A list of ENISA's 2015 work programme publications

The following table presents links to the ENISA Work Programme 2015 deliverable

	Deliverable	Status
SO1 – To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network & Information Security (NIS)		
WPK 1.1 – NIS Threats Analysis		
D1	Annual Threat Analysis/Landscape Report (Q4/2015)	"ETL 2015" https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015
D2	Risk Assessment on two emerging technology/ application areas (Q4/2015)	1) "Big data Threat landscape" https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/bigdata-threat-landscape 2) "SDN Threat landscape" https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/sdn-threat-landscape
WPK 1.2 – Improving the Protection of Critical Information Infrastructures		
D1	Stock Taking, Analysis and Recommendations on the protection of CIIs (Q3/2015)	1) "CIIP Governance in the European Union Member States" *[restricted report]* 2) "Stocktaking, Analysis and Recommendations on the Protection of CIIs" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis
D2	Methodology for the identification of Critical Communication Networks, Links, and Components (Q4/2015)	"Methodology for the identification of Critical Communication Networks, Links, and Components" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/communication-network-interdependencies-in-smart-grids/
D3	Analysis of ICS-SCADA Cyber Security of Devices in Critical Sectors (Q4/2015)	"Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/maturity-levels
D4	Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector (Q4/2015)	"Secure Use of Cloud Computing in the Finance Sector. Good practices and recommendations" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/cloud-in-finance
D5	Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services (Q4/2015)	1) "Security and Resilience in eHealth. Security Challenges and Risks" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth_sec/security-and-resilience-in-ehealth-infrastructures-and-services 2) "Security and Resilience in eHealth. Annex A: Countries' Report" *[restricted report]*
WPK 1.3 – Securing emerging Technologies and Services		
D1	Good Practices and Recommendations on the Security and Resilience of Intelligent transportation systems (Q4/2015)	1) "Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/good-practices-recommendations 2) "Cyber security for Smart Cities. An architecture model for public transport" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/smart-cities-architecture-model
D2	Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4/2015)	"Big Data Security. Good Practices and Recommendations on the Security of Big Data Systems" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/big-data-security/
D3	Good Practices and Recommendations on the Security and Resilience of Smart Home Environments (Q4/2015)	"Security and Resilience of Smart Home Environments. Good practices and recommendations" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices
WPK 1.4 – Short- and mid-term sharing of information regarding issues in NIS		
D1	Establish necessary procedures, workflows, tools, etc. to enable ENISA to carry out the Info Notes service (Q2/2015)	Internal procedures are well defined and applied in practice
D2	Info Notes on a specific NIS issue (ongoing service with pilot from Q2/2014; conclusions on first year of activity in Q4/2015)	[Available upon request]

SO2 – To assist the Member States and the Commission in enhancing capacity building throughout the EU		
WPK 2.1. – Assist in public sector capacity building		
D1	Support and Advise Member States on the establishment and evaluation of National Cyber Security Strategies (NCSS) (Q4/2015)	workshop done in September 2015 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2015/cyber-security-strategies-critical-information-infrastructures-protection-and-ics-scada-event
D2	Assistance in National CERTS training and education (ongoing)	Article 14 requests
D3	Maintaining CERT good practice and training library (Q4/2015)	1) "Mobile Threats Incident Handling. Handbook, Document for teachers" https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/mobile-threats-incident-handling-part-ii-handbook-document-for-teachers 2) "Introduction to advanced artefact analysis. Handbook, Document for teachers" https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/introduction-to-advanced-artefact-analysis.pdf 3) "Advanced dynamic analysis. HANDBOOK, DOCUMENT FOR TEACHERS" https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/dynamic-analysis-of-artefacts-handbook.pdf 4) "Advanced static analysis. Handbook, Document for teachers" https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/static-analysis-of-artefacts-handbook.pdf
D4	Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap (Q4/2015)	"Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations" https://www.enisa.europa.eu/activities/cert/support/vulnerability-disclosure/
D5	Impact evaluation on the usefulness of the ENISA guidelines on capacity building. (Q4/2015)	"Leading the way. ENISA's CSIRT-related capacity building activities. Impact Analysis – Update 2015" https://www.enisa.europa.eu/activities/cert/other-work/leading-the-way-enisa-s-impact-in-operational-security
WPK 2.2. Assist in private sector capacity building		
D1	ENISA report "Status of Privacy and Network and Information Security course curricula in MSs" (Q4 2015)	"Status of privacy and NIS course curricula in Member States" https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/status-of-privacy-and-nis-course-curricula-in-eu-member-states
D2	Further development of ENISA application "NIS self-assessment" (dissemination material, Q4 2015)	"Cyber Security Month NIS quiz" (available on https://cybersecuritymonth.eu/)
D3	On-request support for MS decision making (Q4/2015)	Article 14 requests.
WPK 2.3. – Assist in improving awareness of the general public		
D1	Provide guidance and support for European Cyber-Security Month (dissemination material, Q4 2015)	1) Website: https://cybersecuritymonth.eu/ 2) "The European Cyber Security Month 2015. Deployment report" https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2015/ecsm15-deployment-report
D2	Basic Cyber hygiene: guidelines for recognizing and using trustworthy security and privacy products for the general public (Q4/2015)	"Online privacy tools for the general public. Towards a methodology for the evaluation of PETs for internet & mobile users." https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/basic-cyber-hygiene
SO3 – To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security		
WPK 3.1. – Provide information and advice to support policy development		
D1	Analysis of standards related to eID and/or TSPs (Report, Q4 2015)	"Analysis of standards related to Trust Service Providers. Mapping of requirements of eIDAS to existing standards" https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/tsp_standards_2015
D2	Report analysing the terminology and definitions used by eIDAS and (including recommended technological means used by TSPs) (Report, Q4 2015	"Qualified Website Authentication Certificates. Promoting consumer trust in the website authentication market" https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/qualified-website-authentication-certificates/
WPK 3.2. – Assist EU MS and Commission in the implementation of EU NIS regulations		
D1	Analysis of Annual 2014 Incident Reports (report) (Q3/2015)	"Annual Incident Reports 2014. Analysis of Article 13a annual incident reports" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2014
D2	Recommendations on addressing root causes of specific incidents (report) (Q3/2015)	1) "Guideline on Threats and Assets. Technical guidance on threats and assets in Article 13a" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-threats-and-assets 2) "Security incidents indicators - measuring the impact of incidents affecting electronic communications" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/studies/security-incidents-indicators

D3	Guidelines on Minimum Security Measures for Trusted Service Providers (workshops, report) (Q4/2015)	[The deliverable has been postponed. The Amending Work programme 2015.]
D4	Impact assessment on the effectiveness of incident reporting schemes (e.g. Art13a and Art 4) (Q4/2015)	“Impact evaluation on the implementation of Article 13a incident reporting scheme within EU” https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/studies/impact-evaluation-article13a
D5	Guidelines on Incident Reporting Scheme for Article 15 (report, Q4 2015)	“Proposal for Article 19 Incident reporting. Proposal for an Incident reporting framework for eIDAS Article 19” https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/article19/technical-guideline-for-incident-reporting
WPK 3.3. – Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation		
D1	Readiness analysis for the adoption and evolution of privacy enhancing technologies (Q4 2015)	“Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. Methodology, Pilot Assessment, and Continuity Plan” https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets
D2	Building blocks for PETs update (Q4 2015)	[restricted report]
D3	Annual Privacy Forum 2015, APF’2015 (Q4 2015)	Organised on 7- 8 October 2015, in Luxembourg http://privacyforum.eu
D4	State-of-the-art analysis of data protection in big data architectures (Q4 2015)	“Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics” https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection
D5	2015 edition of the annual report on ‘Indicative list of appropriate cryptographic protection measures’ (Q4 2015)	“2015 Algorithms, Key Sizes and Parameters Report” *[restricted report]*
WPK 3.4 – R&D, Innovation & Standardisation		
D1	Good Practice Guide for aligning Policy, Industry and Research (Q4/2015)	“Governance framework of the European standardisation. Aligning Policy, Industry and Research” https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/policy-industry-research
D2	Standardisation Gaps in Cyber Security (Q4/2015)	“Definition of Cybersecurity. Gaps and overlaps in standardisation” https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/standardisation-gaps-in-cybersecurity
D3	Guide to standardisation for the SME Community (Q4/2015)	1) “Information security and privacy standards for SMEs. Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises” https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/standardisation-for-smes 2) “Cloud Security guide for SME’s. computing security risks and opportunities for SMEs” https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes
SO4 – To enhance cooperation both between the Member States of the EU and between related NIS communities		
WPK 4.1. – Support for EU cooperation initiatives amongst NIS –related communities in the context of the EU CSS		
D1	Develop and provide guidance based on best practice for cooperation between key stakeholder communities (Trust building for and reaching out to new communities) (CERTs, CIIP community, Law Enforcement, Financial Services; Data Protection, etc.) (Q4/2015)	1) “Information sharing and common taxonomies between CSIRTs and Law Enforcement” https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement 2) “CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs” https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/csirt-capabilities/ 3) “Inventory of CERT activities in Europe” https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe
D2	Identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues (Q4/2015)	“Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches” https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing
WPK 4.2. – European cyber crisis cooperation through exercises		
D1	Evaluation Analysis and Actions from CE2014 (restricted report, Q2 2015)	“ENISA CE2014 After Action Report” https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/ce2014-after-action-report
D2	Pan European Cyber Exercises Plan: CE2016 (restricted report, Q4 2015)	*[restricted report]*
D3	EU-US Cybersecurity Exercise after-action Report[2] (public/restricted report, Q2 2015)	*[restricted report]*
D4	Evaluation and recommendations for improved communication procedures between EU MSs (public/restricted report, Q4 2015)	“Common practices of EU-level crisis management and applicability to cyber crises” https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/eu-level-crisis-man/