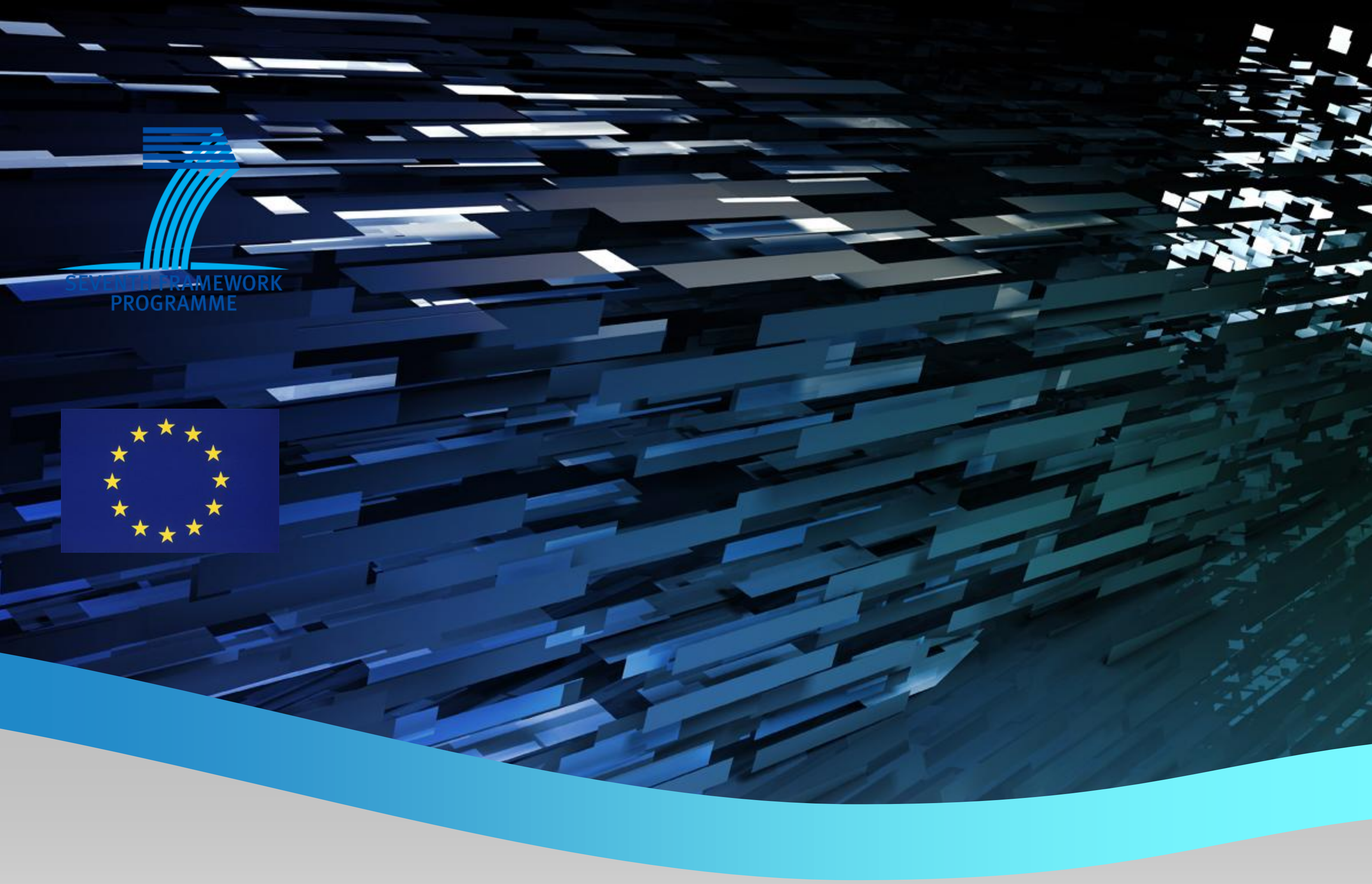

TDL Recommendations to NIS (WG3/SRA)

Editors: Pascal Bisson, Jim Clarke, Amardeo Sarma, Daan Velthausz, Volkmar Lotz, Arthur Leijtens, Stefan Bumerl

Contributors: community members at large with special input from Harm Jan Arendshorst, Eric Blot-Lefevre, Svetla Nikova, Antonio Skarmeta

Date: April 27th2015

Version: v1.1

TDL | Trust in Digital Life

www.trustindigitallife.eu

Table of Contents

Table of Contents

1.0 Introduction

Following the work undertaken by the Network and Information Security Public Private Platform (NIS Platform [1]), in particular, the NIS Strategic Research Agenda (SRA), it has become a priority for Trust in Digital Life (http://www.trustindigitallife.eu/) to support this initiative by sharing knowledge and aligning priorities. Hence, the necessary steps were taken by TDL to be present in the membership of NIS Platform and get organized to contribute inputs. Apart from TDL representatives already involved and contributing to NIS, it was decided to provide a short report herein highlighting some of the key (early) findings that could altogether be perceived as a TDL value-add proposition to the NIS platform with a clear focus on the SRA. In addition to addressing the SRA, it is likely that the recommendations herein could also be a value-add to other NIS Platform reports, including Secure ICT Research landscape, Business Cases & Innovation paths, and Education & Training for workforce development.

After a short reminder on the TDL Vision and how it could be beneficial to the NIS Platform, the TDL value proposition is presented. This is done under the format of a number of recommendations to NIS Platform at both research and instruments level. Overall actions here proposed by TDL are aiming to complement or supplement the work done by the NIS Platform.

This report primary targets NIS platform's SRA, prepared by its WG3, and focusses on issues related to Cyber Security research and innovation in the context of the EU Strategy for Cyber Security. However, the report is also relevant for other NIS WGs (i.e. WG1 on Risk Management and WG2 on Information Sharing) and the SRA community at large.

2.0 TDL Vision

TDL's view on research priorities is driven by an observed erosion of trust, caused by both opportunistic and organized cybercrime with increasing impact and frequency. In addition, privacy threats to citizens and society with numerous incidents and breaches of trust and privacy are on the increase. This leads to an increased awareness of security and privacy topics, as reflected, for instance, in European initiatives for directives targeting security and privacy. Paradoxically, at the same time, the online behavior of people is less risk-aware than in the physical world. Hence, research priorities should address the establishment of trustworthy ICT[1] solutions from a technical, economic and societal perspective, with the concepts,

[1] In accordance with the EC's definition [4], trustworthy ICT provides security, privacy and trust in major information and communications technological areas, for example: cloud computing, mobile services and the management of cyber incidents, amongst others.

methodologies and technologies being able to adapt to the rapid changes in ICT solutions and business models encountered in the recent past and continuing in the future.

3.0 TDL Recommendations on Research Topics

Following a comprehensive review of the NIS Platform WG3 SRA [2] made available for this report, TDL has recommendations for NIS Platform on four areas, in no particular order:

- Economics of Trustworthy ICT;
- Assurance;
- Privacy;
- Compliance to new regulations.

The identification of those areas is a result of discussions among the TDL membership (kicked off at a workshop held on the September 2014 TDL meeting) and the editors/contributors of the document. They are highlighted due to the fact that they correspond to research areas of shared interest and priority, on which TDL has been active and remains active (see TDL SRA [3]).

Each of them are hereafter considered in the light of what has been covered and a rationale for further coverage required.

In the following sections, we thus detail each of the recommendations highlighting some of the research priorities perceived from the TDL perspective as an industry-driven research initiative.

3.1 Economics of Trustworthy ICT

R1. TDL recommends emphasis on **investigation into the economics context**, together with **research that focuses on cost and benefit aspects of trustworthy ICT as well as market conditions and dependencies**. **Multidisciplinary research** is essential including stakeholders from technology, economists, sociologists, computer scientists, etc.
Overall TDL recommends that the EC should work directly with the **Member States and Associated Countries** to come up with **new / sound business models for trustworthy ICT in the EU**.

TDL acknowledges the critical role of economic factors in the provision of trustworthy ICT: technology solutions need to translate into business for providers of trustworthy ICT. That security and privacy have been identified as business and societal priorities alone does not suffice. Industry is responsible for deploying trustworthy infrastructures and solutions, and the provision of such products and services will only be successful if there are incentives for businesses and the customers. Currently, such incentives do not exist. For instance, the business value derived from additionally gathered data for marketing purposes exceeds gains that can be made out of privacy friendly services. This provides no incentives for data providers to follow the principle of data minimization beyond the required minimum necessary for compliance. Penalties for non-compliance in several cases are calculated as low or medium impact risk factors.

TDL has introduced the **concept of business value of trust** to better understand the relations between the impact of incidents, the transparency of incidents and the willingness of consumers and vendors to invest into trustworthy ICT. This concept helps to investigate the requirements for a trust paradigm shift, addressing the **challenge of increasing the net customer value of trustworthy ICT solutions** and, hence, their adoption rate. In addition to positive effects by laws and regulations, this can be achieved by actions that *decrease the costs of development and maintenance of trustworthy ICT*[2], thereby increasing the perceived need for trustworthy solutions and the preparedness to pay for it. Paying does not automatically imply that ICT will become trustworthy.

A critical part of this trust paradigm shift will be in a transition to a business and technical environment where the economic benefits of protecting the assets, in particular, the situation where the benefits from protection of the data of citizens and enterprises, exceeds the benefits from exploiting the assets and data. In this environment, businesses and customers will be automatically informed how their data are stored and processed, the security measures the data processor implemented and they will decide if they allow to use their data for marketing purposes and they can set the price for this use.

Therefore, TDL recommends research on the economic and technical solutions needed to enable this transition. The research would need to involve economists, sociologists and psychologists in addition to security and privacy researchers. In the future, it should become a net business risk to not provide trustworthy solutions. In relation to the economics of trustworthy ICT, TDL sees a need to increase the investment in research related to:

- ***Trust as an economic factor***. Trust is fundamental to the economy, where exchange of goods and services are separated in space and time. One can frequently hear the sound statements like „The currrency of new Economy is

[2] Such actions may include, for instance, the adoption of technical innovations increasing the degree of automation of secure development, security monitoring tools, low-cost certification schemes, and more

trust" or „We are entering the trust economy". Indeed, at the starting point of the future internet era, economists and ordinary people have to understand the value of trust not only on a conceptual level but on the level of everyday practice. Understanding the economic, societal and psychological aspects of trust in the internet economy helps companies in design and implementation of trusted ICT systems. Industry focuses on security, but security is not equivalent to trust. Market value of an ICT product or service is basically determined by the perceived trust of the customers rather than the measurable technical security. The proposed research should aim at understanding the security – trust transition and its use in the product design and marketing.

- ***Economic value of personal data.*** Social networks, search engines and many other ICT service providers have built and implemented very successful business models on the exploitation of user's personal data, as demographic data, geolocation, interests, buying habits etc. They provide free services in exchange for personal data. The question arises if this exchange determines the economic value of personal data, and if the answer is yes, what is the value of our data? Knowing the value of one's personal data and the quality and quantity of services used in exchage helps making informed decisions about trusting or distrusting the service.

- ***Distributed trust.*** We have learned from the evolution of the Bitcoin type of cryptocurrencies that if a sufficient number of anonymous members in a network guarantees the validity of a transaction or statement, it builds up a trust equivalent to the trust generated by traditional institutions, e.g. banks. Even large banks consider the use of the blockchain technology for general ledgers, as an equivalent to the centralized ledgers. In the era of future internet and shared economy, a few traditionally trusted institutions will not be relevant, and the only replacement might be distributed trust, or „trust by the crowd". The research should aim at the development and implementation of ICT technologies of distributed trust.

3.2 Assurance

R2. TDL strongly supports the NIS SRA emphasis, expressed by all Areas of Interests (AoIs), on assurance and recommends a focus on **cost-effective approaches to assurance**, including all different flavors reaching from **security and privacy by design** to **certification schemes** and **informed user decisions based on risk assessment**.

Overall focus should be put on **cost reduction and risk reduction for all stakeholders**, not only to assurance but **to security in general,** including legislation: having a "security framework" in place that balances the trade-off between cost and risk reduction. When it comes to liability (assets value, guarantee digital evidence value) assurance has also to be put in relation to Economics of Trustworthy ICT (see R1).

TDL supports the emphasis on assurance that has been expressed by all Area of Interest viewpoints in the draft version of the NIS Platform SRA. At the end, it is not sufficient to provide trustworthy products and services, if the level of trustworthiness cannot be **demonstrated to** and **assessed by** the **users and consumers**. TDL recommends an increase of the investment in research related to:

- **Cost-effective approaches** to assurance, including all different flavors reaching from security and privacy by design to certification schemes and allowing the user to make informed decisions based on risk assessment. Beyond the development of novel and effective assurance methods and technologies, multi-disciplinary research on their dependencies, the user's perceptions and the economic context is encouraged, involving all of the relevant stakeholders.

  "Cost-effective" means that the effort that is spent to demonstrate security and privacy qualities of a software or a service is adequate with respect to the protection needs and the risk in the given system context. Hence, a prerequisite to achieve cost-effectiveness is the understanding of the related security and privacy requirements as well as a quantified statement on the respective risks. This foundation of a **security engineering discipline** is currently insufficiently developed, as they have only focused on technical aspects rather than business considerations. New approaches to **security requirements engineering, security metrics and risk assessment schemes** based on the latter are needed.

- **Security and privacy by design**, including all methods, techniques and tools that aim at enforcing security and privacy properties on software and system level and providing guarantees for the validity of these properties has the greatest potential to provide assurance at adequate costs: it is common understanding that investments in the early phases of development pays off. Empirical research to back up this understanding by providing hard figures, together with approaches that allow a smooth migration of legacy systems is key to establish "by design" methodologies. TDL recommends a focus on software security and privacy friendly design, since those are addressing today's most important concerns and sources of vulnerabilities.

- **Certification schemes** – including both product and process certification – have been shown as a meaningful approach to security and privacy assurance, in particular, being recognised by users as an assurance means. However, many of the schemes suffer from a trade-off between the expressiveness of the certificate and the effort required to achieve a certificate. Hence, investigations into cost-effective schemes (for both suppliers and consumers of systems and services) can boost the value and proliferation of certification schemes.

In summary, TDL recommends to *further* **invest in research related to cost-effective approaches to assurance**; TDL also encourages multidisciplinary research on dependencies of the novel and effective assurance methods and technologies developed as well as the user's renderings and perceptions also in the economic context.

3.3 Privacy

R3. TDL supports an emphasis on investments in research relating to **privacy of citizens**, in particular, how the privacy friendly and privacy enhancing technologies can **translate into** and **support viable business models of the future.**

To establish trust in digital life, protecting the privacy of citizens is an essential ingredient. Many research results for privacy friendly and privacy enhancing technologies have been delivered; however, their translation into innovative products and services that support a viable business model is still in its infancy. Key questions mentioned in the NIS Platform draft SRA, including cost effectiveness and simplicity, usability, relation to security aspects, and interoperability still need to be solved. TDL supports an emphasis on investments in research relating to these priorities, in particular, since recent technology and business developments, including cloud computing and Big Data, are on their way to dominate the market, raising additional privacy concerns. As a recurring theme, multi-disciplinary research, including economic, psychological, legal, and societal aspects, is required to gain deeper insights into the mechanisms and incentives for enabling privacy friendly technologies to become a viable business case for Europe and beyond.

Therefore, in complement with priorities shared by NIS on the Privacy topic, TDL recommends to invest on research related to new privacy concerns resulting from new business developments (e.g. Cloud computing, Big Data) and also calls for multi-disciplinary research to gain insights and be more successful on the creation of a viable business out of the privacy friendly / enhancing preserving technologies to date and in the future.

In relation to privacy, TDL sees a need to increase the investment in research related to:

- **Challenges in Privacy Engineering.** A key open challenge is how to integrate PETs, established and custom, into an overall process of secure software development to ensure they meaningfully contribute to the protection of users. A key research challenge involves the design of PETs that are easier to compose and integrate into designs, and PETs that are more usable for both designers, engineers and end-users.
- **Location privacy.** The widespread adoption of mobile devices, and the richness of location data has raised concerns with respect to location privacy. Designing mechanisms and location-based services that effectively prevent the unwanted disclosure of location data remains an open challenge. One of the difficulties of finding effective location privacy solutions lies in the tradeoffs between utility and privacy inherent in many mobile applications, in which location information is used to customize content (e.g. nearest points of interest). More research is also needed to enable anonymous access to services or the web from mobile devices.
- **Privacy-preserving cryptographic protocols.** Engineering encryption systems that hide meta-data, such as the timing and volume of communications, the end-point identities, etc., is still an open problem. More research is needed on how to co-design the services and encryption channels to hide important meta-data with the minimum amount of additional traffic or delay.
- **Dynamic Privacy**: Need to move from actual model of static privacy and security to a user centric dynamic vision of securities and privacies with offering different level of privacy and security based on the context, where concepts like circles of trust will affect the way trust is managed. What will be needed is a dynamic negotiation of the capabilities and policies that will be applied to the communications within different trust zones.
- **Privacy Preserving techniques**. It is important to investigate into better integration of claim based authentication infrastructures, access control and policy based solutions in order to empower users with control on how their data is disclosed and incorporate data minimalization solutions as default.

- **Security, privacy and trust in 5G and advanced networking paradigms like SDN, data centric networking,** etc. These paradigms represent a new approach to data exchange and data sharing that needs to adapt the security and privacy framework to take into account new requirements like group communications and distributed access control policies.

3.4 Compliance with new legislations/regulations

R4. TDL recommends to investigate in the **upcoming EU directives (e.IDAS, Data Protection, NIS)**, and advance **technologies, standards methods** and **processes** in order to provide practical (actionable) and interoperable (ICT) solutions on which to leverage, and which can be certified as compliant with these new legislations.

Most of the research recommendations below are based on extensive work performed by TDL on regulations – more specifically, on the e.IDAS regulation on electronic identification and trust services for electronic transactions in the internal market, a regulation adopted on 23 July 2014 and becoming effective on 1 July 2016.

A common characteristic of the new regulations (e.IDAS/Regulation of exchanges, Data Protection/Privacy and future Directive NIS/Risk Management) is the transfer of performance obligations. For instance, e.IDAS shifts responsibility for material proof from individuals and their subcontractors to online trust service providers. These trust providers are now responsible for jointly establishing electronic proof, under the control of a validation and legal certification authority, on behalf of individuals and their clients.

The new trustworthy architecture of security, privacy and probative value (evidence value) dedicated to all transactions, payments and correspondence mailing on line has also to be compliant with instantaneous interoperability and resilience IS0 27006-35 (correspondence banking & correspondence mailing issues).

While e.IDAS is focusing on online trust and the NIS directive is focusing on CyberSecurity, the overall objective remains comparable: ensure that the ICT system at hands – typically of complex socio-technical nature – is indeed compliant/conformant with the legislation(s)/regulation(s) that apply(ies). This needs to be done in an auditable and certifiable way. This calls for a number of capabilities (also practicalities) to be enabled through advancement of research and technology, mainly in the area of compliance (live-cycle) management (although not uniquely) for regulations/legislations to be supported through proper tooling and processes leading to operational solutions. For what concerns compliance with legislations/regulations, TDL recommends to invest in the following areas:

- Research on the **economics of compliance** to get a better understanding of the economic drivers including the costs of non compliance (also its root-causes),
- Research on **"ICT actionable" legislation/regulation** to encourage a new engineering approach to legislation and/or regulation in order to make them actionable from an ICT perspective. Co-engineering would be here key to achieve,
- Research on **compliance management** including developing a better understanding of the full life cycle for compliance management as well as the enabling tools and/or techniques at each of the steps (from design to deployment going through development and certification). Challenges may range here from qualifiction of all mandated stakeholders together with their interfaces (especially with respect to validation instances that apply) to implementation of user and root user control policies, their enforcement through conforming management and control functions, the detection and resolution of compliance conflicts, liability management, accountability, creation of documentary certification schemes for all correspondence and more.
- Research on drivers for compliance solutions adoption. This includes research on standards advancement to ensure interoperability of the compliance solutions but also compatibility with existing offer (e.g. service in SaaS mode from ERP vendors)

In summary, what is at stake here is the co-engineering of practical solutions (i.e. simple and **low-cost solutions** that still maintain compliance), their enablement through research and technology advancement and the ease of their adoption.

4.0 TDL Recommendations on Research and Innovation Instruments

In the previous section, a number of recommendations on research priorities to NIS platform's SRA have been made from the TDL (industry-driven) perspective. Most of them result from puttingthe NIS Platform's SRA (as per today) back into perspective of TDL's SRA as it has been defined and so far implemented. Overall, this has shown some complementarity between the two SRAs and highlighted areas of shared interest where further research is recommended and so might be included to be reported in the NIS SRA.

Apart from key contributions the TDL SRA may provide to the NIS Platform's SRA, TDL has also gained significant experience on how to turn successful research results into successful innovations. Accordingly, it has developed a number of enabling concepts and/or instruments and it was felt advantageous to raise the awareness of these to the NIS Platform and EU Commission at this point, especially those proven to be effective in bridging the gap between research and innovation.

Overall, those proven concepts and instruments are highly valued by the TDL Community members because they enrich applied research and help to validate what it has accomplished. The next sections will highlight these instruments of TDL and provide recommendations on how such instruments can provide added value for the NIS Platform and indeed the wider European research programmes.

4.1 SPRINTs

SPRINTs are short term (3 to 6 months) collaborative projects aiming at the validation of innovative product - or service concepts. Their focus is not on the establishment of new technical research results, but on investigations into the usage and the integration of existing results in larger-scale architectures, infrastructures or system and service landscapes. For instance, take a novel solution for a privacy-friendly trust service that is meant to be used in a cloud platform – in a SPRINT project, the providers of the trust service and the cloud platform can experiment the integration of this service in the platform, receiving feedback from the development activities on technical improvements as well as from a user trial on the usability and utility of the solution. Such a SPRINT can lead to the identification of new research challenges (to be addressed in follow-up research projects), standardization activities, or updates of the technical solutions.

Example of sprints run by TDL include

- the development of a framework and architecture for serving complex identity infrastructures,
- a cyber-security sprint that conducts compliance checks and risk assessments using a BYOD scenario in an SME environment
- a user trail investigating into privacy preferences for online services

SPRINTs provide significant value to the TDL ecosystem by enriching of existing services and products by combining and adding functionality and making existing products or services more trustworthy by following design principles and adding new functionality.

4.2 TDL download corner

TDL believes in the value of sharing research results and making their tangible outputs (i.e., software components and services) available for experimentation by the membership. To facilitate this exchange, the “download corner” on the TDL web site provides a service where TDL members can offer, use and validate trustworthy elements (e.g. technology components). TDL members have the possibility to “play around” with technology that is offered and can provide feedback to the element provider (i.e. the publisher). The requirements for element publishers to deploy trust elements to the download corner are the provision of a stand-alone service element, first level support, and optional an online questionaries’ to be filled in by the users to gain user insights.

Such a download corner could be made accessible to the European research and innovation community via the NIS platform, to use the available elements as well as to add new elements. This facilitates the uptake of research results by providing an easy means for experimentation and validation beyond the project scope in which they have been developed.

4.3 TDL portfolio management

TDL has implemented tooling for strategic portfolio management. This tooling environment is used to plan, monitor and improve the innovation roadmap and project portfolio funnel of TDL. It implements an architectural framework with models and calculations on the economic value and social & trust impact. Using the portfolio management tool, TDL identifies the white spots and bottlenecks and analyses the impact of new/changing law and regulation. Input is gathered from EU projects, from market research by consulting firms such as Gartner, from EU Commission strategy, and SRAs (e.g. including the NIS platform’s SRA). By explicitly demonstrating the business and societal potential of research work, the transition of results into practice is accelerated.

The TDL portfolio management can be utilized, adapted and made accessible to the NIS platform to monitor the implementation of the cyber security strategy by mapping public and private projects on the priorities of the European Commission and forecasting the social and economic impact.

5.0 Conclusions

This document has highlighted some of the (early) recommendations of TDL for the NIS Platform WG3 in charge of the Strategic Research Agenda (SRA). The recommendations relate to four main research topic areas: Economics of Trustworthy ICT, Assurance, Privacy, and Compliance with new regulations.

The report details research challenges for each main area in which further emphasis and investment should be considered by the NIS platform, given from the perspective of the industry-driven TDL SRA.

Overall, it shows that TDL is committed to support a Cyber Security ecosystem through not only TDL's own SRA and its revision but also expertise and experience gained as well as tools, assets, techniques and processes put in place at the TDL Community level. TDL has shared interests with the NIS Platform and is strongly interested to provide its support to develop the NIS Platform SRA.

Of course, the work started here will be continued and these recommendations would be further detailed and possibly complemented with new ones to further align towards the NIS SRA latest developments. Conversely, the cross alignment with the NIS SRA will also be utilised to revise the TDL SRA in order to better align it towards topics in scope.

References

[1] Network and Information Security Public Private Platform portal
https://resilience.enisa.europa.eu/nis-platform
[2] NIS SRA: SRA-draft-v02.63
[3] TDL SRA: TDL-SRA-version-2
[4] ICT Work Programme 2013, http://cordis.europa.eu/fp7/ict/docs/ict-wp2013-10-7-2013-with-cover-issn.pdf