

**Dear NIS Platform WG1 members**

*We would like to wish you a very relaxing holiday period, and thank you for all the useful contributions you gave during the 4<sup>th</sup> NIS Plenary Platform on 25.11.2014.*

*The Plenary and in particular the animated group discussed marked a new beginning in our way of working. Our rapporteur Andro Kull, Ian Morton, Guillermo Manent and us have since then worked on integrating the input received into Chapter 1 – Organisational structures and requirements for risk management.*

*You should receive the next version of Chapter 1 for your validation in early January. We have accommodated all comments that we could, taking into account the scope of the document and our focus on cybersecurity risk management best practices – rather than all topics associated with cybersecurity. Some input will be more appropriate for one of the forthcoming guidance Chapters and has not been taken into account into Chapter 1.*

*The approach within the NIS Platform is to form a rough consensus views. This is reflected in the Member's Charter that you have agreed to when reconfirming your commitment to the NIS Platform process. Even though we did not detect any major differences in view during the last Plenary it cannot be excluded that someone might want to have a dissenting opinion recorded. But hopefully this will not be the case, to increase the value of NIS Platform guidance.*

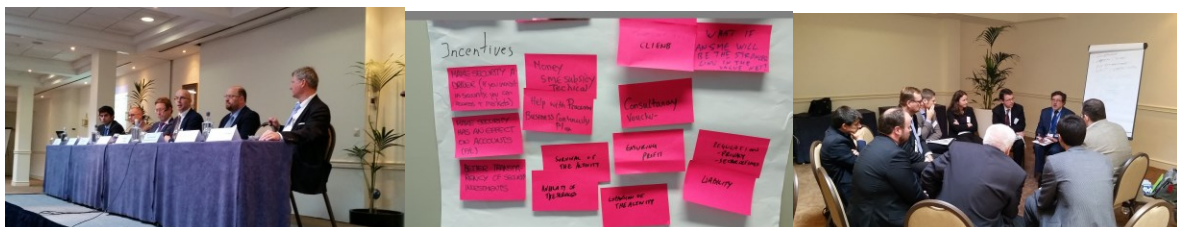
*A summary from the animated group discussion can be found below. Below you will also find a table summarising the planned work on future NIS Platform guidance Chapters.*

*To refresh the good memories from the Plenary meeting you can go to the Platform website<sup>1</sup> to see all the flip-charts and power point slides produced. And the pictures! (Un)Fortunately we cannot reproduce the bang of the bell!!*

*Looking forward to continued work with you in 2015.*

*Season's Greetings*

Carl Colwill and Miguel A. Sánchez Fornié  
Chairs of WG1



<sup>1</sup> <https://resilience.enisa.europa.eu/nis-platform/output-subgroups-4th-plenary-november-2014> If you have problems accessing please contact [nisplatform@enisa.europa.eu](mailto:nisplatform@enisa.europa.eu)

**Breakdown and tentative timing of Chapters per Working Group:**

	October – December 2014	February – April 2015	June – September 2015	<i>EU Policies/Programmes that NISP work relates to</i>
<b>WG1</b> Chapters  <b>Risk management</b>	1. Organisational structures and requirements (skills part to be added in June 2015 based on WG3 output)	2. Verification and auditing of requirements	8. Incentives for the uptake of good cybersecurity practices (labels, public procurement, cyber insurance, certification, taxation etc.)	<i>Commission recommendation on good cybersecurity practices (end 2015)</i>
<b>WG2</b> Chapters  <b>Information sharing and incident notification</b>	3. Voluntary information sharing	6. Guidance on data protection	4. Incident response  5. Mandatory incident notification	
<b>WG3</b> Chapter  <b>Secure ICT research and innovation</b>	Work already planned (Secure ICT landscape; Business cases and innovation paths; Education and training; Strategic research agenda) + 7. Recommendations on research challenges and opportunities			<i>Horizon 2020 (Work Programmes 2016-2017; 2018-2019; etc.)</i>

**Summary from animated WG1 risk management discussion groups (1-7). Note that these are only a summary and the Chairs and Rapporteurs are working to review the substantial and varied feedback to extract key points for the next Chapter draft.**

**Group 1: What good practices regarding organisational structures have emerged to ensure effective cybersecurity risk management? Animated by Ralph Eckmaier**

Managers have to commit with risk management, it is not only for IT staff. Indeed different roles on risk management can be identified: governance, business process risk, implements controls.

Better not to personalize roles in one person as it depends much on the organizations and one role could be played by more than one person, or one person to take various roles, as it is in SMEs.

Another point raised by group was on the accountability of these roles, accountability of performance.

**Group 2: What controls can be implemented within an organisation structure to ensure effective cybersecurity risk management? Animated by Miguel A Juan**

Make cybersecurity risk a subject of interest to all across the organization and not only a matter for IT department. SMEs should include risk assessment in the strategic plan of the company to help it identify its acceptable risk.

Three key recommendations:

- Promote the share of information also among SMEs integrated in the value chain of the organization.
- Reduce complexity, especially for SMEs. Make it more practical, specific.
- Better leverage of exiting information to tackle risk.

**Group 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. Animated by David Francis**

The vision on cybersecurity risk should be led by CEO (not CSO<sup>2</sup>), should be a commitment behind, as it is every ones responsibility and should be accompanied by key performance indicators (KPIs).

Important to differentiate training for compliance and awareness in organizations, and to appropriately allocate the responsibilities, making it also visible in the job description in order to get full commitment from employees.

**Group 4: How should an organisation determine its risk appetite? Animated by Andro Kull**

---

<sup>2</sup> Chief Security Officer

Important to differentiate two big groups, private and public, with different metrics on how to identify the risk appetite. For that purpose important to identify the critical information assets. Moreover the evolution of threats landscape and environment make it necessary to periodically review the set of indicators and risk appetites.

In regard of the definition of risk appetites important to identify those risks that we accept, those that we delegate and the ones we will mitigate. A cost-benefit analysis will help us in defining the risk appetite.

#### **Group 5: Why should SMEs address cybersecurity risks? Animated by Ulrich Meuser**

Discussion turned around three questions: Why should SMEs address cybersecurity risks; what are the incentives for doing it; what are the different ways to deal with cybersecurity risk e.g. is outsourcing a way.

On why, there was a common agreement on main driver is to stay in business. Because you are part of the supply chain, you are participating in procurement and it is a requirement; to protect your profit; to build up trust with your customer but also of your bank, insurer etc.

On incentives, it should be a business driven approach, only minimum by regulation, make the investment on cybersecurity risk visible, maybe by establishing some EFQM (quality?) levels, important to facilitate the access to cybersecurity information and skills. Another incentive can be to issue consultancy vouchers to carry out tech consultancy of on business processes.

On ways, there was consensus that technological risk can be outsourced, but business risk cannot, it has to stay internal and managed internally.

#### **Group 6: How should SMEs manage cybersecurity risks? Animated by Rob Kloots**

SME are usually part of the supply chain and therefore important contributors to the overall risk management in big organizations. Governments should help in some way SMEs. Putting in place simple solutions that can be tailored to the need of SMEs. Another way to help is including cybersecurity risk requirements in public procurement.

#### **Group 7: What specific frameworks or lighter requirements are there to enable SMEs to implement an organisational structure that ensures effective cybersecurity risk management? Animated by Rob Kloots**

Governments can contribute with official frameworks, such as UK cyber essentials and 10 point guide to cybersecurity, and the Belgian cybersecurity guide. A multi qualification level certification, expressing the maturity of an organisation, was also proposed. Important than any framework is endorsed by government or regulated; could be required as a precondition/license to operate services as well as both in public and private procurements.