This questionnaire is circulated on the basis of the plan for the review of the 2002 Security Guidelines agreed at the 32nd WPISP meeting on 9-10 May 2012 [DSTI/ICCP/REG(2012)1].

Delegates are invited to provide answers to this questionnaire by 20 July 2012. Responses should be sent to laurent.bernat@oecd.org and michael.donohue@oecd.org.

Laurent Bernat; E-mail: laurent.bernat@oecd.org; Tel: +33 1 45 24 93 83
QUESTIONNAIRE FOR THE REVIEW OF THE OECD 2002 SECURITY GUIDELINES

1. In its 2002 Recommendation Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Security Guidelines), the OECD Council recommends that Member countries “review the Guidelines every five years so as to foster international co-operation on issues relating to the security of information systems and networks”. This review mechanism, which is common in OECD instruments, aims to ensure that the Guidelines remain relevant and provides an opportunity for revision when countries agree that it is needed.

2. The Security Guidelines form one of the fundamental building blocks for the work of the WPISP and their review is strategic to take a fresh look at the issues in light of recent developments, consider progress achieved since the adoption of the Guidelines and set out the road ahead. Thus one of the benefits of this review process is to feed the reflection on the role of the OECD in the new international cybersecurity landscape and on future WPISP activities in general.

3. The questionnaire below aims to collect views of delegations regarding the relevance of the Guidelines in the current environment and the best way forward. It includes open-ended questions followed by some suggestions to help prepare responses. Respondents should feel free to address the questions as they see fit including beyond these suggestions and illustrations. Questions 1 to 6 address the Guidelines themselves. Question 7 is related to the next step of the process for the review. The last question provides an opportunity to make any suggestions and remarks that other questions might not have addressed.

4. The annex includes background to help delegates respond to the questionnaire. As agreed at the 32nd WPISP meeting in May 2012, parts of it will be made public separately as a reference document about the Guidelines.

5. In responding to the questionnaire, delegates are invited to take into account the Draft Comparative Analysis of National Cybersecurity Strategies which was discussed at the 32nd WPISP meeting and is in the process of being finalised [DSTI/ICCP/REG(2011)12/REV1].

6. Responses should be sent by 20 July 2012 to the Secretariat (laurent.bernat@oecd.org, michael.donohue@oecd.org). Based on the responses received, the Secretariat will prepare a report to feed the discussion regarding the next step for the review at the 33nd WPISP meeting on 18-19 October 2012.
Questionnaire

1. Are there developments in the context of the security of information systems and networks that would indicate a need to modify the Guidelines? (cf. “recognising” section of the Recommendation and Preface of the Security Guidelines)

   In 2002, the key driver for the revision of the 1992 Guidelines was the emergence of interconnectedness. What changes in the environment, the technologies, the people and their processes, if any, may drive a modification of the 2002 Guidelines and why? ¹

2. Are the aims and scope of the Guidelines still in accordance with the current context described in question 1? (cf. Section I of the Security Guidelines)

   For example, the Guidelines aim to foster greater confidence in information systems and networks, they do not explicitly aim to protect systems and networks on which the functioning of the economy and society increasingly rely. Further, is the notion of security of information systems and networks still relevant or should it evolve to include the protection of information assets?

3. Taking into account response to question 2, are the principles still relevant to address the aims and scope of the Guidelines? Are there areas that are not adequately addressed by the principles? (cf. section II of the Security Guidelines). Please explain why.

   For example: Are there new principles that need to be added (e.g. on resilience or business continuity)? Should some existing principles be removed or rewritten? etc.

4. Is there a need to develop an explanatory memorandum and if so, what should it focus on?

5. The Guidelines do not address how the principles should be implemented. Is there a need to develop guidance related to the implementation of the principles and if so, which aspects should require particular attention? What should be the scope of such implementation guidance (e.g. public policy and co-operation at national and international levels, policy development within public and private organisations)?

   For example: i) the 2007 review highlighted the need to foster research and development, public-private co-operation, international co-operation, and linkages between security and privacy, ii) recent WPISP work on national cybersecurity strategies highlighted the need for a national strategy, the development of a cybersecurity industry sector and relevant skills, etc. iii) Some of the concepts of the 2008 Recommendation on Critical Information Infrastructures Policy might also help in guiding the implementation of the Guidelines.

6. The 2002 Security Guidelines and the 1980 Privacy Guidelines are interrelated and there is an overlap in their review processes. Should the intersections between the two instruments be reinforced and, if so, how?

¹ The draft report on national cybersecurity strategies provides some elements on this aspect. See OECD, 2011a.
7. What additional elements should be included as part of the process for the review of the Security Guidelines?

− Is there a need to collect more information to carry out the review and if so, what are the best means to do so? For example, drafting an analytical report, organising a workshop similar to the 2001 OECD Tokyo Workshop on Security in a Networked World, conducting a consultation of various experts including from the private sector, etc.

− How can we ensure that potential revised Guidelines have global impact? Should the OECD engage non-member economies and international organisations in the review and if so, what would be the best means to do so?

− How can we ensure in an environment that changes at fast pace that potential revised Guidelines remain relevant 5 to 10 years ahead.

8. Please indicate other observations not addressed in the above.
ANNEX

Background for the review of the security guidelines.

7. Although the Security Guidelines, like all OECD Recommendations, are a non-binding instrument of the Organisation, they have a great moral force. They represent the political will of Member countries and there is an expectation that Member countries will do their utmost to fully implement them. The brief history of the OECD Security Guidelines illustrates that they received strong support from OECD members and beyond, served as a widely recognised international standard, and maintained the OECD’s leadership in this policy area since the early 1990s. It is followed by a section that provides some considerations as to be reflected upon in reviewing the Guidelines.

A brief history of the OECD Security Guidelines

The 1992 Security Guidelines and their revision

8. OECD interest in the security of information systems dates back to 1988 when the Committee for Information, Computer and Communications Policy (ICCP) agreed to prepare a study on the security of information systems. Four years later, in November 1992, the OECD Council adopted a Recommendation Concerning Guidelines for the Security of Information Systems based on the recognition that “the increasingly significant role of information systems and growing dependence on them in national and international economies and trade and in social, cultural and political life call for special efforts to foster confidence in information systems” (OECD, 1992). The Guidelines were intended to provide a foundation from which countries and the private sector, acting singly and in concert, may construct a framework for security of information systems.

9. The substantive core of the Recommendation consisted of an Annex with a “Principles” section including nine items (accountability, awareness, ethics, multidisciplinary, proportionality, integration, timeliness, reassessment, democracy) and an “Implementation” section with five items (policy development, education and training, enforcement and redress, exchange of information and co-operation). The Annex also included four other sections: Aims, Scope, Definitions, and Security Objective. Following a set of recognising statements, the main part of the Recommendation included recommendations to member countries and called for a review of the instrument every five years. The Recommendation was accompanied by an explanatory memorandum.

10. A first review of the 1992 Guidelines was undertaken in 1997 by the ICCP Committee, through its Group of Experts on Information Security and Privacy (prior to being renamed Working Party on Information Security and Privacy (WPISP)), by means of a questionnaire issued to member countries. The review concluded that the 1992 Guidelines were still adequate to address the issues and purposes for which they had been formulated. However, it also recognised that since their publication, various other security issues and challenges had emerged, e.g. with regard to the increased connectivity between information systems, the related broadening

2. Recommendations are adopted in accordance to Article 5 of the Convention on the OECD which states that “In order to achieve its aims, the Organisation may: […] (b) make recommendations to Members; […]”
scope of communication systems, and the emergence and use of the global information infrastructure (OECD, 1997).

11. The following review started in October 2000 and focused on “the development of inter-connected and interdependent information systems which are fundamental to modern economies” (OECD, 2000). An expert group was created to collect information on existing threats, vulnerabilities and actions taken by governments and the private sector. Japan offered to host a Workshop on Information Security in a Networked World in Tokyo on 12-13 September 2001 to exchange and share information with a view to developing a common understanding of information security and enhance OECD’s involvement in this area (OECD, 2001a). A number of non-members participated including Brazil, China, Malaysia, Russia, South Africa and Thailand (OECD, 2001b).

12. This second review was marked by a sense of urgency which resulted from i) the recognition that developments affecting the security of information systems in a world characterised by global ubiquitous networks significantly reduced the relevance of the 1992 Guidelines and ii) the events of September 11 which took place at the beginning of this process, the day before the Tokyo Workshop. At the WPISP meeting following the Tokyo workshop, delegates agreed to form a new group of experts to revise the Guidelines. Over five months, this group met three times in Washington, Sydney and Paris to develop a first draft. In March 2002, WPISP delegates agreed with a proposal from the United States to expedite the review process for completion by early September 2002, building on the outcomes of three additional ad hoc WPISP meetings. On 25 July 2002, the OECD Council adopted new Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. As a consequence of the speed of the process, the revision was limited to the Principles and both the implementation section of the 1992 Guidelines and the explanatory memorandum were removed.

The 2002 Security Guidelines

13. As compared to their predecessor, the 2002 Security Guidelines reflect a fundamental change in the approach to the security of information systems which is the generalisation of interconnectedness.

• The 1990s security paradigm

In the early 1990s, information systems were operated in silo and did not interoperate easily. Security focused on internal threats. Protection against the outside world resulted from reinforcing the main characteristic of information systems: keeping them closed by default and opening them only by exception and under tight controls. It was the age of perimeter security, where the isolation of the system kept threats away and protected it by avoiding risk.

14. Twenty years ago, organisations’ IT infrastructure typically consisted of multiple information systems operated in silos, in a closed and isolated manner. Systems were deployed for achieving specific purposes in various branches of an organisation, generally to increase productivity through “business automation”. Although networked computing existed, in practice, different network protocols were used in different contexts within a single organisation and applications were not designed for easily exchanging data with other applications. A fortiori, communication of these systems with other systems located outside of the organisation was exceptional. Siloed information systems resulted from many factors, such as the

3. See OECD, 2001b, p.5, Chairman’s statement. See also the summary record of the WPISP meeting on 9-10 October 2001 (OECD, 2001c) where “delegates concurred that, particularly in light of the events of September 11, a thorough and expedited review should be conducted. In terms of the focus of the review, the majority of delegates emphasized the importance of ensuring the ongoing application of the Security Guidelines given the changing nature of information in a networked world and in considering the review in this context”.

heterogeneity of the technology, lack of basic compatibility or interoperability, imprecision of standards, independent implementation, as well as the corporate culture of that time.

15. The security paradigm that generally prevailed reflected this situation. The priority was to address internal threats such as technical failure or theft of information by an insider. External threats were not the most significant ones because the IT environment did not provide many opportunities for their propagation. They were addressed by reinforcing an already existing state of relative isolation of the information systems from the outside world, prohibiting inbound and outbound flows of information by default unless specifically authorised, and placing these exceptionally authorised external flows under tight security control. This approach, which aimed to avoid external risk, was generally based on “perimeter security”, and pictured metaphorically as the thick walls, high towers and deep moats that surrounded middle-age cities with few guarded gates and bridges. Thus systems were not closed because of security; rather computing was closed and siloed as a result of limited demand and technical opportunity for openness and interconnectedness. The security paradigm was simply aligned with this operational reality.

Figure 1. Metaphor: Security of Information Systems in 1992

Note: City of Carcassonne, France. Source: Mipsotour Web site.

As of the second part of the 1990s, the IT environment paradigm progressively switched to network openness, enabled by the generalisation of Internet technologies which facilitated the interconnection of information systems. This evolution was mainly driven by the economic and social benefits of interconnectivity which generated an insatiable demand for increased information flows within and across organisations and even jurisdictions’ boundaries. In 2008, the OECD recognised the Internet Economy as a driver for economic growth, prosperity and quality of life.

16. The wide adoption of Internet technologies—the so-called layered TCP/IP network stack—unified network technologies and fostered networked communications both vertically within one organisation’s subsystems and horizontally, across the information systems of different organisations. Seamless interoperability and interconnectivity enabled the various, previously siloed, IT components of organisations to morph into joined-up information systems, within which information could flow freely. Moreover, information flows could henceforth extend beyond the constraints of organisational boundaries, and even national borders and jurisdictions.
17. Progressively, network interoperability became available by default on every component of information systems, switching the IT environment paradigm from isolation to openness. However, while the technology certainly enabled this evolution, the **business benefits of interconnectivity** were the real driver of the strong demand for opening networks and enabling more information to flow within and across organisations. Over the course of a few years, generalised interconnectivity profoundly modified business operations by enabling, for example, real time supply chain management, just in time production strategies (JIT) and enterprise resource planning (ERP). Other, sometimes simpler, applications such as email, voice and video conference, also transformed businesses and governments’ activities. In parallel, ICT and Internet penetration to households took off exponentially, connecting hundreds of millions of home, business and government users together across the Internet, forming a single global network of networks and enabling e-commerce, e-government and many other forms of digital interactions. Finally, progress in the technologies, liberalisation of telecommunication markets and increased bandwidth capacity, among other factors, fed an insatiable demand for more interconnectivity. The paradigm shift from closed networks to the open Internet gave birth to the Internet Economy, a driver for economic growth, prosperity and quality of life, as recognised by the OECD in June 2008.

18. The metaphoric representation of information systems as isolated fortified cities of the early 1990s became outdated. Instead, a single global ecosystem formed by myriads of widely interconnected groups of subsystems emerged, changing the walled cities metaphor to one giant megalopolis with varied open districts in permanent contact and exchange with each other.

*Figure 2. Metaphor of the IT environment in 2002 and after*

Note: London metropolitan area from above. Source: François Roche. http://www.flickr.com/photos/13066221@N03/2279144581/. Some rights reserved (CreativeCommons BY-NC-SA 2.0).

---

5. OECD, 2008e.
19. As economic and social interactions migrated to the Internet, so did crime. The attractiveness of the digital world for criminals of all kinds increased with the value of the assets they could reach in that space and with the reliance of people and organisations on interconnected information systems. Unfortunately, as these threats increased, the effectiveness of security measures designed to protect a closed environment progressively diminished, creating ever more opportunities for external malicious actors. Although they remained present, internal threats lost the main focus of IT security and external threats, characterised by their fast changing nature, became the main priority.

... While, the security paradigm tailored to a closed, relatively static and predictable environment was increasingly ineffective in addressing the fast-evolving nature of threats, the growth of information flows, and the dynamism and instability of the new interconnected and opened environment.

20. The security paradigm designed for a closed environment was fundamentally challenged by network openness. The multiplication of entry/exit points in information systems undermined the principle of establishing security by keeping systems as much isolated as possible. With generalised interconnectedness, the volume of information flows increased by several orders of magnitude without any limit being set. A scalability challenge emerged as security controls designed for addressing limited information exchanges became less effective when applied to massive information flows. Moreover, as interconnectedness enabled new devices, new computer code and new usages to be constantly introduced in systems, the IT environment switched from static, stable, and predictable to dynamic, unstable and unpredictable. Each change in the environment was potentially creating a new vulnerability, ready for exploitation by malicious actors of various kinds. By introducing instability in the IT environment, interconnectedness made obsolete both security mechanisms tailored for a stable environment and the objective of creating a stable state of security within information systems.

21. With varying degrees, depending on corporate cultures and contexts, tensions appeared between security requirements and business demand. From a security perspective, the evolution towards more openness in the name of potential business benefits was perceived as undermining the protection of organisations’ assets. From a business perspective, however, security requirements which limited and controlled openness were perceived as an obstacle to harnessing the potential business benefits of interconnectedness.

22. Ultimately, the demand for interconnectivity and free flow of information across networks became such that perimeter security blocking information flows by default and enabling them by exception became untenable from a business perspective. Eventually, the IT operational paradigm switched from closed to open networks despite its fundamental contradiction with the then dominant security paradigm. A new security paradigm had to be introduced to realign security with the new reality of the operational environment.
• The 2002 Security Guidelines: concepts for security in an open environment

The 2002 Security Guidelines: concepts for security in an open environment

In order to realign security with the new open and interconnected IT environment, the 2002 Security Guidelines shifted the security paradigm from static risk avoidance to dynamic risk management.

23. The 2002 Security Guidelines realigned security with the new digital environment, where the benefits of the free flow of information enabled by open and interconnected networks make it impossible to continue avoiding external risk by closing the system (so-called “perimeter security”). The Guidelines started from the premise that if the environment is open, information assets are going to be constantly exposed to a changing risk which cannot be totally eliminated, but can be managed and reduced before it is accepted. The Guidelines switched the paradigm of security of information systems and networks from risk avoidance to risk management, where perimeter security is one among many other means for reducing risks. In so doing, they transposed in the digital world the security reality of the physical world.

The principles of the Guidelines create a framework for security in an open digital world where participants reduce risk before accepting it, instead of avoiding risk by limiting interconnectivity.

24. All the principles of the Guidelines flow from this logic. While within a closed system, security can be taken care of by the operator of the system without users having to think too much about it, managing risk in an open, dynamic, instable and uncertain environment requires awareness of all the participants. Everybody has to play a part to reduce this uncertainty because no central authority can control all the flows at the gates anymore: there are too many access points and the information flows are too large and complex. All participants have some responsibility for security, according to their role (2. Responsibility), a responsibility that requires an increased level of awareness about the need for security (1. Awareness). Likewise, if there is uncertainty, then security incidents and emergencies will happen. Detecting and responding to them becomes vital to protect business operations (3. Response).

25. Furthermore, interconnected networks now form a single distributed (i.e. decentralised) network. All participants can be considered as part of a single society because they operate in a shared environment and are, to some degree, interdependent: the consequences of participants’ actions in one part of the network are not blocked by the walls protecting another part anymore but rather actions flow across networks, and may harm others just as they may benefit them. Therefore, participants’ behaviours should take into account that the Internet is a shared environment where some social norms should be respected, for the benefit of all. Participants should respect the legitimate interests of others (4. Ethics) and those who implement security measures should do so in a manner that respects the values of a democratic society (5. Democracy). Social values shared by OECD countries in the physical world should be shared in the digital world as well.

26. Risk is the result of potential threats which can exploit vulnerabilities to cause detrimental consequences. Managing risk requires first to conduct risk assessments to identify these threats and vulnerabilities, and understand their potential detrimental impacts (6. Risk Assessment). Because all assets placed in the open environment will face some degree of risk, security should be a fundamental element of all products, services, systems and networks. Participants should incorporate security as an essential element of information systems and networks (7. Security design and implementation). They should also adopt a comprehensive approach to security management, encompassing all levels of participants activities and all aspects of their operations (8. Security management).

27. Finally, because threats can originate from anywhere on a network which connects almost all systems across the globe, they continuously evolve in nature, intensity and characteristics. Organisations as well as technologies also evolve continuously, shaping an ever changing environment where new
vulnerabilities appear all the time. Therefore participants should continually review, reassess and modify all aspects of security to deal with evolving risks. An open world is a dynamic world. This dynamism enables creativity and innovation for better and for worse. Therefore, security should not be static. Consistent with the nature of the environment, it should be dynamic (9. Reassessment).

The impact of the 2002 Security Guidelines

28. The 2002 Security Guidelines had a considerable impact. The press release announcing their adoption was widely disseminated and commented by the media and the Guidelines set the 2002 record of the “most downloaded document in one month” on the OECD web site. As part of their commitment to disseminate them, member and non-member countries volunteered to translate the Guidelines and several months later, they were available in Chinese, Hungarian, Italian, Norwegian, Polish, Russian, Slovak, Spanish, Swedish and Turkish. The United Nations Resolution Concerning the Creation of a Global Culture of Cybersecurity (United Nations, 2002) reflected the nine principles of the Guidelines and invited “Member States and all relevant international organizations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005”. The Guidelines were also reflected in the European Council Resolution “on a European approach towards a culture of network and information security” (European Council, 2003) and in the Asia-Pacific “Strategy to Ensure Trusted, Secure and Sustainable Online Environment” (APEC, 2005).

After the adoption of the 2002 Guidelines

29. To complete the process for the development and adoption of the Guidelines over less than a year, delegates had agreed to focus on the Principles’ section. As a result, the current Guidelines do not include a revised implementation section and the 1992 explanatory memorandum, never updated, became obsolete.

30. After 2002, the WPISP followed-up on the adoption of the Guidelines by pursuing two different streams of activities, respectively between 2002 and 2005 and after 2005.

31. Immediately after 2002 and before 2005, the OECD focused on sharing experience and best practices across member and non-member countries, and on monitoring implementation of the Guidelines. The WPISP developed an implementation plan (OECD, 2003) and BIAC published with the International Chamber of Commerce (ICC) an International Business Companion to the 2002 OECD Guidelines. The Secretariat developed a Culture of Security Web Site which included a list of national and international initiatives carried out by countries to implement the Guidelines. Norway hosted an OECD Global Forum on Information Systems and Networks Security (OECD, 2004a) with member and non-member economies, business and civil society to share information, take stock of progress made in national implementation, and discuss on expanding the culture of security. The WPISP carried out two surveys on the implementation of the Security Guidelines (OECD, 2004b, 2005a) and held a workshop jointly with APEC in Seoul, Korea, to share information, experience and best practices to develop a culture of security (OECD, 2005b).

32. After 2005, the WPISP shifted the focus to specific areas of implementation of the Guidelines, such as Critical Information Infrastructures Protection (CIIP). A comparative analysis of national CIIP policies (OECD, 2008a) led to the adoption of a Council Recommendation in 2008 (OECD, 2008b). The Working Party also developed guidance on Radio-Frequency Identification including with respect to security (OECD, 2008c). Malware (OECD, 2009) and more recently Proactive Measures by ISPs against

---

6. www.oecd.org/sti/cultureofsecurity
Botnets (OECD, 2011b) were also addressed. Finally, a comparative analysis of national cybersecurity strategies was carried out (OECD, 2011a) to explore recent evolutions of public policies in this area and to feed into the 2012 review of the Security Guidelines.

The 2007 review of the Guidelines

33. In 2007, the Working Party reviewed the 2002 Security Guidelines by way of a questionnaire circulated to WPISP delegations (OECD, 2007a) to which only eleven countries responded. No consensus emerged on the need to revise the Guidelines at that stage. Potential new concepts that emerged in the discussions were related to implementation, such as interdependent information systems and networks, research and development, and enhanced international cooperation and collaboration (between regulatory agencies on the one hand and Governments and the private sector on the other hand) in addressing threats to both the security of information systems and networks and the security of users of those systems. The importance of taking into account the linkages between information security and privacy were also highlighted (OECD, 2008d).

Considerations for the 2012 Review

34. This section provides some observations based on the above for consideration by delegates as they respond to the questionnaire. It is far from being comprehensive and aims to trigger respondents’ reflection rather than providing definitive views. It should be read in conjunction with the draft comparative analysis of cybersecurity strategies (OECD, 2011a) which provides additional elements in particular in relation to possible implementation guidance.

As regards the principles themselves

- Continued validity of the principles and potential new principles

35. It may be interesting to explore what the 2002 principles mean to today’s practitioners, whether they are still relevant to address current and emerging challenges and will remain so in the next five to ten years.

36. For example, the Response (3) principle introduces the notion of timeliness (participants should act in a timely and co-operative manner to prevent, detect, and respond to security incidents). Is “timeliness” still a relevant concept to address the current environment or should the thinking shift towards “real time” as a more appropriate notion? Going one step further, should the notion of dynamism be introduced more explicitly at the core of the thinking, explicitly discarding a static approach to security as being ineffective and inefficient in an open environment?

37. As another example, the Guidelines do not address the need to ensure business continuity including when the IT environment is degraded, or to ensure that the information system can return to an operational state quickly and easily. This is however a consequence of the switch to a risk management approach which implies that some risk has to be accepted (because it cannot be totally eliminated) and that, therefore, some incidents will happen.

7. The absence of the concept of international co-operation in the Guidelines had previously been highlighted in a paper which mapped the findings of the work on Critical Information Infrastructure Protection Policy with the principles of the Security Guidelines (OECD, 2007b). The 2008 Council Recommendation on the Protection of Critical Information Infrastructure (OECD, 2008b) addresses both domestic and international policies.

8. A concept sometimes called “resilience”, although the definitions of this term vary.
• The focus on “security of information systems and networks”

38. One of the difficulties faced by organisations to implement security in an open digital world is to change the culture from security being a technical problem for IT experts to a challenge shared by all participants according to their role. This is explicitly addressed in the Guidelines for example in the Responsibility principle (2) (*All participants are responsible for the security of information systems and networks*). However, the Guidelines’ title refers to “security of information systems and networks” as if the problem was only about securing a technical environment.

39. Concretely, the scalability challenge raised by open networks requires security to focus on the information assets as much as on the systems and networks that contain them. In an open world, it is not possible to protect everything at the highest level, therefore the level of risk carried by different categories of information assets should determine the level of security controls. However, the level of risk and required level of protection of each information asset depends on the potential business impact of these assets being successfully targeted. Assessing this impact is therefore a business responsibility rather than a technical one. The responsibility of owners of information assets is however not set out in the Guidelines, which may be a consequence of the sole focus on “security of information systems and networks”.

As regards the implementation of the principles

• Lack of implementation guidance

40. The brief narrative of the Guidelines’ history shows that the 2002 instrument focuses on the key concepts for understanding security in an interconnected world but does not address how to implement them. For example, risk analysis and risk management are placed at the core of the new mindset but the Guidelines do not provide guidance for how they should be approached.

41. The principles of the 2002 Security Guidelines are very high level: they can be used by organisations for developing a high level information security policy, by policy makers in governments to develop a national public policy/strategy and even by policy makers at the international level for guiding international co-operation. However, the lack of guidance on how to implement the principles in each of these contexts, make the Guidelines difficult to use concretely by participants. Nevertheless, OECD work since 2002 includes some building blocks that might be helpful for complementing the Guidelines’ principles with concepts for their implementation. In particular:

---

9. See above, the impact of interconnectedness on the security paradigm.

10. The choice of the “Information Systems and Networks” (ISN) language is not a neutral one and thinking about an alternative can be quite challenging. In 2002, delegates decided to extend the title of the 1992 Guidelines “for the Security of Information Systems” with a reference to networks. This had consequences with respect to the core substance of the instrument since the title reflects its scope. The remarks made in this paper do not lead to a simple solution in terms the language that can best take into account an updated thinking. In particular, the notion of “information security” which comes to mind is a source of misunderstanding as it is used in some countries with a different scope and meaning as in the OECD and should therefore be used with caution. It might be wise to draw conclusions on the terms to be used only after a consensus is reached on the concepts and scope of the Guidelines, and after carefully weighing the various language options. Interestingly, the United Nations’ Resolution which reflects the nine principles of the Guidelines calls for the “Creation of a global culture of cybersecurity” (United Nations, 2002).

11. Implementation was addressed in the implementation plan declassified by the ICCP Committee in 2003. This document was however never re-examined and its level of visibility remained relatively low.
The findings of the 2007 review of the Guidelines (OECD, 2008d), which included, as noted above, the concepts of research and development, public-private partnerships, international co-operation and linkages between security and privacy protection;

- WPISP’s work on CIIP, which provides guidance on how to implement the principles in a specific area both at domestic and cross-border levels (OECD, 2008b);

- The comparative analysis of national cybersecurity strategies which provides a direct insight into the most current national policies (see annex II and OECD, 2011a) and highlights, for example, the need for a comprehensive national strategy with appropriate leadership, government co-ordination, public-private partnerships, policies for the development of a cybersecurity industry sector and of cybersecurity skills.

Need for updated and improved contextualisation and explanations

42. The elements of contextualisation provided by the Recognising statements and Preface of the Guidelines may need some adjustment to take into account the current risk context. For example, the change in scale regarding the reliance of the economy and society on ICT and the Internet, the professionalisation of cybercriminals and the changing nature of their motivations with the emergence of state and non-state actors pursuing political objectives in cyberspace.\(^{13}\)

43. In the absence of an explanatory memorandum, the contextualisation and explanations provided in the Guidelines are limited. The Recognising statements and the Preface include some indications on the context and rationale, but do not form a sufficient basis to understand the breadth of the required change in the security mindset. For example, the Guidelines do not explain risk as a concept, or detail what a risk approach implies and why it is needed. The lack of explanations can be seen as a limiting factor in the value of the Guidelines as a practical tool for security policy making.\(^{14}\)

44. Since 2002, at operational level, many participants have maintained an approach fundamentally based on risk avoidance supported by a closed perimeter security model although the IT environment switched to openness. This inevitably led to more security incidents and tensions with business demand for such openness. In this respect, implementation guidance would help improve the applicability of the Security Guidelines’ principles by enabling the translation at a more operational level of the security paradigm shift that they establish at the highest level. Such guidance could also help use the concept of “perimeter security” as one tool among others in a risk management strategy rather than as the only option for a strategy only based on risk avoidance.

45. The lack of implementation guidance and contextualisation partly results from the fast pace adopted for the revision which required setting the implementation section and the explanatory memorandum of the 1992 Guidelines aside. It also partly results from the recognition that participants were still debating how to implement these concepts and were not ready to address them in an OECD instrument. It is likely that more can be said today on how to implement the principles based on their experience since 2002.

\(^{12}\) This report was discussed at 32\(^{nd}\) WPISP meeting in May 2012. It is being finalised based on the comments received.

\(^{13}\) For a description of the current consensus regarding the changing environment which drives the adoption of new cybersecurity strategies by governments, see OECD, 2011a.

\(^{14}\) Risk transfer, for example, is not introduced as an option.
As regards the process for the review

- A forward looking exercise

46. Figure 3 Provides a striking indicator of how visionary the OECD was in 2002 when it set the standard for information systems and networks’ security policy in an emerging interconnected world. This might partially explain the considerable interest the Guidelines raised at national and international levels. Their review ten years later should therefore aim to approach the subject matter with a similar mindset, taking into account not only the current state of play, but also key future trends. This suggests asking what, among emerging trends, will characterise the digital environment until 2022 that may impact the concepts for security and their implementation.

**Figure 3. Broadband subscription per 100 inhabitants in OECD countries in 2001 and 2011**

Source: OECD.

47. The WPISP’s comparative analysis of national cybersecurity strategies highlights some key characteristics of the current environment. In particular, such as risks faced by critical information infrastructures, make cybersecurity a challenge not just for individuals and organisations but also for the society as a whole. With the emergence of cybersecurity as a national security policy priority, what is the role of the OECD and what should be its key message? The emergence of cyberspace as a domain where tensions and conflicts between states can expand is another important trend. Other key trends include the fast expansion of wireless broadband (Figure 4), the evolution towards connectivity reaching objects such as electricity plugs and automobiles (Figure 5), or the openness of information systems supporting critical infrastructures (e.g. SCADA). These, and other trends, should be examined from the perspective of their impact on security taking into account their economic and social impacts, changing business operations within firms (e.g. value chain), commercial and other social interactions.
Note: Wireless Internet connections increased rapidly from 2001 and overtook the number of fixed broadband subscriptions around 2009. After 2009, the growth rate for wireless Internet subscriptions increased and now there are nearly twice as many wireless broadband connections (590 million) in the OECD as fixed broadband subscriptions (309 million) as of June 2011. OECD Internet Economy Outlook, Chapter 1. (OECD, 2011c).


Figure 5. Stages of Internet integration

Note: "While Internet development has clearly hit something of a stride with the expansion of connectivity to mobile devices, it is also on the cusp of a potentially much larger expansion to objects that typically did not have communication capabilities. Everything from television sets, electricity plugs, GPS devices, automobiles and even light bulbs and water levels are increasingly connected to the Internet as a way to introduce new functionality. This is the forthcoming third wave of Internet connectivity and it is expected to involve connecting a vastly larger number of objects to the Internet. This will lead to a shift from a situation where users have one (or a few) personal devices to a situation where a family may have ten to a hundred connected devices and companies may manage thousands or potentially millions of devices." OECD Internet Economy Outlook, Chapter 1.

Source: OECD, 2011c.

- Reaching out to non-members

48. The Internet Economy is a global phenomenon and reaching out to key non-members is a goal for the ICCP Committee and its Working Parties. Cybersecurity is amongst the challenges which require a global approach and international co-operation for progress to be achieved. How can non-members be associated to the review of the Security Guidelines?
How to enhance the level of information of the WPISP, if needed?

49. A key question is whether the level of information of the working party is sufficient to address the problem. For example, should the OECD solicit outside expert views to get a better understanding of the characteristics of recent evolutions and emerging new concepts that would support the review of the Guidelines? Is there a need to develop a paper on new and emerging information security concepts? Is there a need, prior to drawing conclusions of the review, to organise a workshop with members, non-members, non-governmental stakeholders and international organisations, following the example of the 2001 Tokyo workshop on “Information Security in a Networked World”?

Building on core OECD values

50. The review of the Guidelines provides an opportunity to further OECD’s international leadership in the area of national economic and social policy for cybersecurity for the years to come. It should not be perceived as an opportunity to confirm what other groups or organisations have already stated but rather to put into practice the OECD’s core values15:

- **Bold**: challenge conventional wisdom starting with our own,
- **Pioneering**: identify and address emerging and long term challenges,
- **Open**: encourage debate and a shared understanding of a critical global issue,
- **Objective**: develop analyses and recommendations that are independent and evidence-based,
- **Ethical**: Our credibility is built on trust, integrity and transparency.

15. See www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html.
REFERENCES

APEC (2005), APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment. Available at www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.ashx


OECD (1992), Recommendation of the Council Concerning Guidelines for the Security of Information Systems. Available at www.oecd.org/document/19/0,2340,en_2649_34255_1815059_119820_1_1_1_1,00.html


OECD (2009), Computer Viruses and Other Malicious Software: A Threat to the Internet Economy.


OECD (2011c), Internet Economy Outlook. ICT developments supporting the Internet. [DSTI/ICCP/IE(2011)13/CHAP1]