

NIS PLATFORM PLENARY MEETING

WG1 – Chapter 1 Organisational structures and requirements

Brussels, November 2014

NIS PLATFORM WG1 – RISK MANAGEMENT

AGENDA

1. WG1 FUTURE WORK PLAN
2. CHAPTER 1 – SCOPE OF WORK
3. PLENARY MEETING
4. NEXT STEPS

NIS PLATFORM WG1 – RISK MANAGEMENT

WG1 FUTURE WORK PLAN

* Tentative timing of WG1 chapters –

	October – December 2014	February – April 2015	June – September 2015
WG1 Chapters	1. Organisational structures and requirements (skills part to be added in June 2015 based on WG3 output)	2. Verification and auditing of requirements	8. [Optional] Incentives for the uptake of good cybersecurity practices

* timing of these deliverables will depend on the active contribution by members, in line with the Member's Charter

NIS PLATFORM WG1 – RISK MANAGEMENT

CHAPTER 1 – SCOPE OF WORK

The recommendation should specify existing risk management standards and best practices that organisations, depending on their size and needs, can use to tailor their own approach

1. The contents of this chapter must address all sizes of organisations, preferably across all sectors
2. The NISP working groups have identified as a priority small to medium enterprises (SMEs); these organisations have less resource to apply to effective cybersecurity risk management and need the greatest guidance

NIS PLATFORM WG1 – RISK MANAGEMENT

PLENARY MEETING

- * Small groups session so that all participants have the opportunity to input
- * Chapter conclusions will depend on the input provided
- * To foster input and participation, seven key questions have been issued, split into two groups:
 - General Requirements – Applicable across all organisations
 - SMEs specific application

NIS PLATFORM WG1 – RISK MANAGEMENT

General Requirements – Applicable across all organisations

Key question 1

What good practices regarding organisational structures have emerged to ensure effective cybersecurity risk management?

- Practical and pragmatic cases, quantify and qualify benefits.

Key Question 2

What controls can be implemented within an organisation structure to ensure effective cybersecurity risk management?

- Risk management measures with more impact, available support.

NIS PLATFORM WG1 – RISK MANAGEMENT

General Requirements – Applicable across all organisations

Key question 3

What are the key roles within an organisation to cultivate a risk management culture? E.g. CEO, CISO, risk managers, IT-purchaser, auditor, employee, etc.

- Responsibilities of roles, outsourcing

Key Question 4

How should an organisation determine its risk appetite?

- How to agree risk exposure, risks to accept

NIS PLATFORM WG1 – RISK MANAGEMENT

SME specific Application

Key question 5

Why should SMEs address cybersecurity risks? Incentives to address cybersecurity?

Key Question 6

How should SMEs manage cybersecurity risks? Internally vs externally?
Implications of outsourcing

Key Question 7

What specific frameworks or lighter requirements are there to enable SMEs to implement an organisational structure that ensures effective cybersecurity risk management?

NIS PLATFORM WG1 – RISK MANAGEMENT

NEXT STEPS

- * Complement Chapter 1 with additional feedback from the plenary meeting
- * Issue practical recommendations
- * Start Chapter 2: Verification and auditing of requirements