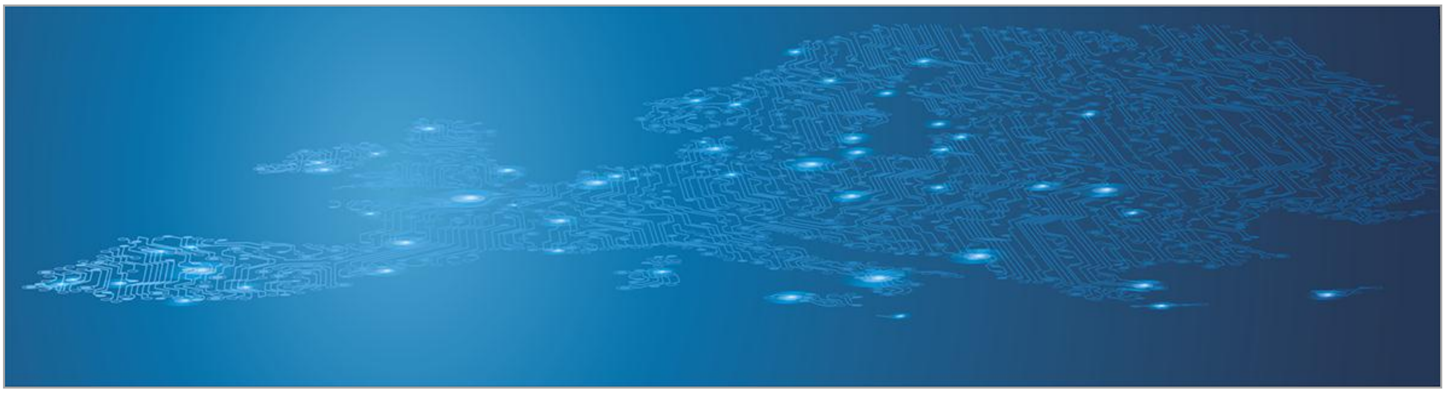


EP3R 2013 – Position Paper

Task Forces on Terminology Definitions and Categorisation of Assets (TF-TDCA)

December 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Editors

Lionel Dupré, ENISA

Rossella Mattioli, ENISA

Contact

For contacting the authors please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The following EP3R Experts volunteered to participate in the task forces:

Terminology Definitions

- Athina Fragkouli RIPE NCC
- Bastiaan Goslings AMS-IX
- Christian Doerr University of Delft
- Cornelia Kutterer Microsoft
- John Michael Foley Danish Ministry of Defence / Project office for Cyber Security
- Michele Minichino Enea
- Octavia Frota High-Ads
- Simona Cavallini Formit
- Wim Degezelle CENTR

Assets Categorisation

- Athina Fragkouli RIPE NCC
- Benjamin Lambrecht BSI - German Federal Office for Information Security
- Chris Buckridge RIPE NCC
- Genseric Cantournet Telecom Italia
- Luis Ángel Fernández Escabías Bdigital
- Octavia Frota High-Ads
- Bastiaan Goslings AMS-IX
- Patrick Palm Ericsson
- Peter Biro Ministry of Finance of the Slovak Republic

- Uwe Jendricke BSI - German Federal Office for Information Security

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Executive summary

Since 2011, the plenary sessions of EP3R addressed a number of topics ranging from Trusted Information Sharing, Incidents Preparedness and Management, Mutual Aid Assistance and the Protection of Critical Information Infrastructure.

As EP3R discussions progressed, participants realised gradually that many concepts and terms were not clearly defined.

During Summer 2012, the EP3R constituency devised a number of Work Objectives, and the initial Working Group 1 on Key Assets Categorisation led to the Creation of two Task Forces to issue a proposal for a methodology. The two topics addressed would be “Terminology Definitions” on one hand, and “Categorisation of Assets” on the other hand.

Since a common terminology is the base of the characterisation of assets, it was later decided to use the latter to initiate the first.

Both Task Forces were given 3 months to reach a conclusion on both topics. A few teleconferences and individual contributions helped to build this document.

Together, the efforts of these two different task forces also represent the starting point for future efforts to secure and improve resilience in Europe’s cross-border and cross-organization context.

Another important trait of these two task forces with the other EP3R position papers is the use of the Mutual Aid for Resilient Infrastructure In Europe (MARIE) ingredients in order to offer to all the interested stakeholders a comprehensive and articulated approach for cooperation and collaboration.

The work produced by both Task Forces includes:

- A list of commonly accepted Terminology sources; (see Annex A)
- A proposal to categorise Terminology definitions according to their context; (Annex C)
- An initial devise of key terms, those initially necessary to all Task Forces and further EP3R works; (Chapter 2.4)
- An ontology for categorisation of assets and future development of Terminology Definitions; (Chapter 3.2)

As a common approach to subsequent activities (such as Risk Management, Business Continuity Management, etc). The Task Force recommends the pragmatic adoption of the 8 Ingredients devised in the M.A.R.I.E. (Mutual Aid for Resilient Infrastructure in Europe) as root Categories for Key ICT Assets. Should other sectors be later considered, a similar ontology could be developed where needed.

Those recommendations were intended for EP3R, but however are valid for any Public-Private Partnership including EP3R’s successor, the NIS Platform.

Table of Contents

1 Introduction 1

2 Adoption of Terminology Sources 3

2.1 Key Terminology 3

2.2 Terminology Sources 3

2.3 Categorising Terminology 4

2.4 Adopted Terms 5

3 Assets Categorisation Principles 9

3.1 Introduction 9

3.2 Initial Ontology 9

4 Conclusions 11

1 Introduction

This Position Paper intends to establish the foundations of a commonly accepted and adopted methodology to define proper Terminology within EP3R, and later allow a concise Key Assets Categorisation.

Such a Position Paper was intentionally kept small so it could be easily communicated and shared among EP3R participants to foster common understanding in a fast and effective way.

The principle adopted within EP3R was that each Task Force would establish their own specific Terminology whenever required, and use this approach as a principle.

Goal

The purpose of inventorying Terminology sources was initially to ensure that all Participants could work on the same grounds, and allow discussions to be cleared from any misunderstanding.

Target audience

This Position Paper is addressed to all EP3R participants and the NIS Platform Working Groups.

The methodology used in these task forces is similar to previous EP3R efforts. Several seasoned industry experts from different organization and backgrounds provided their expertise and advice in the definition of the contents.

Following to on-site meetings and the desktop research, some individual feedback and recommendations where provided and used to integrate the materials collaboratively exchanged and produced via email and during the open teleconferences. The contents and participation to these task forces was renewed in two different occasions and cover a wide spectrum of expertise and different type of organizations and backgrounds.

These initial efforts lasted two months during Spring 2013.

Terminology Definitions

During the early stages of work in the EP3R working groups, Participants have many times reported that several words were lacking a clear definition and also a common understanding.

As a consequence, discussions were hanging on details to clarify, instead of allowing a seemless and fluid debate.

The EP3R Working Group 1 on Key Assets therefore recommended that a Glossary is collegially adopted by EP3R constituency as a reference for further works.

For these reasons the scope of the Task Force was focused on:

- Taking stock of existing Terminology definitions available freely (to avoid licencing issues);
- Identifying commonly used terms in the CIIP sector;
- Providing or reuse (where possible) for each term a simple and effective definition, avoiding controversial definitions as much as possible.
- Using free sources for such definitions where available to build up their recommendations, or get authorisation from relevant author(s).

The Deliverable of the TF was defined as follows in the EP3R Work Objectives:

- A list of Terms commonly used in the CIIP Industry;

- A proposal of definition for each term, reusing where possible open and free dictionaries;
- A list of commonly used Sources in the ICT Sector.

Assets Categorisation

A risk assessment of the protection level of Critical Information Infrastructures depends initially on a comprehensive inventory of all the components which constitute them.

These are generally referred to as “assets” and comprise equally physical and technical assets, facilities, but also resources (e.g. supply chain), functions (i.e. Human operations), and regulatory environment (e.g. Policies, Standards, etc).

A proper risk analysis approach would take into consideration any ingredient of the resulting service operated, and assess each asset category’s risk occurrence and likelihood.

Since EP3R focuses on the proper operations of Critical Information Infrastructures (and unlike the Art.13a regulation *not* on the services), the actual operations of the CII are under the initial scope of reflection.

The Task force was requested to undertake all necessary actions to define a proper and useful approach to the usage of CII stakeholders to ensure all Critical Assets supporting CIIs are encompassed in risk analysis, business continuity planning and disaster recovery exercises, hence ensuring proper preparedness and response capability for disasters or incidents.

This requirement arose following the presentation during an EP3R Plenary Session (December 2011) of a major Telecom Operator’s Risk Management methodology.

Among the activities undertaken, the following have been considered:

- Taking stock on current practices in place in Member States for defining NCIs;
- Taking stock on Industry’s Risk Identification and Risk Management good practices;
- Evaluating the setup a reference framework and initiate a research activity on the methodology for the identification of ECIIs. “Functional” supply chains could be identified together with connections/ interconnections.
- Convergence to a final, simple result.

The Deliverable of the TF was defined as follows in the EP3R Work Objectives:

- A taxonomy of typical components which constitute a Critical Information Infrastructure.
- From the various methodologies proposed, select the parts relevant to Critical Information Infrastructures Protection, and establish a formal recommendation for a set of criteria allowing “Key Assets Identification”.

2 Adoption of Terminology Sources

2.1 Key Terminology

During the discussions of the Task force it was decided to start addressing the issue using a taxonomy approach. Due the short timeframe and the voluntary basis involvement it was considered difficult to produce a comprehensive glossary covering all the possible terms. Therefore the TF decided to give a clear and unique definition only of the most important concepts that represent the foundations of all EP3R efforts.

The result is close to 160 definitions gathered from free access sources, properly referenced, and some definitions developed by the TF members themselves when the existing ones were not satisfactory.

For the broader glossary it was preferred to define a first list of most common term and for those not covered use taxonomy to characterize the most important clusters and bound them with the most relevant references present in literature.

The following definitions were identified, adopted by the Task Force, and used as foundation for all discussions relating to Critical Information Infrastructures.

2.2 Terminology Sources

While discussing the allocation, it was possible to pinpoint the following list of references from authoritative resources for each cluster.

ICANN

- Bylaws for Internet Corporation for Assigned Names and Numbers

IETF

- Internet Engineering Task Force - RFC 4949

ISACA

- Control Objectives for Information and Related Technology (COBIT)

ISO/IEC

- 27000 series - Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ITGI

- IT Control Objectives for Sarbanes-Oxley

NATO

- AAP-6, NATO Glossary of terms and definitions

IARU

- The Tampere Convention

United Kingdom's Cabinet Office

- Information Technology Infrastructure Library (ITIL)

European Commission

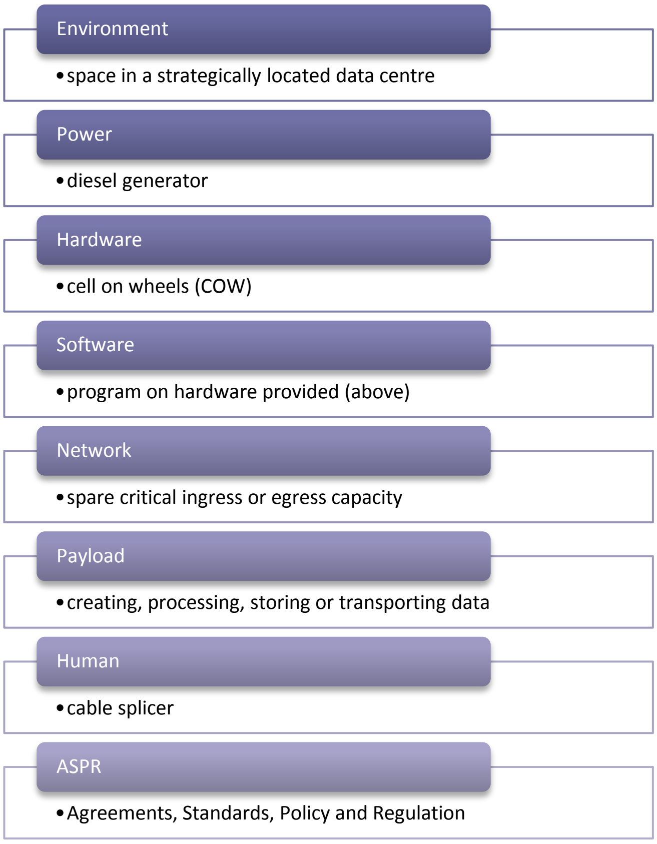
- Council directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection
- Green paper on a European programme for critical infrastructure protection - COM/2005/0576 Final

ENISA

- Risk Management - Glossary
- Inter-X: Resilience of the Internet Interconnection Ecosystem

The present list does not cover all the possible references but can allow the creation of a common baseline in defining typical components which constitute a Critical Information Infrastructure.

2.3 Categorising Terminology


Environment
- space in a strategically located data centre

Power
- diesel generator

Hardware
- cell on wheels (COW)

Software
- program on hardware provided (above)

Network
- spare critical ingress or egress capacity

Payload
- creating, processing, storing or transporting data

Human
- cable splicer

ASPR
- Agreements, Standards, Policy and Regulation

A given term may take different meanings depending of the context of use, and therefore the use of categorisation will allow to overcome controversy in the adoption of terms.

The process of organising the terminology required an initial assumption, and more specifically to avoid reinventing the wheel. It was suggested to use the 8 ingredients mentioned in the MARIE report[1] in order to align this output with previous works and to provide continuity both in scope and terminology.

The full list of Categorised Terminology is attached in Annex C.

The definition of an agreed common terminology definition not only poses the baseline for Categorization of assets, but fosters also a the definition of mutual efforts between cross-industry and cross-border communities. Basing the terminology cluster reference on the Mutual Aid for Resilient Infrastructure In Europe (MARIE) eight ingredients provides a mutual starting point but also maximize the convergence of the task forces outputs, starting with the establishment of proper Terminology in each Category.

[1] Rauscher, K.F., Krock, R.E. & Runyon, J.P., 2006. Eight ingredients of communications infrastructure: A systematic and comprehensive framework for enhancing network reliability and security A. P. Macwan, K. K. Mutha, & R. S. Hanmer, eds. *Bell Labs Technical Journal*, 11(3), pp.73–81.

2.4 Adopted Terms

The table below includes a (short) version of the definitions proposed by the Task Force Participants.

We have selected initially terms extract from sources which do not originate from the ENISA Risk Management glossary.

A list of approximately 160 terms and their source and categorisation, please refer to the list attached in Annex C:

Term	Categorization	Definition	Source
Backbone	Network	The central core of a network aroudn which the remainder is built.	EP3R TF-TDCA
Component	Hardware, Network	An item of electronic communications equipment that forms part or all of a node.	EP3R TF-TDCA
Critical Information Infrastructure	Network	Information infrastructure (like networks, hardware, software, etc.) that is critical to the functioning of a nation or country, like IT that supports health- or energy-sectors.	EP3R TF-TDCA
Critical Infrastructure	Hardware, Network	an asset, system or part thereof located in Member States that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions.	„COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection“
Disaster	ASPR	means a serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as the result of complex, long-	The Tampere Convention

Term	Categorization	Definition	Source
		term processes.	
Disaster mitigation	ASPR	measures designed to prevent, predict, prepare for, respond to, monitor and/or mitigate the impact of, disaster 12. Relief operations means those activities designed to reduce loss of life, human suffering and damage to property and/or the environment caused by a disaster.	The Tampere Convention
Fixed network	Network	A network in which service delivery to the customer is primarily over the physical communication links (e.g. copper or fiber potic cables). The end-user's connection into the network does not move.	EP3R TF-TDCA
Gateway	Network	A point of connection between two dissimilar networks (e.g. between a fixed and mobile network)	EP3R TF-TDCA
Incident	ASPR	Any circumstance or event having an actual adverse effect on security.	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union
Interconnection	Network	The connection between two similar networks (e.g. a link between to CSPs and ISPs as a means of passing traffic between them.	EP3R TF-TDCA
ISP	Network, Human	An Internet Service Provider - normally not providing fixed or	EP3R TF-TDCA

Term	Categorization	Definition	Source
		mobile voice services.	
Likelihood	ASPR	The chance of something happening.	EP3R TF-TDCA
Location	Environment	The physical presence of a node.	EP3R TF-TDCA
Mobile Network	Network	A network in which service delivery to the customer is primarly over virtual communication links (e.g. radio). The end-user's connection into the network does may move, and the network will maintain the connection.	EP3R TF-TDCA
Network	Network	A network is a system of interconnected nodes, each of which is able to deliver a function or service local to that node, but which may be a component in delivering services more widely.	EP3R TF-TDCA
Node	Network, Hardware	A node is a single point of connection. At a high level, nodes interconnect with one another to form a network.At a low level, nodes are used to connect customers into the network.	EP3R TF-TDCA
Protection	Security		EP3R TF-TDCA
Resilience	Network		ISO Guide 73
Risk	Security	The effect of uncertainity on objectives.	EP3R TF-TDCA
Telecommunication assistance	ASPR	the provision of telecommunication resources or other resources or support intended to facilitate the use of telecommunication resources.	The Tampere Convention
Telecommunication resources	Network, Hardware	personnel, equipment, materials, information, training, radio-frequency spectrum, network or	The Tampere Convention

Term	Categorization	Definition	Source
		transmission capacity or other resources necessary to telecommunications.	
Telecommunications	Network, Hardware	any transmission, emission, or reception of signs, signals, writing, images, sounds or intelligence of any nature, by wire, radio, optical fibre or other electromagnetic system.	Tampere Convention
Traffic	Network	The actual voice or data communication sent and received between two nodes.	EP3R TF-TDCA
Traffic shaping	Network	When traffic through packed based networks becomes slow, and latency increases, traffic shaping is the action of controlling the volume of packets sent into the network (sometimes referred as bandhwidth throttling)or the rate at which they are sent (rate limiting).	EP3R TF-TDCA
Vulnerability	Security	The intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.	EP3R TF-TDCA

3 Assets Categorisation Principles

3.1 Introduction

Since the beginnings of EP3R, the Assets Categorization Task Force has discussed several approaches on how to address the most important issues and which best practises to consider. During the teleconferences several methods have been discussed in order to create an initial risk mapping ontology in order to follow the path traced by existing literature[2] regarding CI. Existing experiences like the one in Finland[3] and UK[4] were cited as possible examples to refer to.

The initial idea was to focus on public networks and align the work with the Art 13a[5] content, which is the obligation for the Telecom Operators to report incidents. Therefore it was decided to proceed initially with definitions of Critical Infrastructure / Critical Information Infrastructure / European Critical Infrastructure.

Moreover the different business models that can be applied in the Telco sector (fixed/mobile/connectivity provider) were emphasised and also the consequent different definitions of criticality.

3.2 Initial Ontology

During the initial open teleconferences the task force decided to tackle the problem starting from the differences between Internet Exchanges points (IXs) and manufacturers methodologies: IXs are more focused on the physical and supply chain and the data/control plane repercussions, while Manufacturers will concentrate on the meta-classification of specific assets.

Moreover the different business models that can be applied in the Telco sector (fixed/mobile/connectivity provider) were emphasised and also the consequent different definitions of criticality.

In the course of the proceedings and discussions with the experts it was decided to use **primarily** the Mutual Aid for Resilient Infrastructure in Europe (MARIE) eight ingredients to align the output with the other task forces.

This effort helps to draw a red line between the different goals and have a more holistic approach.

In the presented table the effort of the TF are sketched in order to give the an overview of the possible different aspects that must be addressed.

The following ontology should therefore be viewed as a means of gaining a foothold in an extensive, dynamic subject rather than as a statement of universally accepted fact.

[2] JRC-IPSC, ''Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art'' http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf

[3] Ministry of Transport and Communications , ''Communications Market Act'' , Finland http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf

[4] Ofcom, The UK Communications Infrastructure Report, United Kingdom http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/broadband-speeds/infrastructure-report-2012/

[5] Official Journal of the European Union, DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Art 13a

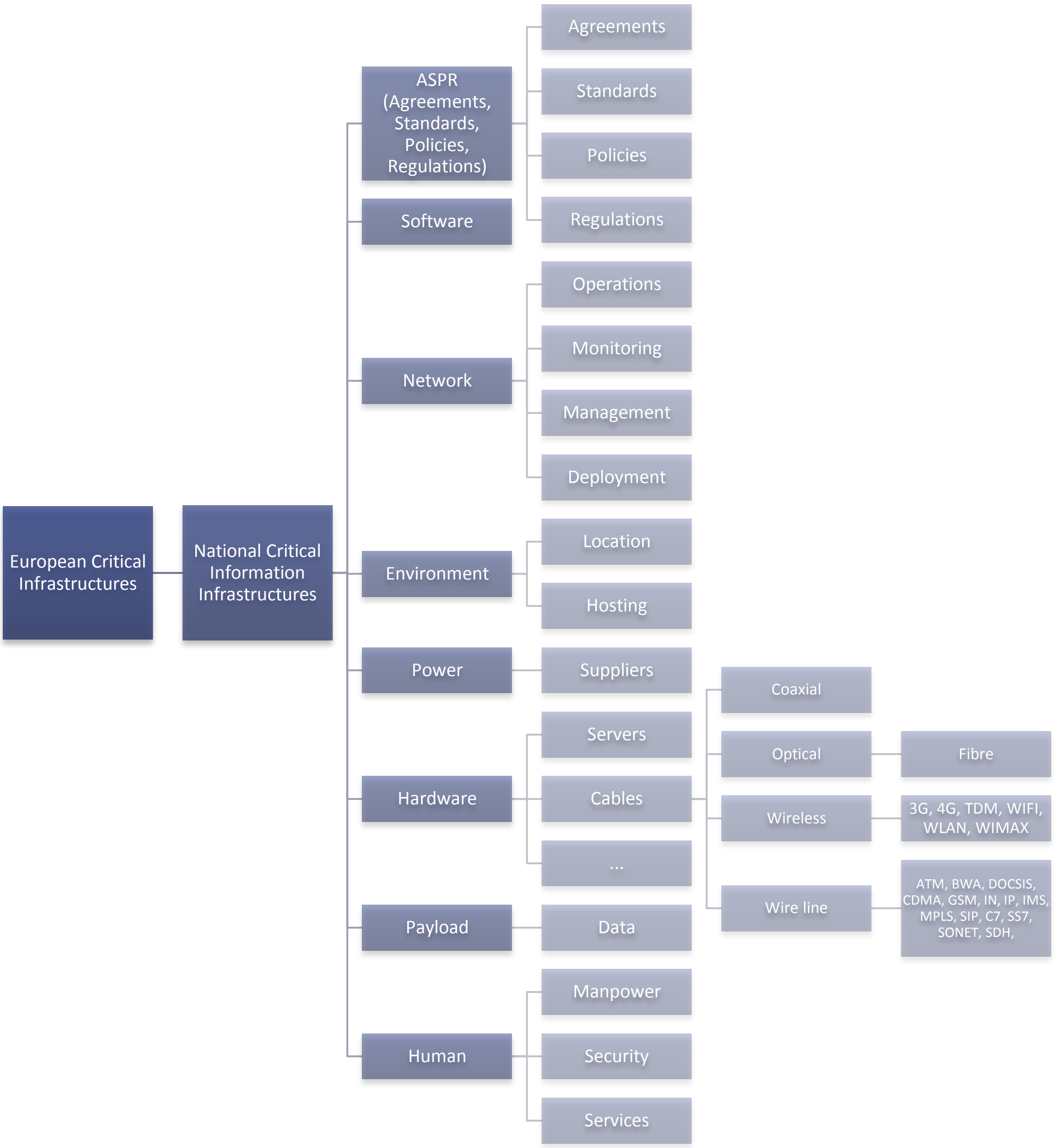
[5]http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

In the presented table the effort of the TF are sketched in order to give the an overview of the possible different aspects that must be addressed

The idea was to identify generic high level critical component that can be, once the ontology is released, tailored due to the specific business model and size of the organization.

Thus by using the Mutual Aid for Resilient Infrastructure In Europe (MARIE) eight ingredients this could be also connected with all the related literature and efforts and allow the interested parties to foster collaboration based on the same terminology baseline. For this reason also the terminology definition approach that follows makes use of the same categorisation.

The figure below shows a **<u>initial proposal</u>** classification of activities, assets and paves the way for Terminology categorisation and development as well.



4 Conclusion

This work was intended to be a very first step within EP3R that could be a foundation for later developments. The Task Forces ran for two months, just before the EP3R was subsumed to the NIS Platform.

This was actually the first attempt within the European Public Private Partnership for Resilience to reach convergence points in Participants' understanding, and allow to prevent many misunderstandings as they used to happen in the past.

The Task Force acknowledges that this iteration solely addresses the Telecom Sector, and suggests that it should be expanded to Sectors which depend on ICT, such as Health, Finance, Transports, Energy.

But also, such definitions might be also needed for the specifics of CyberSecurity areas: Botnets, Cyber Police, etc.

The process for each Sector should be similar, i.e. the identification of Terminology Sources relevant to the Sector considered, submitting a consolidated listing of terms to a panel of Experts, and their formal adoption of one definition per term.

Among the important uses of Terminology Definitions, the Task Force felt that Mutual Aid Assistance was probably the most crucial, since all participants in the Agreement need to speak the same language.

Some specifics of Mutual Aid Assistance should therefore be explored and a proper list of defined terms adopted.

In the Working Groups meeting of the NIS Platform, a few participants raised the need for starting a similar initiative. EP3R therefore hands over its initial conclusions so their starting point is already more advanced than for EP3R, 4 years ago.

Annex A: Glossary and Terminology Sources

- ISO/IEC 27000 series - Information technology — Security techniques — Information security management systems — Overview and vocabulary. http://standards.iso.org/ittf/PubliclyAvailableStandards/c056891_ISO_IEC_27000_2012(E).zip
- United Kingdom's Cabinet Office - Information Technology Infrastructure Library (ITIL) http://www.itil-officialsite.com/home/home.aspx
- ISACA - Control Objectives for Information and Related Technology (COBIT) http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx
- ITGI - IT Control Objectives for Sarbanes-Oxley 2nd Edition http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Sarbanes-Oxley-2nd-Edition.aspx
- MERIDIAN PROCESS resources http://meridianprocess.org
- NATO - AAP-6, NATO Glossary of terms and definitions http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf
- ENISA Risk Management - Glossary http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
- NIST - Glossary of Key Information Security Terms http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
- CIIP Handbook 2004 - section A1 Key Terms http://www.emsec.rub.de/media/crypto/attachments/files/2011/03/ciip_handbook_2004_ethz.pdf
- CRS Report for Congress - Critical Infrastructure and Key Assets: Definition and Identification http://www.fas.org/sgp/crs/RL32631.pdf
- European Commission - Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm
- Final Report to European Commission - Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf
- ITU - List of security-related terms, acronyms and definitions http://www.itu.int/ITU-T/studygroups/com17/def005.doc
- ITU - Technical and Procedural Measures for Cybersecurity http://www.itu.int/osg/csd/cybersecurity/gca/docs/global_strategic_report.pdf#page=76
- DHS - Infrastructure Data Taxonomy: Common Terminology for Describing Critical Infrastructure http://www.dhs.gov/infrastructure-taxonomy

Annex B: Assets Categorisation References

- X.805 – Security architecture for systems providing end-to-end communications http://www.itu.int/rec/T-REC-X.805-200310-I/en
- ISO/IEC 27011 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 http://webstore.iec.ch/preview/info_isoiec27011%7Bed1.0%7Den.pdf
- The European Perspective of Telecommunications as a Critical Infrastructure http://link.springer.com/content/pdf/10.1007%2F978-3-642-35764-0_1.pdf
- Critical infrastructure and key assets: definition and identification http://www.fas.org/sgp/crs/RL32631.pdf
- Rauscher, K.F., Krock, R.E. & Runyon, J.P., 2006. Eight ingredients of communications infrastructure: A systematic and comprehensive framework for enhancing network reliability and security A. P. Macwan, K. K. Mutha, & R. S. Hanmer, eds. *Bell Labs Technical Journal*, 11(3), pp.73–81.

Annex C: Full list of Adopted Terms, and their proposed Categorisation

Term	Categorization	Definition	Source	Link
Acceptable Risk	ASPR	The level of residual risk that has been determined to be a reasonable level of potential loss/disruption for a specific system.	NIST SP 800-16 Information Technology Security Training Requirements - Appendix A	http://csrc.nist.gov/publications/nistpubs/800-16/AppendixA-D.pdf
Access control	Security	Means to ensure that access to assets is authorized and restricted based on business and security requirements.	ISO/IEC 27000 2.1	
Accountability	Security	The property that ensures that the actions of an entity may be traced uniquely to the entity. (ISO/IEC PDTR 13335-1).This may cover non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.	ISO/IEC PDTR 13335-1 / ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Accountability	Security	The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions.	IETF Internet Engineering Task Force - RFC 2828	http://www.ietf.org/rfc/rfc2828.txt
Accountability	Security	Responsibility of an entity for its actions and decisions.	ISO/IEC 27000 2.2	
Asset	Hardware, Software	Anything that has value to the organization	ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=56891

Term	Categorization	Definition	Source	Link
Asset	Hardware, Software	Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission.	ISO/IEC PDTR 13335-1 / ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Asset	Hardware, Software	Anything that has value to the organization. NOTE There are many types of assets, including: a) information; b) software, such as a computer program; c) physical, such as computer; d) services; e) people, and their qualifications, skills, and experience; and f) intangibles, such as reputation and image.	ISO/IEC 27000 2.3	
Attack	Security	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.	ISO/IEC 27000 2.4	
Authentication	Security	The provision of assurance that a claimed characteristic of an entity is correct	ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=56891
Authenticity	Security	Property that an entity is what it claims to be Control (ISO/IEC 27000 2.10): means of managing risk, including policies, procedure, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature. NOTE Control is also used as a synonym for safeguard or countermeasure.	ISO/IEC 27000 2.6	
Availability	Security	Proprety of being accessible and usable upon demand by an authorized entity.	ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security	http://www.iso.org/iso/catalogue_detail?csnumber=56891

Term	Categorization	Definition	Source	Link
			management systems -- Overview and vocabulary	
Backbone	Network	The central core of a network aroudn which the remainder is built.	EP3R TF-TDCA	
Bot	Security	A malicious or potentially malicious bot (derived from the word "robot", hereafter simply referred to as a "bot") refers to a program that is installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a remote administrator, or "bot master". Bots are also known as "zombies". Such bots may have been installed surreptitiously, without the user's full understanding of what the bot will do once installed, unknowingly as part of another software installation, under false pretenses, and/or in a variety of other possible ways.	IETF Internet Engineering Task Force - RFC6561	http://www.ietf.org/rfc/rfc6561.txt
Botnet	Security	A "bot network", or "botnet", is defined as a concerted network of bots capable of acting on instructions generated remotely. The malicious activities are either focused on the information on the local machine or acting to provide services for remote machines. Bots are highly customizable so they can be programmed to do many things. The major malicious activities include but are not limited to identity theft, spam, spim (spam over Instant Messaging (IM)), spit (spam over Internet telephony), email address harvesting, distributed denial-of-service (DDoS) attacks, key-logging, fraudulent DNS pharming (redirection), hosting proxy services, fast flux hosting, hosting of illegal content, use in man-in-the-middle attacks, and click fraud.	IETF Internet Engineering Task Force - RFC6561	http://www.ietf.org/rfc/rfc6561.txt

Term	Categorization	Definition	Source	Link
Business Continuity	ASPR	The capability of the organization to continue delivery of products and services at acceptable predefined levels following a disruptive incident.	ISO 22301:2012 Societal security -- Business continuity management systems --- Requirements	http://www.iso.org/iso/catalogue_detail?csnumber=50038
Business continuity	ASPR	Processes and/or procedures for ensuring continued business operations.	ISO/IEC 27000 2.8	
BusinessImpact Analysis	ASPR	The process of analyzing activities and the effect that a business distruption might have upon them.	ISO 22301:2012 Societal security -- Business continuity management systems --- Requirements	http://www.iso.org/iso/catalogue_detail?csnumber=50038
Component	Hardware, Network	An item of electronic communications equipment that forms part or all of a node.	EP3R TF-TDCA	
Confidentiality	Security	Property that information is not made available or disclosed to unauthorized individuals, entities and processes.	ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=56891
Connection	Hardware, Network	A communication channel between two or more end-points (e.g. terminal, server etc.).	3GPP TR 21.905 V8.5.0 (2008-06) 3rd Generation Partnership Project;Technical Specification Group Services and System	http://www.quintillion.co.jp/3GPP/Specs/21905-850.pdf

Term	Categorization	Definition	Source	Link
			Aspects; Vocabulary for 3GPP Specifications	
Consequence	Security	Outcome of an event. There can be more than one consequence from one event. Consequences can range from positive to negative. Consequences can be expressed qualitatively or quantitatively	ISO/IEC Guide 73 / ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Contingency Plan	ASPR	A plan for emergency response, backup operations, and post-disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis.	IETF Internet Engineering Task Force - RFC 4949	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Control	ASPR		ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Control objective	ASPR	Statement describing what is to be achieved as a result of implementing controls.	ISO/IEC 27000 2.11	
Corrective action	ASPR	Action to eliminate the cause of a detected nonconformity or other undesirable situation.	ISO/IEC 27000 2.12	
Crisis	ASPR		ISO 22300 Societal security — Terminology	
Critical Information Infrastructure	Network	Information infrastructure (like networks, hardware, software, etc.) that is critical to the functioning of a nation or country, like IT that supports health- or energy-sectors.	EP3R TF-TDCA	

Term	Categorization	Definition	Source	Link
Critical Infrastructure	Hardware, Network	an asset, system or part thereof located in Member States that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions.	„COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection“	
CSP		Communication Service Provider - normally providing either a fixed or mobile voice and data service, which may include Internet access.	Technical Specification Group Services and System Aspects;	
Customer		An individual or organization paying for a service from a CISP or a ISP.	Vocabulary for 3GPP Specifications	
Data Availability	Security	The fact that data is accessible and services are operational.	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Data Confidentiality	Security	The protection of communications or stored data against interception and reading by unauthorized persons. (ENISA). The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO/IEC PDTR 13335-1)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Data Integrity	Security	The confirmation that data which has been sent, received, or stored are complete and unchanged. (ENISA) The property that data has not been altered or destroyed in an unauthorized manner. (ISO/IEC PDTR 13335-1)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Definition of Scope	Security	Process for the establishment of global parameters for the performance of Risk Management within an organization. Within the definition of scope for Risk Management internal and external factors have to be taken into account. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Disaster	ASPR	means a serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as the result of complex, long-term processes.	The Tampere Convention	http://www.itu.int/ITU-D/emergencytelecoms/Tampere_convention.pdf
Disaster	ASPR		ISO 22300 Societal security — Terminology	
Disaster mitigation	ASPR	measures designed to prevent, predict, prepare for, respond to, monitor and/or mitigate the impact of, disaster 12. Relief operations means those activities designed to reduce loss of life, human suffering and damage to property and/or the environment caused by a disaster.	The Tampere Convention	http://www.itu.int/ITU-D/emergencytelecoms/Tampere_convention.pdf
Disaster Recovery	ASPR	A coordinated activity to enable the recovery of telecom/IT/business systems to a disruption.	ETSI TR 102 445 V1.1.1 (2006-10)3 Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness	http://www.etsi.org/deliver/etsi_tr/102400_102499/102445/01.01.01_60/tr_102445v010101p.pdf
Disaster Recovery	ASPR	The process of restoring a system to full operation after an interruption in service, including equipment repair / replacement, file recovery / restoration. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Diversity	Network	The ability to use,select or switch between different circuits to avoid congestion and network failure.	ETSI TR 102 445 V1.1.1 (2006-10)3 Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness	http://www.etsi.org/deliver/etsi_tr/102400_102499/102445/01.01.01_60/tr_102445v010101p.pdf
Effectiveness	ASPR	Extent to which planned activities are realized and planned results achieved [ISO 9000:2005]	ISO/IEC 27000 2.11	
Efficiency	ASPR	Relationship between the results achieved and how well the resources have been used.	(ISO/IEC 27000 2.14	
Event	Security	Occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Event	Security	Occurrence of a particular set of circumstances [ISO/IEC Guide 73:2002].	ISO/IEC 27000 2.15	
Evidence	Security	Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. Evidence does not necessarily prove truth or existence of something but contributes to establish proof. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Exposure	Security	The potential loss to an area due to the occurrence of an adverse event. (ISACA) Generally, in the Risk Management process a risk does not always represent a loss or a negative consequence but can also be an opportunity or a result of a positive event. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Fault tolerance	Hardware, Software	Devices that are designed and built to correctly operate even in the presence of a software error or failed components.	ETSI TR 102 445 V1.1.1 (2006-10)3 Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness	http://www.etsi.org/deliver/etsi_tr/102400_102499/102445/01.01.01_60/tr_102445v010101p.pdf
Fixed network	Network	A network in which service delivery to the customer is primarily over the physical communication links (e.g. copper or fiber potic cables). The end-user's connection into the network does not move.	EP3R TF-TDCA	
Gap Analysis	ASPR	A comparison that identifies the difference between the actual and the expected / specified system status.	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Gateway	Network	A point of connection between two dissimilar networks (e.g. between a fixed and mobile network)	EP3R TF-TDCA	
Guideline	ASPR	Recommendation of what is expected to be done to achieve an objective.	ISO/IEC 27000 2.16	
Impact	Security	The result of an unwanted incident . (ISO/IEC PDTR 13335-1)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Impact	Security	Adverse change to the level of business objectives achieved.	ISO/IEC 27000 2.17	

Term	Categorization	Definition	Source	Link
Impact Analysis	Security	The identification of critical business processes, and the potential damage or loss that may be caused to the organization resulting from a disruption to those processes. Business impact analysis identifies: the form the loss or damage will take; how that degree of damage or loss is likely to escalate with time following an incident; the minimum staffing, facilities and services needed to enable business processes to continue to operate at a minimum acceptable level; the time for full recovery of the business processes (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Impact or consequence	Security	The outcome of an event affecting objectives.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
incident	ASPR	any circumstance or event having an actual adverse effect on security.	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union	http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666
Incident	ASPR	An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Information asset	Hardware, Software, Security, Network	Knowledge or data that has value to the organization.	ISO/IEC 27000 2.18	
Information security	Security	Preservation of confidentiality , integrity and availability of information. NOTE In addition, other properties, such as authenticity , accountability , non-repudiation), and reliability can also be involved.	ISO/IEC 27000 2.19	
Information security event	Security	Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.	ISO/IEC 27000 2.20	
Information security incident	Security	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.	ISO/IEC 27000 2.21	
information security incident management	Security	Processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.	ISO/IEC 27000 2.22	
Information security management system ISMS	Security	Part of the overall management system), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.	ISO/IEC 27000 2.23	
Information security risk	Security	Potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization.	ISO/IEC 27000 2.24	
Integrity	Security	Property of protecting the accuracy and completeness of assets.	ISO/IEC 27000:2012 Information technology -- Security techniques --	http://www.iso.org/iso/catalogue_detail?csnumber=56891

Term	Categorization	Definition	Source	Link
			Information security management systems -- Overview and vocabulary	
Interconnection	Network	The connection between two similar networks (e.g. a link between to CSPs and ISPs as a means of passing traffic between them.	EP3R TF-TDCA	
Interested Party	Human	Person or group having an interest in the performance or success of an organization's mission or objectives. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Internet	Network	The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB (RFC 2026) and (b) the name and address spaces managed by the ICANN.	IETF Internet Engineering Task Force - RFC 4949	http://tools.ietf.org/html/rfc4949
ISP	Network, Human	An Internet Service Provider - normally not providing fixed or mobile voice services.	EP3R TF-TDCA	
Likelihood	ASPR	The chance of something happening.	EP3R TF-TDCA	
Location	Environment	The physical presence of a node.	EP3R TF-TDCA	
Management system	Software	Framework of policies, procedures, guidelines and associated resources to achieve the objectives of the organization	ISO/IEC 27000 2.26	
Mitigation	ASPR	Limitation of any negative consequence of a particular event . (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Mobile Network	Network	A network in which service delivery to the customer is primarly over virtual communication links (e.g. radio). The end-user's connection into the network does may move, and the network will maintain the connection.	EP3R TF-TDCA	
Monitor and Review	Network, Human, Software, Hardware, ASPR	A process for measuring the efficiency and effectiveness of the organization's Risk Management processes is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated. This process also implements control activities including re-evaluation of the scope and compliance with decisions. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Mutual Aid Agreement	ASPR		ISO 22300 Societal security — Terminology	
Network	Network	A network is a system of interconnected nodes, each of which is able to deliver a function or service local to that node, but which may be a component in delivering services more widely.	EP3R TF-TDCA	
Node	Network, Hardware	A node is a single point of connection. At a high level, nodes interconnect with one another to form a network.At a low level, nodes are used to connect customers into the network.	EP3R TF-TDCA	
Non Repudiation	Security	The ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.	ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=56891
Patnership	ASPR		ISO 22300 Societal	

Term	Categorization	Definition	Source	Link
			security — Terminology	
Policy	ASPR	Overall intention and direction as formally expressed by management.	ISO/IEC 27000 2.28	
Preventive action	ASPR	Action to eliminate the cause of a potential nonconformity or other undesirable potential situation. [ISO 9000:2005]	ISO/IEC 27000 2.29	
Priority	Network	Sequence in which an incident or problem needs to be resolved, based on impact and urgency. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Probability	Security	The measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainity.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Probability	Security	Extent to which an event is likely to occur.(ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Procedure	ASPR	A written description of a course of action to be taken to perform a given task. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Procedure	ASPR		ISO/IEC 27000 2.29	
Process	ASPR	An organized set of activities which uses resources to transform inputs to outputs. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Process	ASPR	Set of interrelated or interacting activities which transforms inputs into outputs [ISO 9000:2005]	ISO/IEC 27000 2.31	
Process Owner	ASPR	An individual held accountable and responsible for the workings and improvement of one of the organization's defined processes and its related sub-processes. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Protection	Security		EP3R TF-TDCA	
Record	Payload	Document stating results achieved or providing evidence of activities performed. [ISO 9000:2005]	ISO/IEC 27000 2.32	
Redundancy	Network	The inclusion of extra components, which are not strictly necessary to functioning, in case of failure in other components.	The Oxford English Dictionary	http://www.oed.com/
Reliability	Network, Hardware, Software	Property of consistent intended behaviour and results.	ISO/IEC 27000 2.33	
Residual Risk	Security	Risk emaining after risk treatment. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Resilience	Network		ISO Guide 73	
Resilience	Network	The resilience of an organization to resist to being affected by disruption.	ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication	http://www.iso.org/iso/catalogue_detail?csnumber=44374

Term	Categorization	Definition	Source	Link
			technology readiness for business continuity	
Risk	Security	The effect of uncertainity on objectives.	EP3R TF-TDCA	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk	Security	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. (ISO/IEC PDTR 13335-1)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk	Security	Combination of the probability of an event and its consequence. [ISO/IEC Guide 73:2002]	ISO/IEC 27000 2.34	
Risk acceptance	Security	Informed decision of taking a particular risk .	Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk Acceptance	Security	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. (ISO/IEC PDTR 13335-1) Risk acceptance depends on risk criteria defined within the process Definition of Scope. (Definition adopted from ISO/IEC Guide 73 with some modification by ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk acceptance	Security	Risk acceptance (ISO/IEC 27000 2.35): decision to accept a risk (2.34) [ISO/IEC Guide]	ISO/IEC 27000 2.35	

Term	Categorization	Definition	Source	Link
Risk Analysis	Security	Systematic use of information to identify sources and to estimate the risk. Risk analysis provides a basis for risk evaluation , risk treatment and risk acceptance. ISO/IEC Guide 73	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk analysis	Security	systematic use of information to identify sources and to estimate risk [ISO/IEC Guide 73:2002] NOTE Risk analysis provides a basis for risk evaluation , risk treatment and risk acceptance .	ISO/IEC 27000 2.36	
Risk assessment	Security	The overall process of risk identification, risk analysis and risk evaluation.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk Assessment	Security	A scientific and technologically based process consisting of three steps, risk identification, risk analysis and risk evaluation . (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk assessment	Security	Overall process of risk analysis and risk evaluation [ISO/IEC Guide 73:2002]	ISO/IEC 27000 2.37	
Risk avoidance	Security	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk Avoidance	Security	Decision not to become involved in, or action to withdraw from, a risk situation. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Risk Communication	ASPR	A process to exchange or share information about risk between the decision-maker and other stakeholders. The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk communication	ASPR	Exchange or sharing of information about risk between the decision-maker and other stakeholders. [ISO/IEC Guide 73:2002]	ISO/IEC 27000 2.38	
Risk Control	Security	Actions implementing risk management decisions. Risk control may involve monitoring, re-evaluation, and compliance with decisions. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	
Risk Criteria	Security	Terms of reference by which the significance or risk is assessed. Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic aspects, the concerns of stakeholders , priorities and other inputs to the assessment. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk criteria	Security	Terms of reference by which the significance of risk is assessed [ISO/IEC Guide 73:2002]	ISO/IEC 27000 2.39	
Risk Estimation	Security	Process of comparing the estimated risk against given risk criteria to determine the significance of risk. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk estimation	Security	Activity to assign values to the probability and consequences of a risk.[ISO/IEC Guide 73:2002]	ISO/IEC 27000 2.40	
Risk Evaluation	Security	Process of comparing the estimated risk against given risk criteria to determine the significance of risk. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Risk evaluation	Security	Process of comparing the estimated risk against given risk criteria o determine the significance of the risk. [ISO/IEC Guide 73:2002]	ISO/IEC 27000 2.41	
Risk Financing	ASPR, Security	Provision of funds to meet the cost of implementing risk treatment and related costs. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk Identification	Security	Process to find, list and characterize elements of risk]. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk Management	ASPR, Security	The process , distinct from risk assessment , of weighing policy alternatives in consultation with interested parties , considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk management	Security	Coordinated activities to direct and control an organization with regard to risk [ISO/IEC Guide 73:2002] NOTE Risk management generally includes risk assessment , risk treatment), risk acceptance , risk communication (2.38), risk monitoring and risk review.	ISO/IEC 27000 2.42	
Risk modification	Security	A process to modify risk	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk Optimization	Security	Process [G.24], related to a risk [G.27] to minimize the negative and to maximize the positive consequences [G.4] and their respective probabilities [G.22]. Risk optimization depends upon risk criteria [G.34], including costs and legal requirements. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Risk Perception	Security	Way in which a stakeholder [G.50] views a risk [G.27], based on a set of values or concerns. Risk perception depends on the stakeholder's needs, issues and knowledge. Risk perception can differ from objective data. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk reduction	Security	A process to modify risk.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk Reduction	Security	Actions taken to lessen the probability , negative consequences or both, associated with a risk . (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk Retention	Security	Acceptance of the burden of loss, or benefit of gain, from a particular risk Risk retention includes the acceptance of risks that have not been identified. Risk retention does not include treatments involving insurance, or transfer by other means. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk sharing	Security	Form of risk treatment involving the agreed distribution of risk with other parties.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk termination	Security	Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk tolerance	Security	Informed decision to take a particul risk.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Risk transfer	ASPR	Form of risk treatment involving the agreed distribution of risk with other parties.	ISO Guide 73:2009 Risk management –	http://www.iso.org/iso/catalogue_detail?csnumber=44651

Term	Categorization	Definition	Source	Link
			Vocabulary	
Risk Transfer	ASPR	Sharing with another party the burden of loss or benefit of gain, for a risk. Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk. Risk transfer can be carried out through insurance or other agreements. Risk transfer can create new risks or modify existing risk. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk Treatment	ASPR, Security	Process of selection and implementation of measures to modify risk.Risk treatment measures can include avoiding, optimizing, transferring or retaining risk (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Risk treatment	ASPR, Security	Process of selection and implementation of measures to modify risk.[ISO/IEC Guide 73:2002]	ISO/IEC 27000 2.43	
Safeguards	Security	Practices, procedures or mechanisms that reduce risk. The term 'safeguard' is normally considered to be synonymous with the term 'control'. (ISO/IEC PDTR 13335-1)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Security	Security	All aspects related to defining, achieving, and maintaining data confidentiality, integrity, availability, accountability, authenticity, and reliability. A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. (ISO/IEC WD 15443-1)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Separacy	Network	A more reliable means of ensuring that specified circuits are not rerouted over the same cables, equipment or transmission systems and also there are no common physical sites within the circuits rerouting.	ETSI TR 102 445 V1.1.1 (2006-10)3 Emergency Communications (EMTEL); Overview of Emergency Communications	http://www.etsi.org/deliver/etsi_tr/102400_102499/102445/01.01.01_60/tr_102445v010101p.pdf

Term	Categorization	Definition	Source	Link
			Network Resilience and Preparedness	
Service	Software	A component of a portfolio of choices offered by service providers to a user, functionality offered to a user.	3GPP TR 21.905 V8.5.0 (2008-06) 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications	http://www.quintillion.co.jp/3GPP/Specs/21905-850.pdf
Signalling	Network	The exchange of information specifically concerned with the establishment and control of connections, and with management, in the telecommunications network.	3GPP TR 21.905 V8.5.0 (2008-06) 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications	http://www.quintillion.co.jp/3GPP/Specs/21905-850.pdf
Source	Security	Item or activity having a potential for a consequence. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Source Identification	Security	Process to find, list and characterize sources. (ISO/IEC Guide 73) specified way to carry out an activity or a process.[ISO 9000:2005]	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

Term	Categorization	Definition	Source	Link
Stakeholder	ASPR	Any individual, group or organization that can affect, be affected by, or perceive itself to be affected by, a risk. (ISO/IEC Guide 73)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Statement of applicability	Security	Documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS (2.23)	ISO/IEC 27000 2.34	
Telecommunication assistance	ASPR	the provision of telecommunication resources or other resources or support intended to facilitate the use of telecommunication resources.	The Tampere Convention	
Telecommunication resources	Network, Hardware	personnel, equipment, materials, information, training, radio-frequency spectrum, network or transmission capacity or other resources necessary to telecommunications.	The Tampere Convention	
Telecommunications	Network, Hardware	any transmission, emission, or reception of signs, signals, writing, images, sounds or intelligence of any nature, by wire, radio, optical fibre or other electromagnetic system.	Tampere Convention	
Threat	Security	Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. (ENISA)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Threat	Security	Potential cause of an unwanted incident, which may result in harm to a system or organization.	ISO/IEC 27000 2.45	
Threat or hazard	Security	A source of potential harm, an element, which alone or in combination has the intrinsic potential to give rise to risk.	ISO Guide 73:2009 Risk management -- Vocabulary	http://www.iso.org/iso/catalogue_detail?csnumber=44651
Traffic	Network	The actual voice or data communication sent and received between two nodes.	EP3R TF-TDCA	

Term	Categorization	Definition	Source	Link
Traffic shaping	Network	When traffic through packed based networks becomes slow, and latency increases, traffic shaping is the action of controlling the volume of packets sent into the network (sometimes referred as bandhwidth throttling)or the rate at which they are sent (rate limiting).	EP3R TF-TDCA	
Vulnerability	Security	The intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.	EP3R TF-TDCA	
Vulnerability	Security		ISO 22300 Societal security — Terminology	
Vulnerability	Security	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved. (ITSEC)	ENISA Risk Assessment Glossary	http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
Vulnerability	Security	Weakness of an asset or control that can be exploited by a threat.	ISO/IEC 27000 2.46	

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu