

NIS PLATFORM PLENARY MEETING

WG1

Brussels, May 2015

NIS PLATFORM WG1 – RISK MANAGEMENT

AGENDA

1. CHAPTER 1 – DRAFT RECOMMENDATIONS
2. PLENARY MEETING – GROUP SESSION
3. NEXT STEPS

NIS PLATFORM WG1 – RISK MANAGEMENT

CHAPTER 1 – SCOPE OF WORK

- * Scope divided into two areas:
 - * Organisational Structures and General Requirements
 - * Specific requirements for Small and Medium Enterprises

- * Three key attributes to be taken into account:
 - * Confidentiality,
 - * Integrity,
 - * and Availability
 - * Besides authenticity, accountability, non-repudiation and reliability can also be included within the scope

- * Specific technical and procedural controls to mitigate and respond to cybersecurity risks have been provided (ISO 27001, ISO 27005, etc.)

NIS PLATFORM WG1 – RISK MANAGEMENT

Organisational Structures and General Requirements

Cybersecurity risk management organisational structures

- * Risk Management is an ongoing continual process within an organisation.
- * Different functions/roles are involved (Business, Risk, Technical ICT, Governance and audit)
- * Segregation can be adopted – 3 lines of defense Model.

NIS PLATFORM WG1 – RISK MANAGEMENT

Organisational Structures and General Requirements

Key roles to cultivate a risk management culture

- * This section gives an overview of typical key roles required within an organisation to cultivate a risk management culture, which can be incorporated by an organisation as appropriate, depending on factors such as requirements, size or business sector
- * Collaboration across the organisation is important to ensure cyber risk management is effectively implemented.
- * For employees it is absolutely critical that all staff understand they have personal responsibility for cybersecurity, regardless of their role in the organisation

NIS PLATFORM WG1 – RISK MANAGEMENT

Organisational Structures and General Requirements

Organisational controls to ensure effective risk management

- * Cybersecurity risks and vulnerabilities, a subject of interest at every level (including C-level - Commitment)
- * Cyber risk education, awareness and responsibilities need to be driven at varying levels
- * Industry standard approaches to risk management should be considered, e.g. the “Identify, Protect, Detect, Respond, Recover” model.

NIS PLATFORM WG1 – RISK MANAGEMENT

Organisational Structures and General Requirements

Determination of risk appetite

- * Risk Appetite can be defined as the “Willingness of an organisation to accept a defined level of risk”.
- * Risk categorisation may facilitate decisions – i.e. Likelihood/Impact matrix.
- * In order to have comparable risk appetite over time, risk analysis should be repeatable
- * Risk appetites and levels of acceptance should also be communicated up and down supply chains and/or with key partners

NIS PLATFORM WG1 – RISK MANAGEMENT

Specific requirements for Small and Medium Enterprises

The goals of cybersecurity for Small and Medium Enterprises (SMEs)

- * This section gives overview of why should SMEs address cybersecurity risks? Incentives to address cybersecurity.
- * SMEs should look to review and consider complying with appropriate industry cybersecurity standards or requirements.
- * current incentives to encourage SMEs to adopt good cyber risk management are highlighted in the document.

NIS PLATFORM WG1 – RISK MANAGEMENT

Specific requirements for Small and Medium Enterprises

The ways to manage SMEs cybersecurity risks

- * This section gives an overview on how should SMEs manage cybersecurity risks:
 - * Internally vs externally?
 - * Implications of outsourcing: resources, costs, etc.
- * SMEs can look to implement appropriate security standards which provide a good baseline for managing cybersecurity risks.
- * To ensure SMEs outsource to the right partner, SMEs should understand the different cybersecurity certifications. Standardised procurement checklists can be of help when outsourcing risk management.

NIS PLATFORM WG1 – RISK MANAGEMENT

Specific requirements for Small and Medium Enterprises

Risk management frameworks for SMEs

- * This section gives an overview of the specific frameworks or requirements to enable SMEs to implement an organisational structure that ensures effective cybersecurity risk management.
- * there are risk management frameworks or guidance schemes focused on SMEs, promoted by:
 - * National governments
 - * Private initiatives
 - * ENISA
- * Any framework that is implemented by an SME should be simple enough to be managed by personnel with limited expertise and knowledge.

NIS PLATFORM WG1 – RISK MANAGEMENT

PLENARY MEETING

- * Small groups session so that all participants has the opportunity to input
- * Chapter 2 conclusions will depend on the input provided
- * To foster input and participation, four key topics have been issued, split into groups:
 - Managing risks in an organisation: Who, why, benefits and metrics
 - Why we need verification and audit: To follow Plan Do Check Act
 - Internal Audit / External Audit: Requirements & benefits of both
 - External Certification: Consider what are available - select most appropriate.

NIS PLATFORM WG1 – RISK MANAGEMENT

NEXT STEPS

- * Disseminate Recommendations from Chapter 1
- * Complement a first draft document for Chapter 2 with feedback from the plenary meeting
- * Issue draft practical recommendations for comments