5th NIS Platform Plenary 27.5.2015
Group discussions to address, verification and auditing of the organisational risk management requirements and skills needed within an organisation.

Introduction

The next chapter WG1 has been ask to develop for the EU NIS Platform is Chapter 2 verification and auditing of organisational risk management.

This discussion paper should be used as background for group discussions during the 5th NIS Platform Plenary 27.5.2015.

The purpose of this discussion paper is to stimulate ideas and discussion on what WG1 believe is the best approach for organisations to incorporate based on current industry best practice to address verification and auditing of organisational risk management processes.

Risk is a dynamic issue, so some kind of continuous monitoring should be implemented to assure that right decisions are taken at any moment and to ensure a global visibility of the major risks and of the mitigation plan. This monitoring can range from high assurance dynamic risk assessments down to more static discrete mechanisms like periodic security audits, penetration tests, vulnerability assessments, procedures for risk management, feedback. This requires the implementation of a process to define, measure and monitor metrics (easy to understand by management) about business impacts and likelihood of occurrence of threats.

It is important that we keep the needs of SMEs in mind when considering the best approach to verification and audit. The content of chapter 2 needs to be such that it can be implemented by all levels of organisations in any sector business.

The aim of the group discussions is to scope the topics as narrowly and precisely as possible, based on the needs expressed by the NIS Platform community.

Topics to be discussed in groups during the NIS Platform Plenary:

- Managing risks in an organisation.
  - Who / why / benefits.
  - Metrics

- Why we need verification and audit
  - To follow Plan Do Check Act.

- Internal Audit / External Audit
  - Self-assessments
  - Requirements & benefits of both

- External Certification
  - Consider what are available - select most appropriate.

Expected outcome

The outcome of the group discussions should be exploratory with the ultimate aim of delivering recommendations for audit and verification requirements to develop Chapter 2.

WG1 initial recommendations

Assurance

- Service assessment criteria (SAC), based on standards, shall be used to audit for compliance
- Self-assessment should be permitted, however independent assessment will be required in most cases for reasons of:
  - Regulation or legislation;
  - Mutual liability;
  - Insurance;
  - Supply chain contracts;
  - Service provision contracts.
  - Governments and industries should recognise assurance schemes and trust framework providers, who can approve auditors and assessors for each Level of Assurance (LoA) listed in section 6.4 Assess topics identified by additional gap analyses and key findings of the initial recommendations.

Assurance relies on monitoring and security metrics. These metric were defined in WG1's initial recommendations which can be found in section 5.2 Cybersecurity Risk Management Metrics:

https://resilience.enisa.europa.eu/nis-platform/shared-documents/3rd-plenary-meeting-april-2014/wg1_guidance_20140428/view