NIS PLATFORM
PLENARY MEETING

WG1 – RISK MANAGEMENT
FINAL RECOMMENDATIONS

Brussels, April 30th 2014

NIS PLATFORM WG1 – RISK MANAGEMENT

AGENDA

* 1. Initial Priorities – Scope of Work & Topics
* 2. Gap Analysis
* 3. Key Findings
* 4. Recommendations
  * Cybersecurity Risk Management Methods, Standards and Frameworks
  * Risk Metrics
  * Awareness and Education
* 5. Further work
* 6. Topics Recommended for WG3 research

NIS PLATFORM WG1 – RISK MANAGEMENT

INITIAL PRIORITIES – Scope of Work

The NIS platform WG1 will as a matter of priority aim to:

1. Identify and facilitate the up-take of risk management practices, including standards, to enhance cybersecurity; such practices should be process-related and technology-neutral;

2. Develop incentives to adopt the identified practices.

NIS PLATFORM WG1 – RISK MANAGEMENT

INITIAL PRIORITIES – Topics

Based on feedback received at the inaugural WG1 meeting on 25th September, an initial priority of the following topics were proposed and investigated:

1. Methodologies to identify critical information assets, vulnerabilities, impacts, threats and risks and to mitigate and manage risks – from both an individual organization and supply chain perspectives;

2. Risk metrics, to monitor, predict, track and evaluate risk exposures;

3. Means of mapping cybersecurity risk management practices to varying levels of risk and organizational size via an effective framework of methods and standards;

4. The use of Capability Maturity Models to help organizations improve their risk management processes.

NIS PLATFORM WG1 – RISK MANAGEMENT

GAP ANALYSIS

This section contains the main gaps identified during the lifetime of WG1, to be covered in further work or passed for research to WG3.

* Against Initial ToR requirements
* Membership representation
* Standards
* Frameworks and maturity models
* Research

NIS PLATFORM WG1 – RISK MANAGEMENT

KEY FINDINGS of the survey

The purpose of the survey was to identify and capture key reference documents for cybersecurity risk management, and to gather views of all EU nations and lead industries. They key findings were as follows:

* Approaches to cybersecurity risk management
* Choice of risk management standards and methods
* Understanding risk appetite and tolerance levels
* Using risk management frameworks and maturity models
* Challenges when applying risk methods
* Inventory of standards assessed

NIS PLATFORM WG1 – RISK MANAGEMENT

RECOMMENDATIONS - Cybersecurity Risk Management Methods, Standards and Frameworks

Recommendations were mainly based on the feedback obtained from the survey on the following topics:

* Establish Risk Governance Structures
* Establish Overall Organisational Requirements and Responsibilities
* Apply Core Risk Management Methods and Standards
* Apply a Core Set of Cybersecurity Controls
* Agree Cybersecurity Risk Appetites

NIS PLATFORM WG1 – RISK MANAGEMENT

RECOMMENDATIONS – Risk Metrics

Apply a core set of metrics appropriate to the organisation, sector and stakeholders within the supply chain. Different set of metrics have been selected depending on priorities.

* Priority 1 : Metrics that an organisation should apply at a first step. They are considered the most important and applicable.
* Priority 2: Those metrics to apply once the priority 1 metrics have been applied.
* Priority 3: Metrics to be applied in the last steps, once priority 1 and 2 metrics have been applied.
* Risk Metrics for SMEs : reduced set of metrics, extracted from the Priority 1 list, that are considered to be more applicable for SMEs.

NIS PLATFORM WG1 – RISK MANAGEMENT

RECOMMENDATIONS – Awareness and Education

Awareness and Education is based in three tiers of implementation: EC/EU, Member States and individual orgs.

* Raising awareness to acquire and disseminate cyber security knowledge and skills among the staff and at senior level (C-level awareness)
* Approaches to remove barriers to the adoption of best practices to help less advanced organisations progressively increase their level of cyber security
* Linkage with incentives to facilitate the take-up of risk management best practices
* The articulation of roles and responsibilities
* Education and Training

NIS PLATFORM WG1 – RISK MANAGEMENT

FURTHER WORK

Some topics have been selected as candidates for any work that develops from the findings of WG1.

* Continue to seek and assess member input
* Guidance Documentation
* Assess the topics excluded from the original ToR
* Assess topics identified by additional gap analyses and key findings
* Technological solutions

NIS PLATFORM WG1 – RISK MANAGEMENT

TOPICS RECOMMENDED FOR WG3 RESEARCH

* Research to identify the barriers to adoption of best practices
* Research to gauge Risk Management penetration to 'hard to reach' orgs and SMEs establish the best means of communication to raise awareness
* Research to help to solve the lack information to perform statistical/predictive risk analysis
* Research into dynamic risk assessment for cyber threats
* Research on risk metrics

NIS PLATFORM WG1 – RISK MANAGEMENT

WG1 CHAIRMEN AND SG LEADS:

* WG1 CHAIRS:
  * Miguel Angel Sánchez Fornié
  * Carl Colwill

* WG1 SG LEADS:
  * Antonio Ramos García
  * Jeremy Ward
  * Patrick Curry
  * Lorraine Spector