SHARE MORE THAN TECHNOLOGY

proximus NXT cybersecurity

NISDUC

4th NISDUC Conference: building a strong and trusted cybersecurity & NIS2 community towards informed governance

Break-out session 1 - Experience sharing of implementing security measures

From diagnosis to action: How a survey on SMEs informs on NIS2 implementation by identifying gaps to build a winning strategy

Luxembourg, 06th May 2025

Cédric Mauny
Strategic Advisor, Cybersecurity

Sensitivity: PUBLIC

Cisco

Country Digital Acceleration



- Global program that aims at collaborating with government and private sector leaders to build sustainable, secure, and inclusive communities powered by ethical and innovative technology solutions
  - 50+ countries granted with CDA programs
  - 1600+ active, completed, or upcoming projects

- Luxembourg is part of this global program with two CDA signed in 2018 then renewed in 2023 with a scope that fits to Luxembourg's digital strategy
  - Education (2018+2023)
  - Cybersécurité (2018+2023)
  - IoT (2018+2023)
  - Fintech (2018+2023)
  - Sustainability (2023)

Education
Fostering innovation, skills, and education to close skills gaps and empower the workers of today and tomorrow

Sustainability
Addressing environmental challenges across the supply chain, products, and operations, to drive shared global net-zero goals and sustainable stewardship

Critical infrastructure
Improving public safety and operational efficiency by connecting structures and facilities, including buildings, roads, and power supply

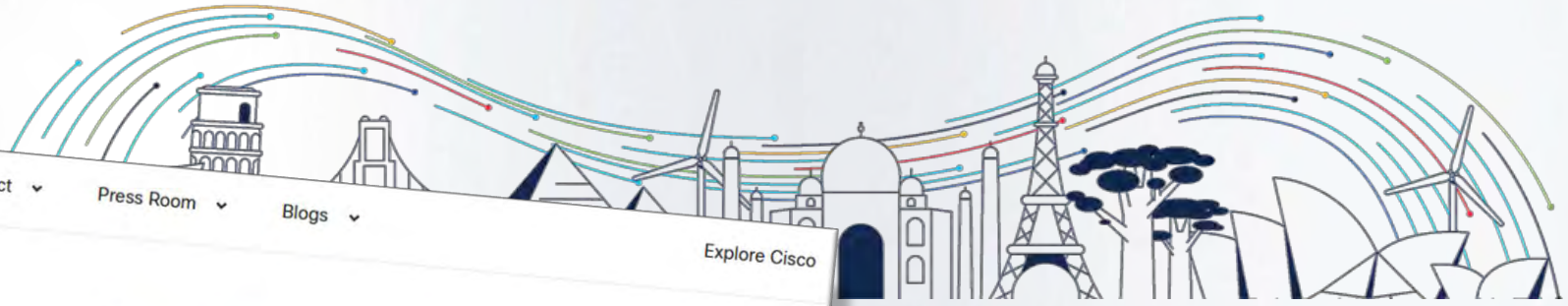
Smart communities
Using digital technology to connect, protect, and enhance the lives of all residents and build resilient communities

Healthcare
Moving healthcare and patient care forward with security and accessibility at the core

Cybersecurity
Protecting vulnerable groups by securing systems, networks, and programs from digital attacks

Cisco

Co… Digital
A…



- Glo… …d private sector leaders to build sus… …nd innovative technology solutions
  -
  -
- Lu… in… L…
  -
  -
  - Sustainability (2023)



CISCO The Newsroom Innovation Impact Press Room Blogs Explore Cisco

Press Release

Luxembourg to Accelerate Digitization with Cisco

Jan 23, 2018

LinkedIn
Twitter
Facebook

Davos (Switzerland), 23 January 2018

The Luxembourg government and Cisco have signed a Memorandum of Understanding today in Davos, Switzerland, to speed up digitization in the Grand Duchy. In line with the 'Digital Luxembourg' initiative, which is the cornerstone of the country's digital policy roadmap, the government and Cisco intend to concentrate on four pillars: education, cybersecurity, the Internet of Things and fintech.

"Luxembourg has the ambition to be a digital leader in Europe", says Prime minister Xavier Bettel. "Therefore we need to be at the forefront of technological development in order to embrace the acceleration in digitization. Luxembourg aims at attracting additional major investments allowing the digital conversion of our industry. We are happy to partner up with Cisco in order to further develop the digital innovation and the competitiveness of our country, which goes hand in hand with the creation of new jobs and will at the same time provide job security to existing ones. By modernising our education, we are going to encourage citizens to actively participate in the digital economy."



Cisco

Co… Dig…
A…

- Glo… sector leaders to build sus… …ive technology solutions
  - …kills, and education to close skills gaps and empower the workers of today and tomorrow
  - …al challenges across the supply chain, products, and operations, to drive shared global net- …e stewardship
- Lu… in… L… …ture
  - …d operational efficiency by connecting structures and facilities, including buildings, roads,
  - …s
  - …onnect, protect, and enhance the lives of all residents and build resilient communities
  - …care forward with security and accessibility at the core
  - …securing systems, networks, and programs from digital attacks



CISCO The Newsroom Inn…

Press Release

Luxembourg t… Accelerate Dig… with Cisco

Jan 23, 2018

LinkedIn
Twitter
Facebook

Davos (Switzerland), 23 J…

The Luxembourg governm… Switzerland, to speed up d… which is the cornerstone of… concentrate on four pillars: e…

"Luxembourg has the ambitio… we need to be at the forefront… digitization. Luxembourg aims… our industry. We are happy to p… competitiveness of our country, … time provide job security to exist… citizens to actively participate in t…

PAPERJAM
BUSINESS ZU LËTZEBUERG

RECHERCHER

DEPUIS LE FORUM ÉCONOMIQUE MONDIAL

Cisco veut accélérer le «Digital Lëtzebuerg»

Partager

Écrit par Thierry Raizer
Publié le 23.01.2018 • Édité le 23.01.2018 à 17:28

L'internet des objets est un des quatre axes de travail retenus pour signer cet accord. (Photo: Ministère d'État)

Au Forum économique mondial, qui a pour objet cette année la définition de nouveaux rapports économiques dans la mouvance de la «shared economy», Cisco et le gouvernement luxembourgeois viennent d'annoncer un accord qui pourrait faire date.

Les deux parties viennent en effet de s'accorder par un protocole d'entente sur une collaboration dans le cadre de la numérisation du pays, en prolongement de l'initiative «Digital Lëtzebuerg».

TOP
RECOMMANDÉS

1 INSTITUTIONS L'émigration luxembourgeoise: le point de vue historique
2 MARCHÉS FINANCIERS L'or brille, les autres valeurs refuges ternissent
3 SERVICES & CONSEILS Marco Houwen (Zentrapreneur): «Je ne savais plus où j'allais»
4 CULTURE Dix rendez-vous à ne pas manquer ce week-end
5 FOODZILLA Benoit Potdevin, l'insatiable chef du K

- Sustainability (2023)

Cisco

Co… Dig…
A…

- Glo… …uild
  sus… …ns
  -
  -
- Lu…
  in…
  L…
  -
  -
- Sustainability (2023)


CISCO The Newsroom Inno…

Press Release

Luxembourg t… Accelerate Dig… with Cisco

Jan 23, 2018

LinkedIn
Twitter
Facebook

Davos (Switzerland), 23 J…

The Luxembourg governm… Switzerland, to speed up d… which is the cornerstone of… concentrate on four pillars: e…

"Luxembourg has the ambitio… we need to be at the forefront… digitization. Luxembourg aims… our industry. We are happy to p… competitiveness of our country, … time provide job security to exist… citizens to actively participate in t…

RECHERCHER

PAPERJAM
BUSINESS ZU LËTZEBUERG

DEPUIS LE FORUM ÉCONOMIQUE MONDIAL

Cisco veut accélérer … Lëtzebuerg»

Écrit par Thierry Raizer
Publié le 23.01.2018 • Édité le 23.01.2018 à 17:28

L'internet des objets est un des quatre axes de travail retenus pour sig… Ministère d'État)

Au Forum économique mondial, qui a pour objet cet… nouveaux rapports économiques dans la mouvance … Cisco et le gouvernement luxembourgeois viennent … qui pourrait faire date.

Les deux parties viennent en effet de s'accorder par… sur une collaboration dans le cadre de la numérisati… prolongement de l'initiative «Digital Lëtzebuerg».

DIGITAL ENERGY SOLUXIONS

CISCO RESIGNE AVEC DIGITAL LUXEMBOURG

Jan 19, 2023 | Data Center | 0 commentaires

DANS LE CADRE DE SON PROGRAMME COUNTRY DIGITAL ACCELERATION, CISCO RÉITÈRE SON SOUTIEN À DIGITAL LUXEMBOURG, LE MOUVEMENT DE NUMÉRISATION À LONG TERME DU GRAND-DUCHÉ.

Cisco

PAPERJAM
BUSINESS ZU LËTZEBUERG

RECHERCHER

ENTREPRISES & STRATÉGIES - TECHNOLOGIES

RENAUD PERSIANI (CISCO)

«Donner une nouvelle dynamique» à la digitalisation du Luxembourg

Partager

Écrit par Mathilde Obert
Publié le 19.01.2023 • Édité le 19.01.2023 à 10:57



Renaud Persiani, country manager de Cisco Luxembourg, détaille les enjeux du MoU signé entre le gouvernement luxembourgeois et l'entreprise informatique américaine. (Photo: Catherine Herpeux/ Cisco Luxembourg)

Le Luxembourg a signé un nouvel accord avec Cisco, lors du Forum économique mondial à Davos, pour la digitalisation du Luxembourg. Il s'articule autour de trois axes: la cybersécurité, l'enseignement et le développement des talents, ainsi que la durabilité.

TOP RECOMMANDÉS

1 INSTITUTIONS
L'émigration luxembourgeoise: le point de vue historique

2 MARCHÉS FINANCIERS
L'or brille, les autres valeurs refuges ternissent

3 SERVICES & CONSEILS
Marco Houwen (Zentrapreneur): «Je ne savais plus où j'allais»

4 CULTURE
Dix rendez-vous à ne pas manquer ce week-end

5 FOODZILLA
Benoit Potdevin, l'insatiable chef du K

Les deux parties viennent en effet de s'accorder par
sur une collaboration dans le cadre de la numérisati
prolongement de l'initiative «Digital Lëtzebuerg».

DIGITAL ENERGY
SOLUXIONS

CISCO RESIGNE AVEC DIGITAL LUXEMBOURG

Jan 19, 2023 | Data Center | 0 commentaires



DANS LE CADRE DE SON PROGRAMME COUNTRY DIGITAL ACCELERATION, CISCO RÉITÈRE SON SOUTIEN À DIGITAL LUXEMBOURG, LE MOUVEMENT DE NUMÉRISATION À LONG TERME DU GRAND-DUCHÉ.

Cisco

RECHERCHER

PAPERJAM
BUSINESS ZU LËTZEBUERG

cisco The Newsroom

ENTREPRISES & STRATÉGIES - TECHNOLOGIES

RENAUD PERSIANI (CISCO)

«Donner une nouvelle dynamique» à la digitalisation du Luxembourg

Partager

Écrit par Mathilde Obert
Publié le 19.01.2023 • Édité le 19.01.2023 à 10:57



Renaud Persiani, country manager de Cisco Luxembourg, détaille les enjeux du MoU signé entre le gouvernement luxembourgeois et l'entreprise informatique américaine. (Photo: Catherine Herpeux/ Cisco Luxembourg)

Le Luxembourg a signé un nouvel accord avec Cisco, lors du Forum économique mondial à Davos, pour la digitalisation du Luxembourg. Il s'articule autour de trois axes: la cybersécurité, l'enseignement et le développement des talents, ainsi que la durabilité.

TOP RECOMMANDÉS

1 INSTITUTIONS L'émigration luxembourgeoise de vue historiqu

2 MARCHÉS FINANCIERS L'or brille, les refuges ternis

3 SERVICES & CONS Marco Houv (Zentrapre savais plus

4 CULTURE Dix rende manquer

5 FOODZILLA Benoit chef d

Les deux parties viennent e
sur une collaboration dans le cadre de la
prolongement de l'initiative «Digital Lëtzebuerg».

RECHERCHER

PAPERJAM
BUSINESS ZU LËTZEBUERG

C.1.1.5.1 Signature d'un Memorandum of Understanding avec CISCO

Le 23 janvier 2018, à l'occasion du World Economic Forum à Davos en Suisse, le Gouvernement a signé un Memorandum of Understanding (« MoU ») avec CISCO. Cet accord prévoit notamment l'instauration du « Country Digital Acceleration » Plan (« CDA ») de CISCO au Luxembourg.

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Rapport d'activité 2018

Le CDA de CISCO est une initiative à travers laquelle la société met à disposition son savoir-faire ainsi que l'infrastructure technique pour les besoins de connectivité via réseaux numériques aux pays participants afin de les soutenir dans leur transition digitale. CISCO a déjà conclu ce partenariat avec une quinzaine de pays (dont les États-Unis, la France, l'Allemagne, le Royaume-Uni, les Pays-Bas, le Danemark, l'Italie, l'Inde, le Mexique et la Chine), mais l'envergure et le contenu spécifique du programme sont adaptés aux besoins de chaque pays participant.

Au Luxembourg, le CDA prévoit notamment une coopération sur les grands axes suivants :

- l'éducation et les e-skills (coopération avec l'Université du Luxembourg, Cisco NetAcademy) ;
- la cybersécurité ;
- l'Internet of Things (IoT) ;
- le FinTech.

Plusieurs projets ont vu le jour depuis la signature du MoU en janvier 2018. D'ailleurs, tous ces projets sont réalisés par des partenaires sur le terrain qui peuvent dès lors bénéficier de l'expertise de CISCO grâce à l'instauration du CDA au Luxembourg.

DANS LE CA
SOUTIEN À DIGITAL LUXEMBOURG,
DUCHÉ.

uild
ns
f today and tomorrow
drive shared global net-
luding buildings, roads,
resilient communities
ITÈRE SON
ME DU GRAND-

proximus NXT cybersecurity

Cisco

Country Digital Acceleration



- Proximus NXT, previously known as Telindus, has been selected as partner for the cybersecurity digitization verticals

- Project was proposed to address and assess the gap for SMEs against NIS2
  - Creation of a questionnaire to survey the gap of SMEs against the ten technical requirements from the Article 21 of the Directive NIS2
  - Joint event with CISCO for disseminating the concept of the event and call for interest to take part (on March 21st 2024)
  - Face-to-face interviews to fill out the questionnaire with the IT responsible person, CIO or CISO (from June to July 2024)
  - Publication of a personalized report on the critical items and recommendations to meet the technical key requirements

- Financing Details and rules of disclosure
  - CISCO financially supported the performance of the whole process
  - Customers who took of the CDA were informed on the involvement of CISCO in the process
  - CISCO was aware of the participants' customer but never received any report / weaknesses on individual participants, only the overall results

Education
Fostering innovation, skills, and education to close skills gaps and empower the workers of today and tomorrow

Sustainability
Addressing environmental challenges across the supply chain, products, and operations, to drive shared global net-zero goals and sustainable stewardship

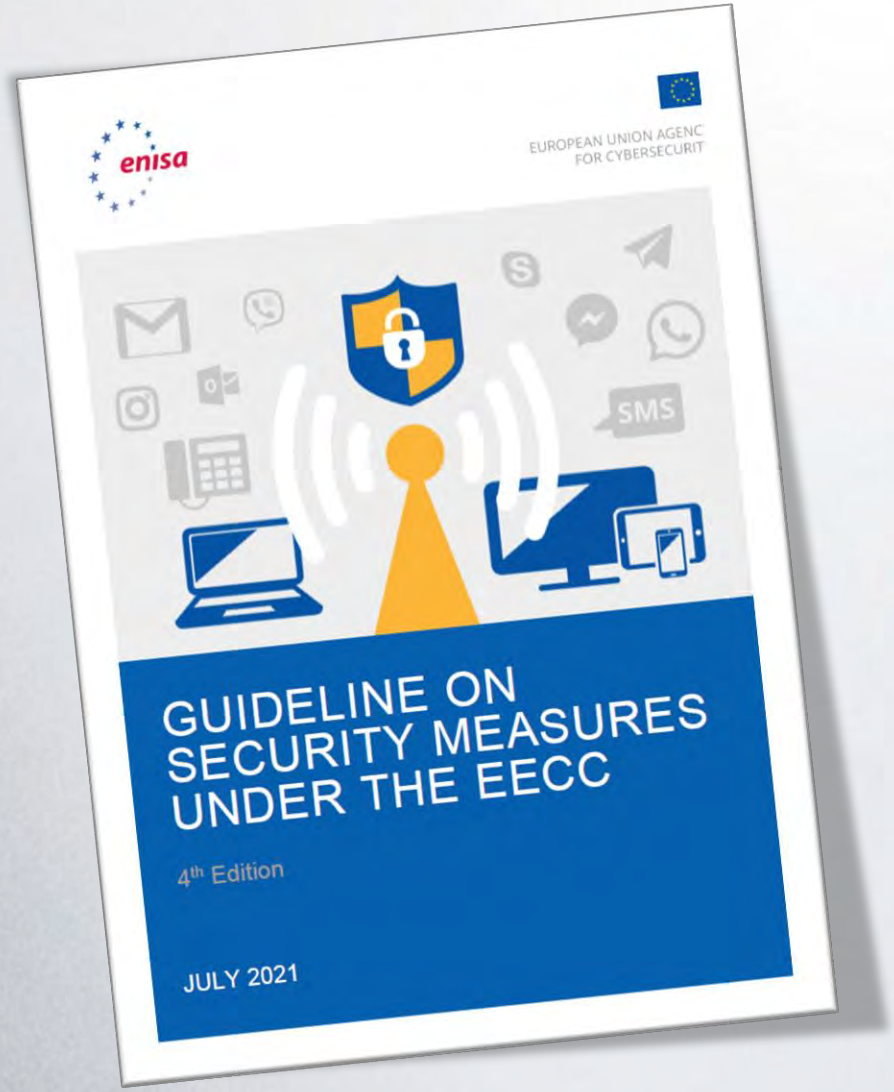
Critical Infrastructure
Improving public safety and operational efficiency by connecting structures and facilities, including buildings, roads, and power supply

Smart communities
Using digital technology to connect, protect, and enhance the lives of all residents and build resilient communities

Healthcare
Moving healthcare and patient care forward with security and accessibility at the core

Cybersecurity
Protecting vulnerable groups by securing systems, networks, and programs from digital attacks

Creation of a survey-questionnaire based on ENISA guidelines to assess the gap of SMEs against the ten technical requirements from the Dir. Art. 21 / Projet de Loi LU Art. 12





- Based on the Proximus NXT expertise, the default guidelines were augmented
  - to address the 10 requirements from the Article 21 of the Directive / Article 12 of the PL, and
  - considering ISO 27002 best practices

proximus NXT cybersecurity

Creation of a survey-questionnaire based on ENISA guidelines to assess the gap of SMEs against the ten technical requirements from the Dir. Art. 21 / Projet de Loi LU Art. 12

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

It was key to address the 10 security requirements from the Directive / Projet de Loi

INSTITUT LUXEMBOURGEOIS DE RÉGULATION

Art. 12. (1) Les entités essentielles et importantes prennent les mesures techniques, opé
et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la
réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activi
fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les in
sur les destinataires de leurs services et sur d'autres services.

Les mesures visées au à l'alinéa 1er garantissent, pour les réseaux et les systèmes d'info
niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a
lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors
de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré
d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents
et de leur gravité, y compris leurs conséquences sociétales et économiques.

Afin d'identifier les risques, les entités essentielles et importantes utilisent un cadre d'analyse de
risques approprié pouvant être précisé par l'autorité compétente concernée par voie de règlement ou
de circulaire.

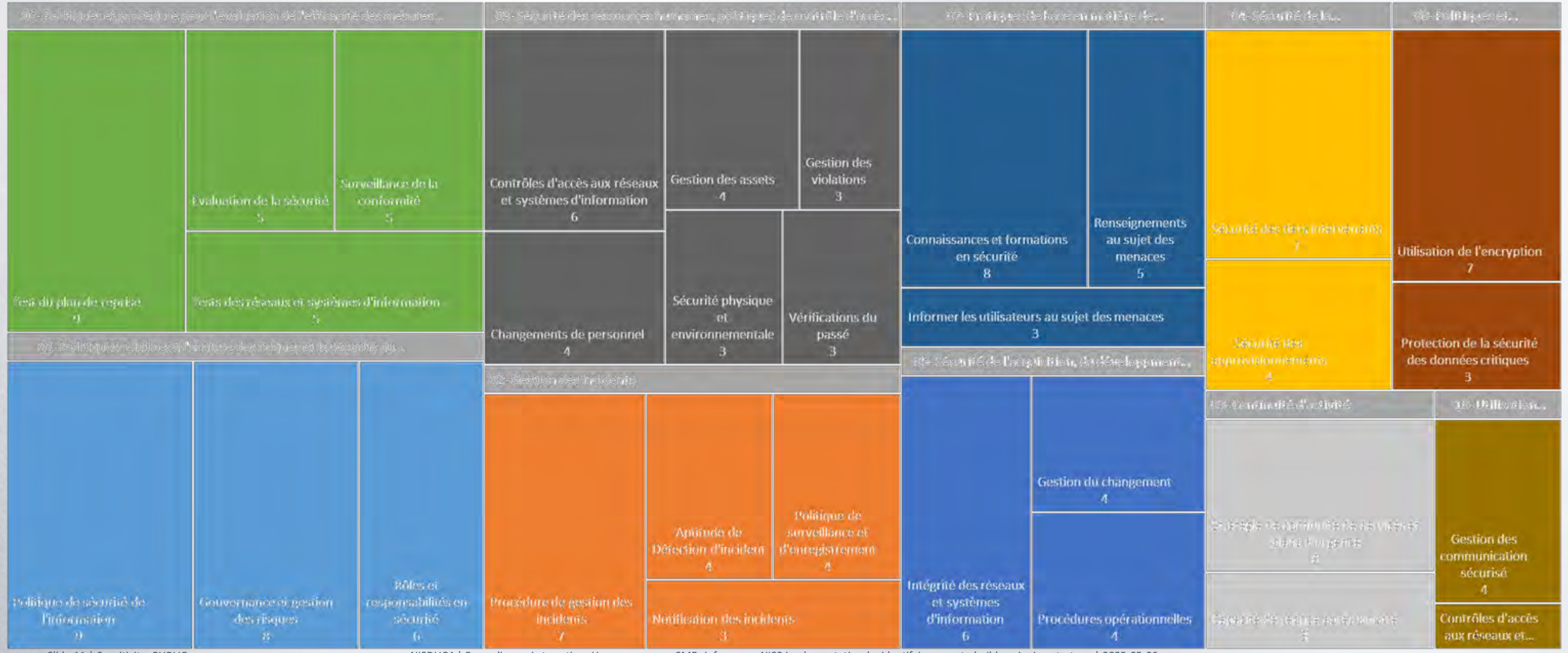
(2) Les mesures visées au paragraphe 1er sont fondées sur une approche « tous risques » qui vise à
protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les
incidents, et elles comprennent au moins :

1° les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ;
2° la gestion des incidents ;
3° la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises ;
4° la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ;
5° la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;
6° des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
7° les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité ;
8° des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
9° la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;
10° l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

(3) Les mesures prises par les entités essentielles sur base des paragraphes 1er et 2 sont notifiées à l'autorité compétente. Les modalités de cette notification, le format et le délai, sont déterminées par l'autorité compétente concernée par voie de règlement ou de circulaire.

Creation of a survey-questionnaire based on ENISA guidelines to assess the gap of SMEs against the ten technical requirements from the Dir. Art. 21 / Projet de Loi LU Art. 12

10 domains → 31 sub-domains → 153 questions



proximus NXT cybersecurity

Each respondent received a personalised report > Global results

Conformity scale

Conformity	Description
Conform	The organisation covers the security objective requirement
Partially conform	Minor gap, the organisation only partially meets the requirements of the security objective.
Not compliant	Major gap, security objective requirements not met

Covering rate NIS2

Qualification	
0 - 50%	Major gap requiring special attention, Significant number of actions required to bring the security objective into conformity
51 - 90%	Moderate gap, Actions required to bring the security objective into conformity
91-100%	Security objective reached or minor actions required to bring the security objective into conformity

NIS 2 requirements domain	Maturity
1. Policies on risk analysis and information system security	38,00%
2. Incident handling	44,00%
3. Business continuity	16,00%
4. Supply chain security	22,00%
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	24,00%
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	38,00%
7. Basic cyber hygiene practices and cybersecurity training	42,00%
8. Policies and procedures regarding the use of cryptography	25,00%
9. Human resources security, access control policies and asset management	28,00%
10. Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	48,00%



Echelle de conformité

Conformité	Description
Conforme	L'organisme couvre l'exigence de l'objectif de sécurité
Partiellement conforme	Écart mineur, l'organisme ne couvre qu'en partie les exigences de l'objectif de sécurité
Non conforme	Écart majeur, les exigences de l'objectif de sécurité ne sont pas respecté

Taux de couvertures NIS2

Qualification	
0 - 50%	Écart majeur nécessitant une attention particulière, Nombres importants d'actions demandée pour la remise en conformité de l'objectif de sécurité
51 - 90%	Écart modéré, Actions demandées pour la remise en conformité de l'objectif de sécurité
91-100%	Objectif de sécurité atteint ou actions mineures demandés pour la remise en conformité de l'objectif de sécurité

proximus NXT cybersecurity

Each respondent received a personalised report > Detailed statements

Domain d'exigence NIS 2	Sub-Domain	Question ID	Question	Answer	Remark
1- Policies on risk analysis and information system security	Information security policy	Q1	Is an information security policy in place?	Conform	
1- Policies on risk analysis and information system security	Information security policy	Q2	Are the organization's security objectives defined?	Conform	
1- Policies on risk analysis and information system security	Information security policy	Q3	Does the policy scope include networks and related services?	Conform	
1- Policies on risk analysis and information system security	Information security policy	Q4	Are critical assets identified and defined in the policy scope?	Partially conform	Criteria to identify critical asset is not formalise
1- Policies on risk analysis and information system security	Information security policy	Q5	Is it communicated to the company's staff?	Partially conform	Information security policy is accessible by staff but no communication about reading the information security policy
1- Policies on risk analysis and information system security	Information security policy	Q6	Does the staff know what it implies for their work?	Not compliant	
1- Policies on risk analysis and information system security	Information security policy	Q7	Is it approved by management?	Conform	
1- Policies on risk analysis and information system security	Information security policy	Q8	Does it mention applicable laws and regulations?	Not compliant	
1- Policies on risk analysis and information system security	Information security policy	Q9	Is the policy reviewed periodically and/or after a change or incident?	Conform	
1- Policies on risk analysis and information system security	Governance and risk management	Q10	Do you have a list of your main risks to network and service security?	Partially conform	Risk analysis done but not up to date (last review in 2015)
1- Policies on risk analysis and information system security	Governance and risk management	Q11	Does it contain the main threats and their potential impacts on critical assets?	Partially conform	Risk analysis done but not up to date
1- Policies on risk analysis and information system security	Governance and risk management	Q12	Is the staff aware of the main risks and how to mitigate them	Partially conform	
1- Policies on risk analysis and information system security	Governance and risk management	Q13	Are the risks re-evaluated periodically and/or after a change or incident?	Not compliant	
1- Policies on risk analysis and information system security	Governance and risk management	Q14	Are the residual risks approved by management ?	Conform	
1- Policies on risk analysis and information system security	Governance and risk management	Q15	Are the risk management methodology and/or tool based on a standard?	Not compliant	

Each respondent received a personalised report > Recommendations

ID	Domain	Sub-Domain	Recommendation	Type	Requirement processed
1	1- Policies on risk analysis and information system security	Information security policy	Define in the information security policy: - critical asset in the scope - applicable laws and regulations	Organizational	Q4, Q8
2	1- Policies on risk analysis and information system security	Information security policy	Share the information system security policy with employees	Organizational	Q5, Q6
3	1- Policies on risk analysis and information system security	Governance and risk management	Conduct a risk analysis using a methodology based on a standard.	Organizational	Q10, Q11
4	1- Policies on risk analysis and information system security	Governance and risk management	Raise awareness among stakeholders about the different levels of risk and how to mitigate them.	Organizational	Q12
5	1- Policies on risk analysis and information system security	Governance and risk management	Formalize the operations surrounding risk management in a policy (methodology and/or tool used, treatment of measures, committee in charge of reviewing risks, etc.)	Organizational	Q13, Q16
6	1- Policies on risk analysis and information system security	Security roles and responsibilities	Formalize a document that: - Defines the roles and responsibilities related to information security (RACI Matrix). - List of specifying who holds these roles and their contact details	Organizational	Q19, Q20
7	1- Policies on risk analysis and information system security	Security roles and responsibilities	Review and update the roles and responsibilities document periodically or when a change occurs.	Organizational	Q23
8	2- Incident handling	Incident management procedures -- Incident detection capability	Develop an incident management policy and procedures compliant with NIS2, defining reporting, types of incidents, objectives, roles and responsibilities,	Organizational	Q26, Q36
9	2- Incident handling	Incident management procedures	Communicate and raise awareness about the incident management policy and procedures to stakeholders.	Organizational	Q27
10	2- Incident handling	Incident management procedures -- Incident detection capability	Review and update the incident management documents periodically or in case of a major change.	Organizational	Q28, Q37
11	2- Incident handling	Monitoring and logging policies	Develop a logging management policy and a monitoring procedure for critical systems, describing the minimum requirements, retention periods, and objectives for storing monitoring data and logs.	Organizational	Q40

The survey

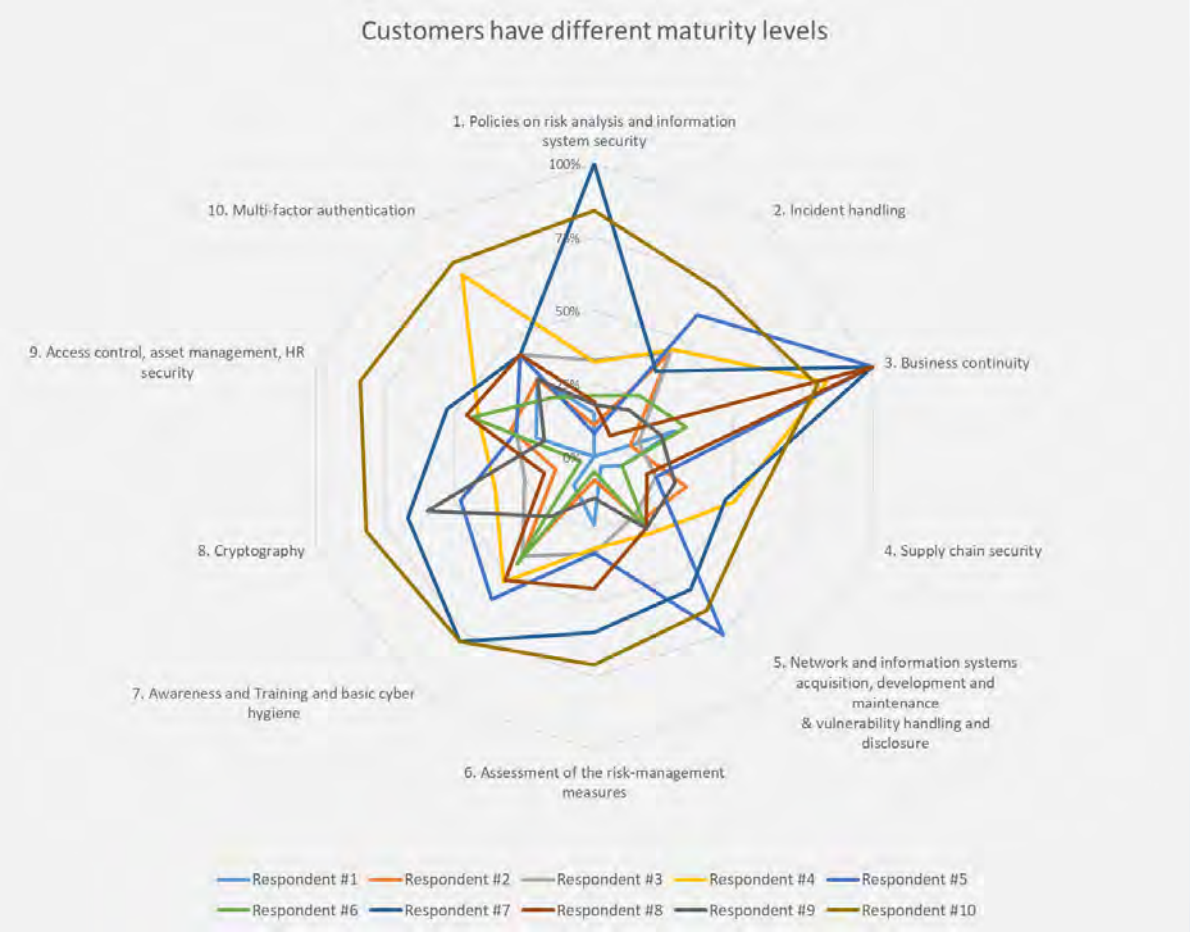
10 customers from 7 economic sectors

SECTORS OF HIGH CRITICALITY

- A1. Energy (1x)
  - A1a. Electricity
- A2. Transport (2x)
  - A2a. Air
  - A2d. Road
- A9. ICT service management (1x)

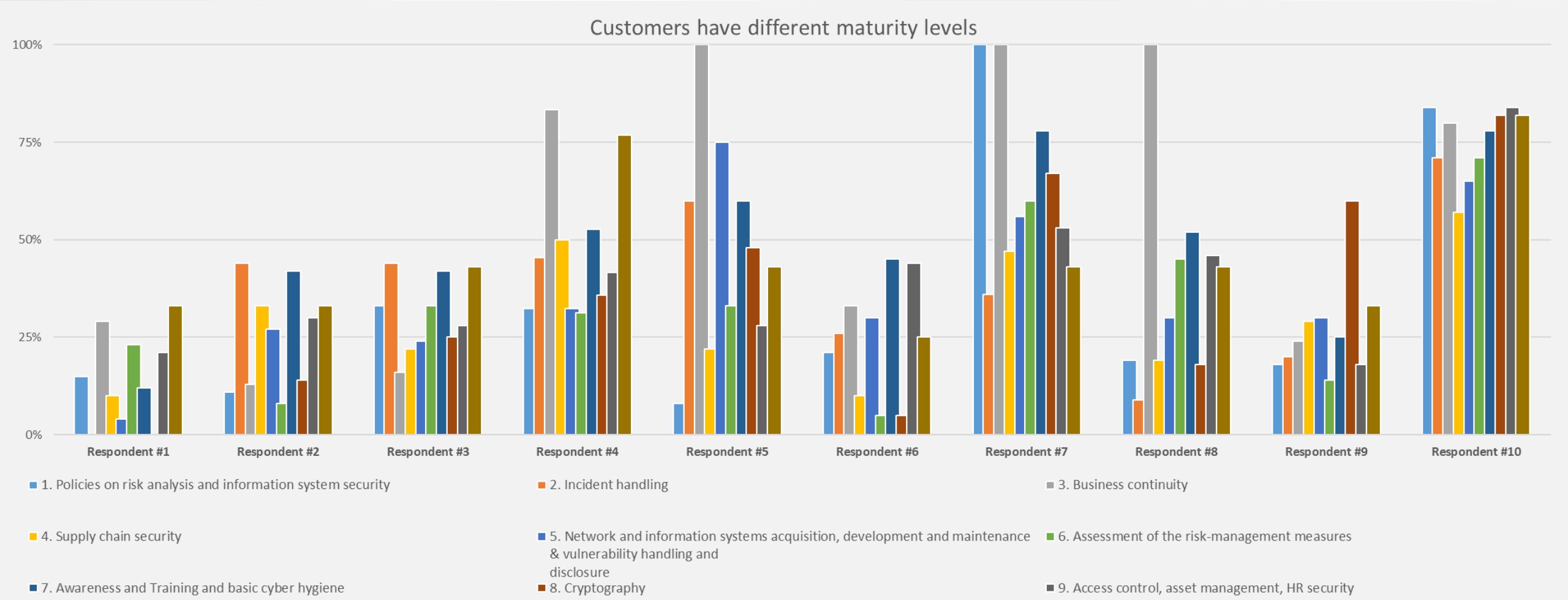
OTHER CRITICAL SECTORS

- B2. Waste management (1x)
- B3. Manufacture, production and distribution of chemicals (2x)
- B4. Production, processing and distribution of food (2x)
- B5. Manufacturing (1x)
  - B5a. Manufacture of medical devices and in vitro diagnostic medical devices

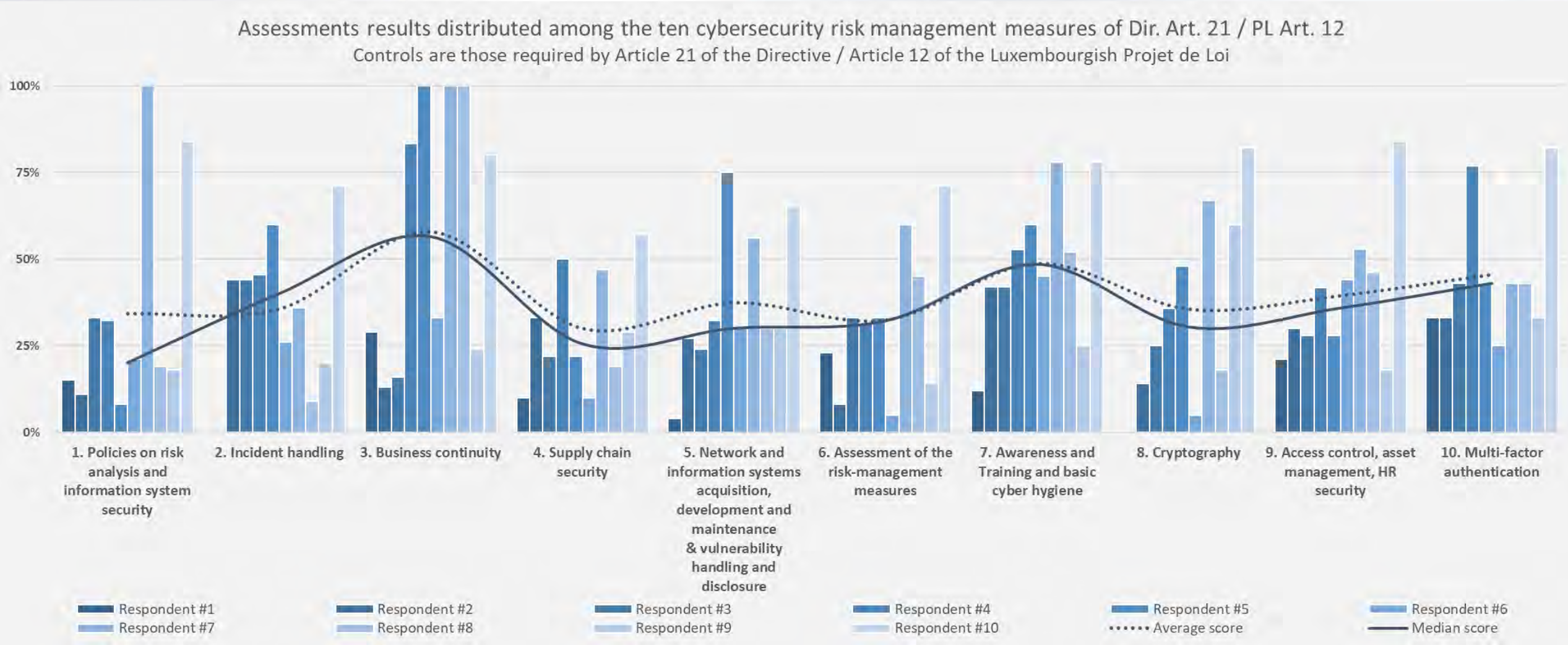


proximus NXT cybersecurity

Maturity levels are different per customers…
All need support in securing their digital journey and for supporting their compliance

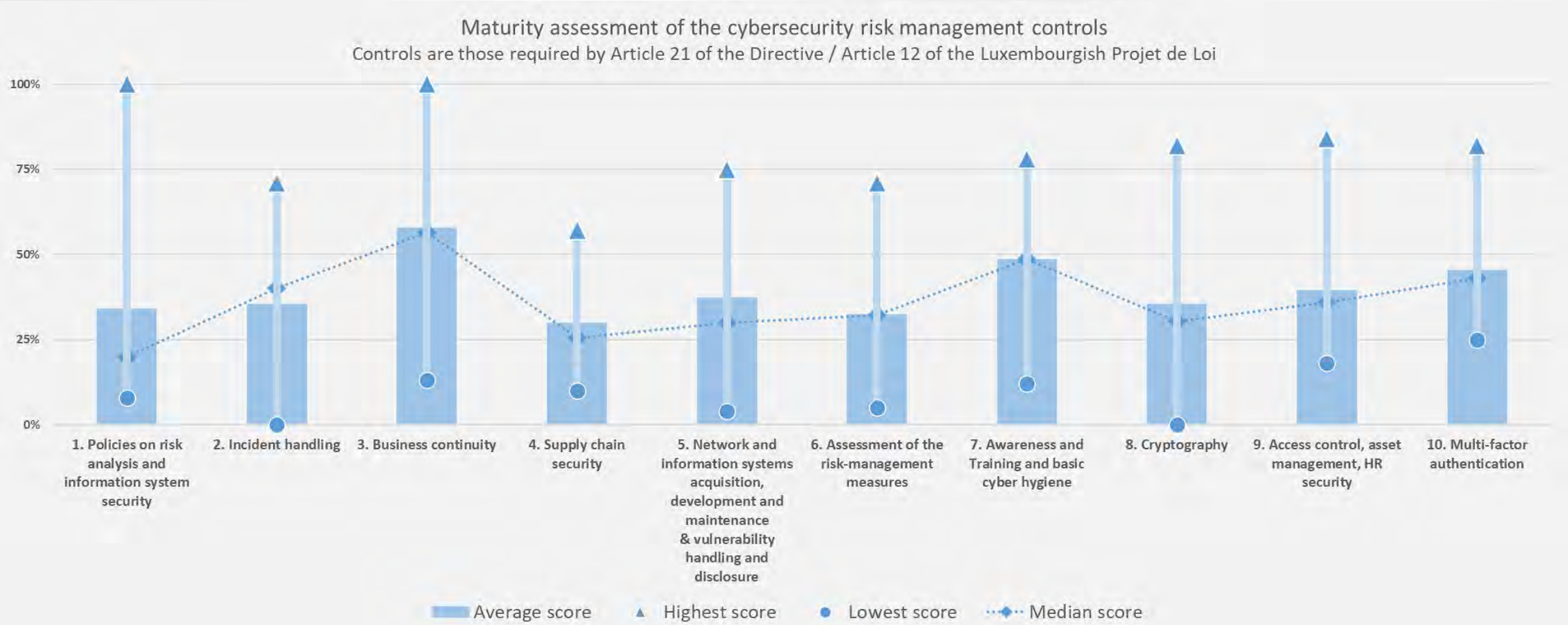


Global view on results per cybersecurity risk management controls for each customer along with average and median maturity level

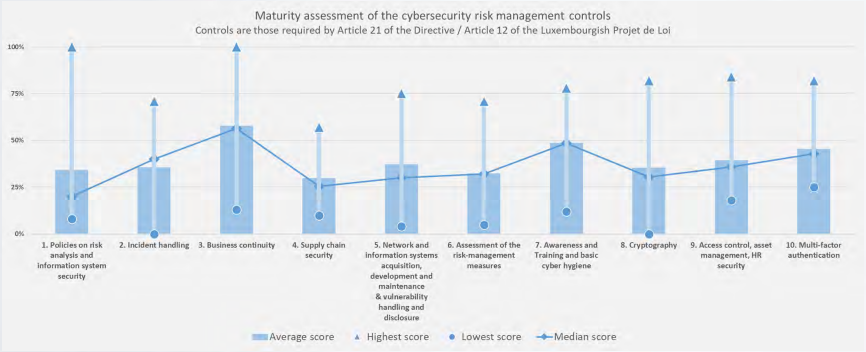


proximus NXT cybersecurity

Global view on results per cybersecurity risk management controls for the highest, lowest, average and median maturity level



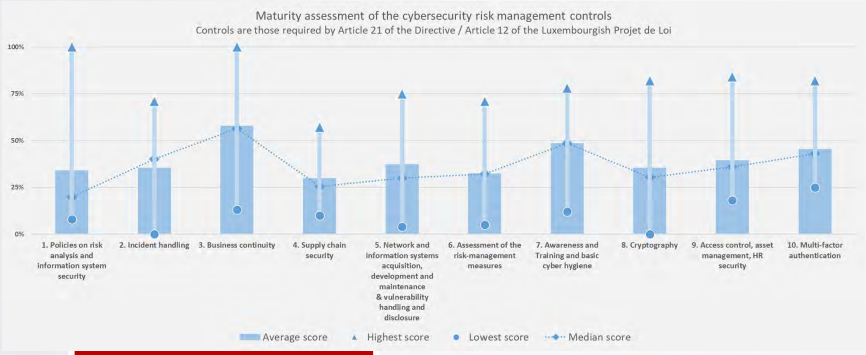
Global view on results (anonymised) per cybersecurity risk management controls



- Maturity level is globally average/low
  - Global average/median maturity below 50%
    - Except business continuity…

- Business Continuity: 3 Customers have been assessed at 100% of maturity score
  1. Recently suffered from major incidents and therefore developed a strong business continuity capabilities… after the incident
  2. Outsourced all their IT to a third-party… which is already regulated
  3. Already regulated customer

Global view on results (anonymised) per cybersecurity risk management controls



- **MFA implementation**
  - One of the highest maturity score… but not sufficient to ensure right security protection
  - Globally less then 50% of maturity
  - Quick-wins already identified to improve the situation and “easy” to implement
- **Awareness, basic cyber hygiene practices and cybersecurity training**
  - Everyone is doing awareness but is it effective?
- **Incident handling**
  - Some of respondents suffered from incident recently… they are now prepared…

- **Policies on risk analysis and information system security**
  - Lack of documentation is a weak point shared by many SMEs
  - Global lack of practices in the risk management field
- **Supply chain security**
  - Globally the lowest maturity level
  - Maturity level is the lowest and the most grouped one
- **Cryptography**
  - Documentation is missing
  - Need to enforce some (good) practices
- **Incident Handling**
  - This requires technical investments (log management and monitoring, alerting, …) and processes
  - Need support from specialists in case of incident (SOC, Incident Response, …)

In the middle

- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- Human resources security, access control policies and asset management

Average of 42 recommendations per customer

proximus NXT cybersecurity

Average of 42 recommendations per customer

37 organizational and 5 technical

- 88% of organisation vs 12% of technical
  - Precise technical measures identified during assessments →
  - Organisational measures are *simple*: who is expected to do what and when
    - Document, document, document
    - RACI, RACI, RACI
    - Many of those organization controls are also linked to technical controls
      - i.e. Patching Management process or Backup Management process need technical effort

Protection of critical security data	Implement measures to secure access to secret data (cryptographic keys and authentication information)
Use of encryption	Implement or activate encryption solutions for communication and storage flows identified as needing encryption.
Training and awareness	Test personnel knowledge regarding information security (phishing session, questionnaire)
Security evaluation	Carry out penetration tests at regular intervals
Management of secure communication	Implement secure emergency communication solutions, such as encrypted messaging systems, secure voice and video communication platforms, and emergency notification applications.
Network and information systems testing	Use automated testing tools for the identification of vulnerabilities (e.g. vulnerability scan…)
Incident detection capability	Implement an incident detection and reporting system (SIEM, SOC, NOC) for collecting, storing logs, and monitoring critical systems to centralize the collection, storage, and analysis of logs from critical systems
Threat intelligence	Establish mechanisms for collecting information for threat intelligence
Recovery plan testing	Carry out DRP/BCP tests with an end-of-test report to evaluate the business recovery plan
Network and information systems testing	Use tools to perform regular and thorough tests, allowing early detection of problems and more effective change management.
Access controls to networks and information systems	Implement MFA

Opportunities

- **Surveyed CISO / CIO / IT Manager are aware of most of their weaknesses, they "only" need**
  - support to push on their projects
  - resources to document the processes… and execute the activities
  - to be aware of new threat trends and get support for "hot topics"

- **Risk-based practices are not generalized**
  - Common sense is the rule
    - But common sense may have some weaknesses like difficulty of prioritisation
  - Generic risks landscape is needed to support companies who are not experienced in the field

    → Share (best) practices within sectoral ISAC

- **Security Awareness is mandatory for all staff**
  - *All* includes the executive committee / board of directors / Conseil d'Administration
    - Their personal responsibility is at stake by NIS2

- **NIS2 is the first framework for (many) previously unregulated companies**
  - Use the Directive/Law for justifying your projects
  - Need a list of detailed "guidelines"? → COMMISSION IMPLEMENTING REGULATION (EU) 2024/2690 of 17 October 2024 → Annex *Technical and methodological requirements* referred to in Article 2 (Technical and methodological requirements) of this Regulation
  - It is no more more "the wish list of the CISO/CIO" but the requirements expressed by the law for *achieving a high common level of cybersecurity across European Union*

ILR issued a set of 6 basics security controls

- Always build on strong foundations



INSTITUT LUXEMBOURGEOIS DE RÉGULATION

6 mesures de sécurité fondamentales

SERVICE NISS

Utilisez les 6 mesures de sécurité fondamentales non seulement comme point de départ vers la conformité à la directive NIS 2, mais surtout pour vous protéger des risques et des menaces cyber toujours plus sophistiquées !

1 Gérez tous vos actifs et les risques y relatifs

(Gestion des actifs, gestion des risques, sécurité dans la chaîne d'approvisionnement)

- Créer et gérer un inventaire détaillé avec tous les actifs (logiciels, matériels, ...) y compris les actifs sous-traités
- Identifier, analyser, évaluer et traiter les risques les plus importants
- Considérer les fournisseurs et les prestataires de services dans le processus de gestion des risques
- Intégrer la sécurité dans tout le cycle de vie des actifs (sécurité par défaut)
- Surveiller et évaluer l'efficacité des mesures de gestion des risques

2 Protégez vos systèmes, réseaux et les communications

(Sécurité des systèmes et des réseaux, communications sécurisées)

- Mettre en œuvre des équipements et logiciels de sécurité (firewall, anti-virus, VPN, ...)
- Configurer les paramètres et fonctionnalités de sécurité (ports, services, protocoles, ...)
- Utiliser des solutions de cryptographie et de chiffrement
- Sécuriser vos connections WiFi et les équipements nomades (clés USB, smartphones, ordinateurs portables, ...)
- Surveiller les activités et la performance et enregistrer les événements

3 Sécurisez vos accès logiques et physiques

(Contrôle d'accès, authentification)

- Utiliser des mots de passes forts et uniques et des solutions d'authentification à plusieurs facteurs (MFA)
- Limiter les droits d'accès aux collaborateurs et aux systèmes
- Attribuer et autoriser les droits d'accès aux collaborateurs seulement sur base de leurs rôles et responsabilités
- Protéger et surveiller les accès aux environnements physiques (bâtiments, serveurs, data center, équipements, ...)
- Revoir régulièrement et, si nécessaire, modifier ou supprimer les droits d'accès

4 Gardez vos logiciels et systèmes à jour

(Gestion des vulnérabilités, gestion des correctifs et mises à jour)

- Utiliser des outils d'identification et d'analyse des vulnérabilités, tout en assurant leur suivi
- Appliquer les correctifs le plus rapidement possible, après avoir sauvegardé les données
- Surveiller les correctifs et les mises à jour publiés par les fournisseurs ou prestataires de services
- Tester et évaluer les correctifs et les mises à jour avant de les installer dans les systèmes de production
- Évaluer les impacts et les conséquences des changements envers les utilisateurs et les activités critiques de l'entité

5 Gérez vos incidents et assurez la continuité de vos activités

(Gestion des incidents, gestion de la continuité des activités)

- Réaliser régulièrement des sauvegardes des données et les tester
- Mettre en œuvre un plan pour gérer les incidents
- Mettre en œuvre un plan de continuité et de reprise des activités et le tester
- Établir et maintenir une liste des contacts clés (support technique, expertise sécurité, parties prenantes externes, ...)
- Établir et maintenir des relations avec les autorités nationales compétentes

6 Sensibilisez et formez vos collaborateurs

(Sensibilisation et formation à la cybersécurité)

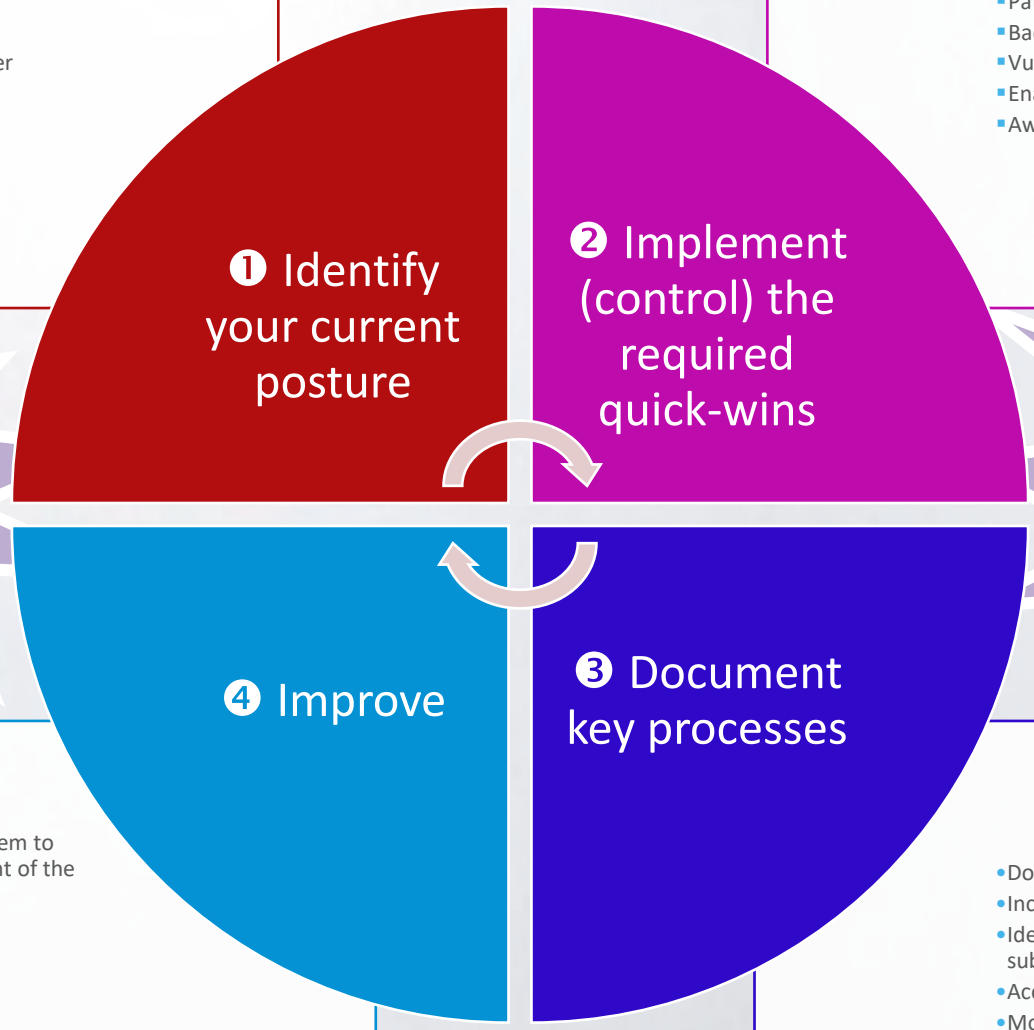
- Sensibiliser régulièrement les collaborateurs sur les menaces et les risques, ainsi que les mesures à prendre en compte
- Informer les collaborateurs et les parties tierces (consultants, fournisseurs, ...) des règles de sécurité de votre entité
- Offrir aux collaborateurs techniques (spécialistes réseaux, ...) des formations sur la sécurité en lien avec leur fonction
- Former les membres des organes de direction aux risques cyber et à leurs rôles et responsabilités
- Tester et évaluer les connaissances des collaborateurs en matière de sécurité de l'information

proximus NXT cybersecurity

How to start?

- Gap Assessment
- High-level risk analysis
- Assessment of business continuity and disaster recovery capabilities

- Patching
- Backup (and restore tests)
- Vulnerability assessment
- Enable MFA on all remote accesses
- Awareness for all staff



Security and Risk Strategie + multi-year roadmap

Support and leadership from top-management

- Start an information security management system to ensure adaptation and continuous improvement of the security approach
- Business Impact Analysis, Business Continuity Management, Disaster Recovery Plans
- Third-party (risk) management

- Document, document, document
- Incident notification process
- Identification of dependencies on subcontractors and suppliers
- Access control policy
- More precise risk analysis to prioritize action plans

proximus NXT cybersecurity

Cisco

Country Digital Acceleration



- The gap assessment project performed during the Phase 1 is part of a more global project

- The Phase 2 will start in the coming days / weeks
  - still part of the CISCO CDA framework
  - will be far more technical oriented by demonstration the capability to create a a technical environment secure and compliant by-default (as far as possible)
  - still enforcing the same confidentiality principles regarding the technical and risk specificities of individual participants

- Stay tuned for more information

Thank you

for your attention

www.proximusnxt.lu

proximus NXT cybersecurity

Questions

& Answers

Contact Information



Cédric MAUNY

cedric.mauny@proximus.lu

(+352) 621.200.707

https://www.linkedin.com/in/cedricmauny/

proximus NXT cybersecurity



proximus NXT

cybersecurity

Sensitivity: PUBLIC