Study on Cybersecurity in the energy sector of the Energy Community

Project methodology

Blueprint Energy Solutions GmbH

Presenter:
Peter Grasselli - CISA, CISSP

Vienna, 11.04.2019.

Team lead of IT security team that supports the implementation and operation of REMIT Information Security Management System for EU Agency for Coordination of Energy Regulators (ACER) on the side of contractor. Team tasks include development and implementation support for REMIT information security framework, information security awareness trainings as well as assessments of ARIS security.

Responsible for methodology development and quality assurance for project "IT security remediation". Project was ordered by one of the leading pharmaceutical companies in the world; more than hundred sites worldwide were assessed during the project.

Security consultant for key evidences (sensitive data) - Ministry of Justice (Slovenia)

CISA Certified Information Systems Auditor® An ISACA® Certification

CISSP® Certified Information Systems Security Professional

More than 30 years of experience in IT

- IT Audit and IT security consultant
- CIO
- IT architect, system administrator, developer

Industries:

- Government and public administration
- Utilities, Energy
- Pharmaceutical
- Financial
- Gaming

AITSA
Advanced Information Technology Security Assessment
peter.grasselli@aitsa-is.com

BLUEPRINT energy SOLUTIONS

Agenda

1. Introduction
2. Overview of study methodology
3. Presentation of questionnaires
4. Next steps

- What are foreseen study deliverables?
- Which information is needed to provide deliverables?
- How we plan to obtain this information?
- Why is important that the information is relevant and accurate?

Introduction - Deliverables

Main objective is to assess and develop proposals for improving the energy-specific cybersecurity capabilities in the EnC at national and regional/pan-European levels

- Overview of regulatory framework
- Overview of cyber threats and risks
- Overview of gaps
- Propose measures to implement minimum common cybersecurity framework
- Make an impact assessment of implementation of proposed measures
- Develop a roadmap for the implementation

Introduction - Information

To provide overview, assess gaps and propose measures as well as prepare implementation roadmap the following information is needed

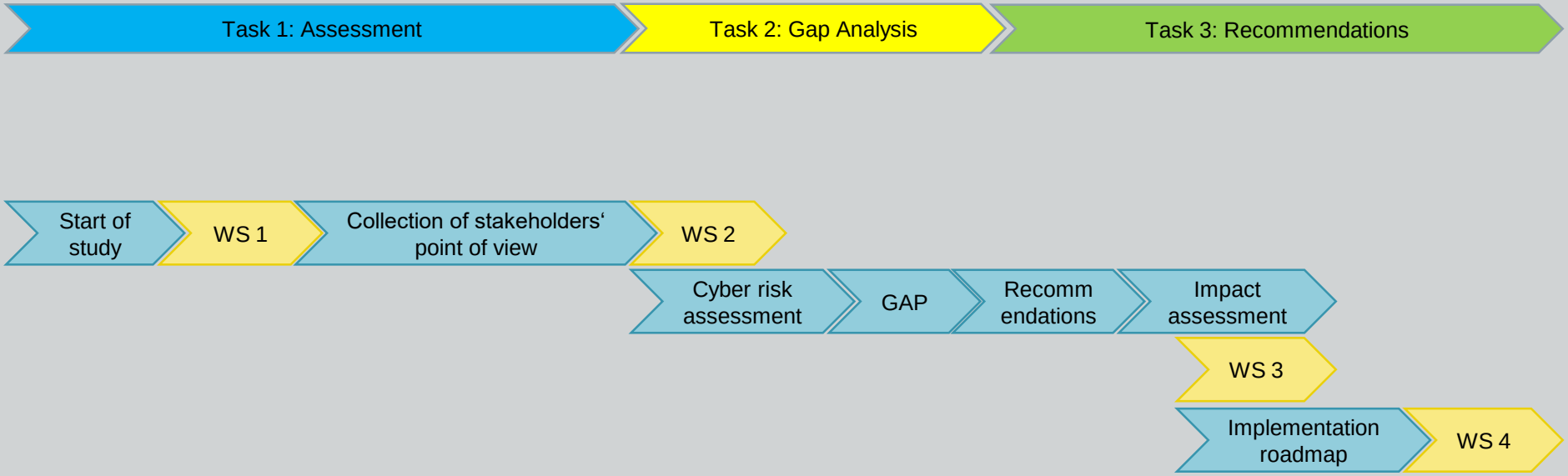
- Legal framework
- Standards
- Institutional framework
- Cross-border initiatives
- Education and training programmes
- Cyber threats and risks

Introduction – Information quality

In order to provide valid and viable results key methodology underlying principles related to information gathering and validation are

- Interaction with stakeholders
  - Workshops, questionnaires, on site visits
- Corraboration of information
  - Desktop research, questionnaires, interviews -> 360^0 view
- Discussion/verification of results with stakeholders
  - Workshops
- Local experts

Methodology - Overview



Remark: Length of arrows does not represent activity duration

Methodology – key tasks

- Information gathering
  - *Awareness raising*
  - Segmented by stakeholders (Q1, Q2, Q3)
  - Interactive

- GAP assessment (that may create obstacles)
  - EU rules and best practices
  - Current state of Cybersecurity in EnC Contracting Parties

- Propose minimum common framework
  - Measures
  - Institutions (necessary to implement measures)
  - Assess impact of proposed measures
  - Implementation roadmap

Methodology – Information gathering

- Budapest convention implementation
- ECI and NIS implementation related information
  - Cybersecurity strategy
  - EnC Critical infrastructure identification/criteria
  - Essential services
  - Incident reporting (contact points)
- Standards
- Cyber security cooperation, projects and assistance
- Awareness, education and training programmes and cooperation

WS 1
Q1 – state level
Q2 - NRA
Q3 – TSOs
DSOs
Prod./Gen.

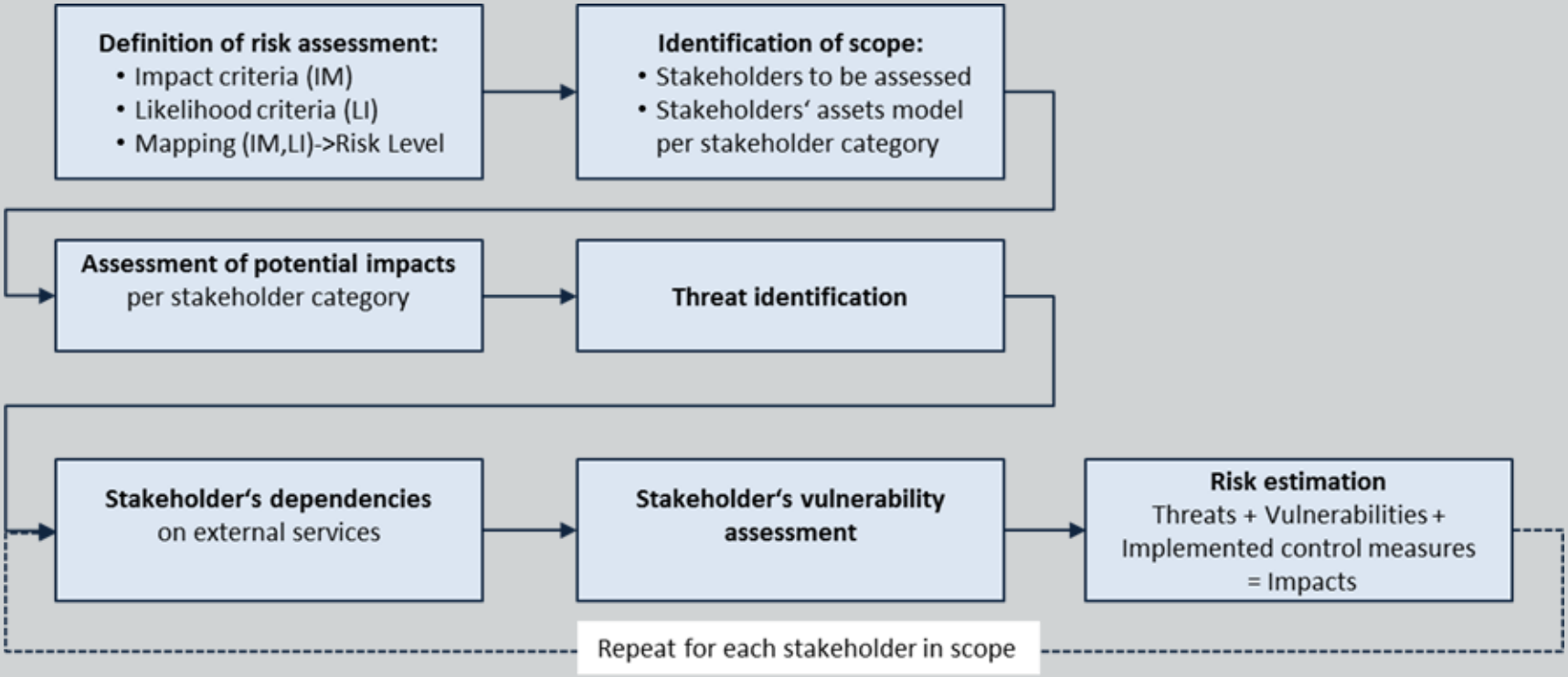
- Cyber risk assessment

WS 2, On-site visits

- Impact assessment of proposed measures

WS 3, *Q4?*

Methodology – Risk assessment



Methodology – supporting team

- Single point of contact (for each state)

- Questionnaire development and analysis team
- Risk assessment team
- Local experts

- Recommendations team

- On-site core team visits planned for May and June

Q1 – Competent Cybersecurity Authorities Questionnaire

1. Definitions and Abbreviations
2. Introduction
3. General information
4. National Cybersecurity strategy and action plan (4)
5. National legislation (10)
6. National standardisation and accreditation schemes (3)
7. Cyber security organisational structures (4)
8. Risk assessment (4)
9. Cyber security cooperation, projects and assistance (6)
10. Awareness programmes, education and cooperation (6)

Q1 – Sample questions

4.1 Is a national Strategy related to the security of network and information systems adopted in your country?

4.2 Is there a nation-wide action plan in place for the implementation of the Strategy?

4.3 Are cybersecurity risks related to critical infrastructure in the energy sector addressed in the Strategy?

4.4 Is there a designated entity which serves as the national single point of contact on the security of network and information systems?

Q1 - Recipients

Intended recipient – institutions responsible for cybersecurity strategy implementation/monitoring

CP	CS strategy	Recipient
Albania	Policy Paper on Cyber Security 2015 – 2017	National Authority for Electronic Certification and Cyber Security (AKCESK)
BiH	Action Plan drafted by the WG on the national level is still pending adoption	For the Federation BiH – Ministry of Security of Bosnia and Herzegovina Republika Srpska - Agency for Information Society of the Republic of Srpska (AIDRS), The Department of Information Security (OIB)
North Macedonia	The National Strategy for Cyber Security 2018-2022	National Council for Cyber Security, Ministry of Information Society and Administration responsible for identification of critical information infrastructure
Georgia	Cybersecurity Strategy of Georgia 2017-2018	The Data Exchange Agency
Kosovo*	State Strategy for Cyber Security and the Action Plan for 2016 to 2019	Officer responsible for implementing the Cyber Security Strategy, Ministry of internal affairs; National Cyber Security Council
Moldova	National Cybersecurity Program of the Republic of Moldova for 2016-2020	Ministry of Information Technology and Communications
Montenegro	Cyber Security Strategy for Montenegro" for the period 2018-2021	Information Security Council
Serbia	Strategy for Development of Information Security in Republic of Serbia 2017-2020	Office for IT and eGovernment (Ministry of Internal Affairs had such office set up since 2015)
Ukraine	Cybersecurity Strategy of Ukraine 2016	National Coordination Center for Cyber Security

*This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence

Q2 – National Energy Regulatory Authority

1. Definitions and Abbreviations
2. Introduction
3. General information
4. National Cybersecurity strategy and action plan (4)
5. National legislation (10)
6. National standardisation and accreditation schemes (3)
7. Cyber security organisational structures (4)
8. Risk assessment (4)
9. Cyber security cooperation, projects and assistance (6)
10. Awareness programmes, education and cooperation (6)

Q2 – National Energy Regulatory Authority

5.2 Is the Energy Community Critical Infrastructure (EnCCI)[7] identification foreseen in the legislation? (ECI)

- Yes

  If yes, please provide:

  Title/reference of the document: _____

  Date of document: _____

  - Please provide a list of Operators of Critical Infrastructure in the energy sector (if already designated)

    _____

    _____

    _____

    _____

    _____

    _____

    _____

    _____

  - In case that identification of EnCCI and Operators in the energy sector started but is not yet finished, how many of them you expect in your country? _____

- No

Q3 – Operators in the energy sector

TSOs, DSOs, Producers/Generators

1. Definitions and Abbreviations
2. Introduction
3. General information
4. Identification of critical infrastructure and essential services (5)
5. National legislation (6)
6. National standardisation and accreditation schemes (2)
7. Cyber security cooperation, projects and assistance (3)
8. Awareness programmes, education and cooperation (3)

Q3 – Operators in the energy sector

4.1 Does the organisation operate or own an energy infrastructure, the disruption or destruction of which would have a significant impact on at least two Contracting Parties and/or Member States (Energy Community critical infrastructure)?

4.2 Does the organisation operate or own energy infrastructure, the disruption or destruction of would have a significant impact in a Contracting Party as a result of the failure to maintain those functions (Critical infrastructure)?

4.3 Is the organisation operator of essential services, for the maintenance of critical societal and/or economic activities that depend on network and information systems, the disruption of which would have a significant effect on the provision of essential services?

4.4 Are criteria for the designation of critical infrastructure and essential services laid out in the legislation?

4.5 Are criteria for the determining the significance of disruptive effect defined in the legislation?

Q3 - Delivery

Best way to obtain list of (for questionnaire delivery)

- TSOs
- DSOs
  - NRAs
  - TSOs
- producers/generators
  - TSOs

Questionnaire delivery, support and collection

- Delivery and collection by e-mail
- Contacts for
  - Questionnaire (contact point on team side)
  - Provided answers (contacts at questionnaire recipient)

Questionnaire	Delivery date	Foreseen return date
Q1	Second half of April	Second half of May
Q2	Second half of April	Second half of May
Q3 - TSOs	Second half of April	Second half of May
Q3 – DSOs, generators	Beginnig of May	End of May

Next steps

- W2 – Risk assessment (early June)
  - Consequences (categories)
  - Capability/motivation and likelihood
  - Risk scenarios

- On site visits (May – June)
  - Competent cybersecurity authorities
  - NRAs
  - TSOs
  - Major DSOs/producers/generators

- First Interim report (July)

Thank you!

Blueprint Energy Solutions GmbH

Presenter:
Peter Grasselli
peter.grasseli@aitsa-is.com

Vienna, 11.04.2019.