Working Group 1 (Risk Management) of the NIS Platform

Terms of Reference

Terms of Reference (ToR) for Working Group 1 (WG1)

The WG1 ToR is based on the initial scoping and objective paper distributed to the plenary meeting of the NIS Platform on 17th June 2013 and updated with the feedback received from the inaugural meeting of WG1 members on 25th September 2013.

In overall terms, WG1 will aim to identify best practice in cybersecurity risk management activities, provide guidance to enhance levels of information security and facilitate the voluntary take-up of the practices; such practices should be organisation process-related and technology-neutral.

The output from WG1 will be a set of guidance documents, which will feed into Commission recommendations on cybersecurity to be adopted in 2014. The guidance from WG1 will be elaborated with a view to assist public and private organisations, including less advanced ones, to comply with the general risk management obligation proposed under the NIS Directive.

Scope

The scope of WG1 will address:

a) cybersecurity requirements and issues as covered by the NIS Platform;
b) organisations of all sizes;
c) cross-sector and cross-border approaches;
d) 'internal' and 'external' risks, for example within supply chains.

WG1's output will also consider linkage with economic, legal and technological incentives that could be used at EU and/or national level to stimulate the take-up of the best practices identified and to help less advanced stakeholders progressively improve their level of information security. Such incentives will have to be economically sustainable and be aimed at ensuring a level playing field among businesses in the EU.

Objectives

WG1 will identify best practices to design, implement and maintain cybersecurity risk management processes throughout an organisation (from SMEs to large organisations, covering both public and private sectors) – proportionate to the risks that different organisation may face; this may include supply chain risks. The WG will recommend the use of best practices within a cybersecurity framework to help organisations implement risk management activities in a consistent fashion. Should gaps in current practices and standards be identified, WG1 will liaise with the Multi Stakeholder Platform for ICT Standardisation to close these gaps.

The output from WG1 will be a set of guidance documents. This will include steps to be taken at strategic, management and operational level to improve risk management activities and manage cybersecurity risks.

Best practices guidance could cover:

- methodologies to identify critical information assets, vulnerabilities, impacts, threats and risks and to mitigate and manage risks;

- risk metrics, to monitor, predict, track and evaluate risk exposures;
- monitoring, testing and auditing networks, systems and cybersecurity controls;
- mapping cybersecurity risk management practices to varying levels of risk and organisational size via an effective framework of methods and standards;
- the identification of minimum security requirements;
- the articulation of roles and responsibilities;
- raising awareness to acquire and disseminate cybersecurity knowledge and skills among the staff and at senior level (C-level awareness).
- procedures to verify the availability and status of assets and operations;
- contingency plans and strategies for incident response and escalation;
- management of the interactions between cybersecurity risk management and the overall risk management/continuity plan of an organisation;
- approaches to remove barriers to the adoption of best practices to help less advanced organisations progressively increase their level of cyber security;
- the use of Capability Maturity Models to help organisations improve their risk management processes;
- linkage with incentives to facilitate the take-up of risk management best practices;
- development of an effective 'glossary' of cybersecurity terms.

WG1 will also identify inputs and outputs to/from WG2 and WG3.

Deliverables

WG1 will produce an initial ToR by 11th October and an initial set of best practice guidance documents by 31st May 2014; additional deliverables are subject to agreement and definition by WG1 Chairs and members and will be delivered in a phased approach. All documents will be living documents and subject to change.

Chairs of WG1

The chairs of WG1 are Carl Colwill (BT, UK) and Miguel A. Sánchez Fornié (Iberdrola, Spain).

Working methods

WG1 working methods are described in the WG1 Rules of Procedure document.

Structure

To be decided: WG1 may be structured by topics, working groups, work package owners, editorial and communication roles, etc.

Platform of work

The preferred online platform for exchanging information is the platform that will be provided by ENISA, which includes a forum, mailing list capabilities, and a document repository: https://resilience.enisa.europa.eu/.

Planning for Delivery

To be decided: based on the agreed scope of the ToR and the structure agreed in terms of division and assignment of work. A phased approach to delivery will be taken, milestones will be set and project management applied.

These Terms of reference may be adapted by the Chairs in the course of the activities of WG1.

CJC/MAS/OB
11/10/13