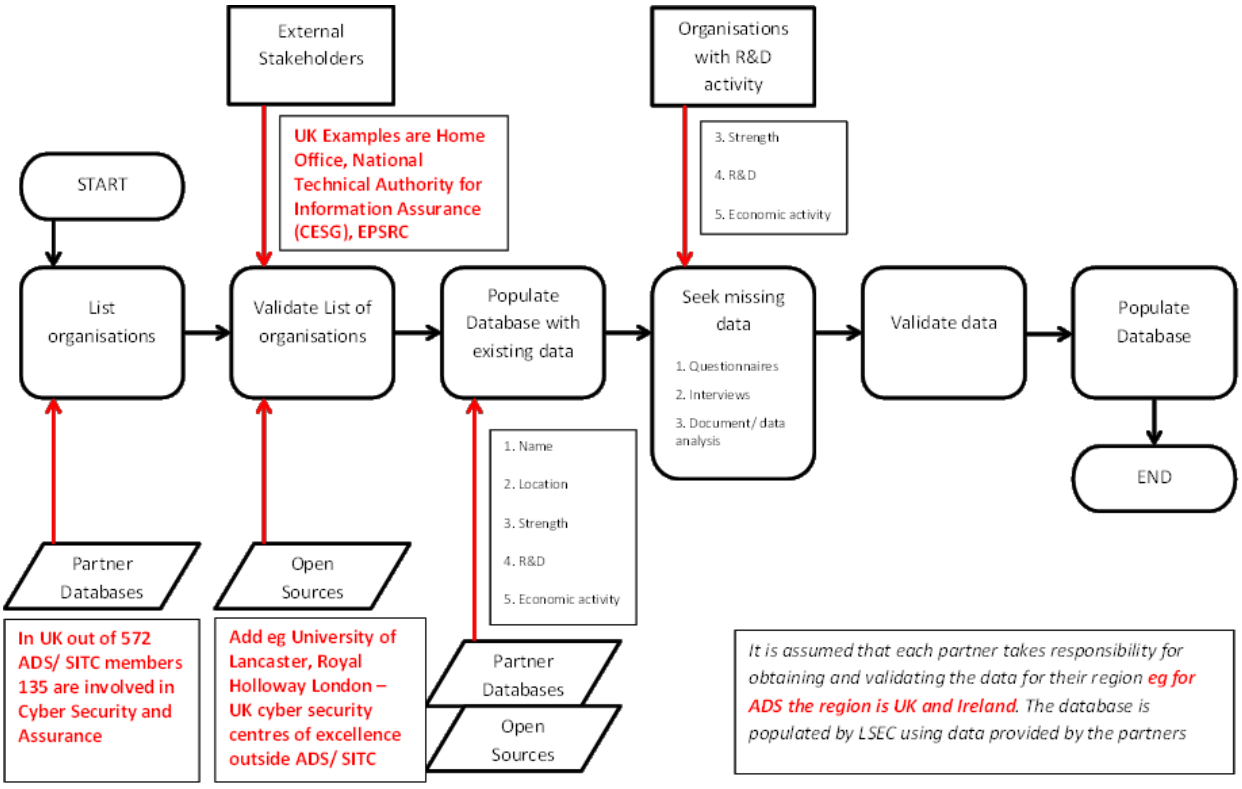


Figure 3 – Example of data collection process

Benefits and Buy-In

Attracting organisations to provide data for this project is a key issue.

Academic organisations could be attracted if the database 'system' provides the following benefits:

1. Identifies long-term research challenges to address industry needs.
2. Offers future funding opportunities – research grants and direct contracts from Industry.
3. Offers collaborative opportunities (industry and academia) – a 'dating service'.
4. Recognition – an accreditation, certification or other form of recognition system that gives enhanced credibility to organisations whose data is entered into and accepted into the database 'system'.
5. Brand/ Logo – a strong brand for the database 'system' that organisations (entered on the system) can display.

but the system will also need to be usable and credible with the following features:

6. Usability and functionality – an effective search system supported by tailored entry points personalised to the individual customer perspective.

Industry could also be attracted if the database 'system':

1. Reduces duplication – allows companies to identify, make use of and if appropriate buy the results of previous research projects and ideas relevant to them, saving them time and money.