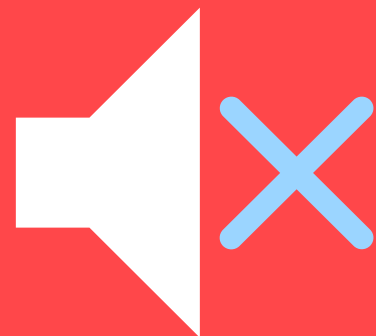


FEDIL

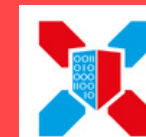
The Voice of Luxembourg's Industry

WHY CYBERSECURITY MATTERS MORE THAN EVER



*Sound is off until the conference
starts at 10AM*

22 | 10 | 2020



CYBERSECURITY WEEK
19//29 OCTOBER 2020



WELCOME WORDS

*Jean-Louis Schiltz,
Vice-Chairman, FEDIL - Chairman of FEDIL-Digital & Innovation Board Group*



PRESENTATION OF THE ISAC CONCEPT

*François Thill,
Director e-commerce and information security, Ministry of the Economy*



The ISAC concept

*François Thill, Director cybersecurity,
Ministry of the Economy.*



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie



- ISAC
- Information sharing
- Adding context



Information **S**haring and **A**nalysis **C**entre

Cyber security is a process, not a product

**The ISAC is a secure channel/place to
broaden the view and increase
understanding in cybersecurity together
with peers**



Information **S**haring and **A**nalysis **C**entre

Cyber security is a process, not a product

The ISAC is about information sharing and context generation for a specific sector



Information **S**haring in risk management

Risk management makes really sense if good intel is available

Risk management can be used for **governance or benchmarking** if comparable scenarios are used by all actors. These scenarios should be based on facts or objective observations.

Risk management can be a good interface to the board.



Information **S**haring in risk management

The risk management challenge

- Primary assets (scope)
- Secondary assets (granularity)
- Threats
- Vulnerabilities
- Risk treatment
- Residual risk acceptance



Information **S**haring in risk management

What is generally **exchanged in the ISAC** concerning risks

- Scope and specific risk scenarios
- Discussion on impacts (consequences) for the company
 - For the management
 - For customers (B2B)
 - For data subjects (GDPR)
- Risk treatment
 - What measures to put in place, what about the effectiveness



Information **S**haring in risk management

The ministry of the economy, securitymadein.lu, [CERT.lu](https://cert.lu), the HCPN and GovCert will publish soon **the first common (not sector specific) cyber weather for Luxembourg**

Based upon:

- MISP (1600 contributors worldwide), D4, BGP-Ranking, ...
- Anonymized Incidents, sightings
- reports



Information **S**haring in operational security

Some MISP platforms share **sector specific threat intel** (telecom, banking, ...) or campaign specific information.



Information Sharing and **A**nalysis **C**entre

The ISAC is about information sharing **and context generation for a specific sector**

To analyze sectorial specificities in impacts, threats, vulnerabilities and risk scenarios



Information Sharing and **A**nalysis **C**entre

- The ISAC is the perfect place **to exchange with peers**,
 - Best practices, experiences, skills, intel, mistakes and so many other things
- The ISAC helps to go beyond technical or organizational security and add specific context

The ISAC underlies strict confidentiality rules



Information **S**haring and **A**nalysis **C**entre

The ISAC **fills the gap between organizational and technical security** and focusses on the needs of the members in a specific sector.

The ISAC lives from collaboration, skills and experiences

**LET'S
MAKE IT
HAPPEN**



IMPLICATION ON SECURITY FOR THE INDUSTRY SECTOR DURING AND AFTER THE COVID-19 CRISIS

*Steve Muller,
Cybersecurity specialist, Ministry of the Economy*

Implications on **security**
for the **industry** sector
during and after **COVID-19**

IND-ISAC

6 key findings



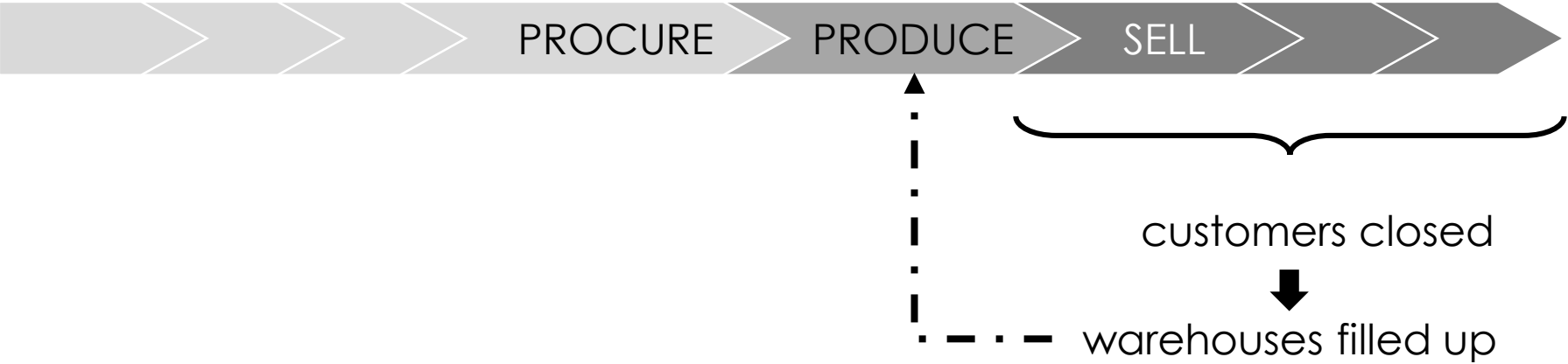
recommendations

	... risk	... measures
review existing ...	•	•
consider additional ...	•	•

1

Stop of production due to no storage space

SUPPLY CHAIN



1

Stop of production due to no storage space

⊕ RISK

“stop of production due to lack of demand” + dependencies

Government restrictions in some countries but not in others



YES

Driving abroad

Last update: 27-07-2020

Have you used our Re-open EU application to spend some time away from home? We are collecting testimonials and feedback from tourists, professionals and agencies on the usefulness of the tool as a part of our promotional campaign. We invite you to get in touch with us regarding your experience with the application and to provide feedback on the design and functionality.

You can reach out to us by e-mail:
JRC-REOPEN-EU@ec.europa.eu

<https://reopen.europa.eu>

2

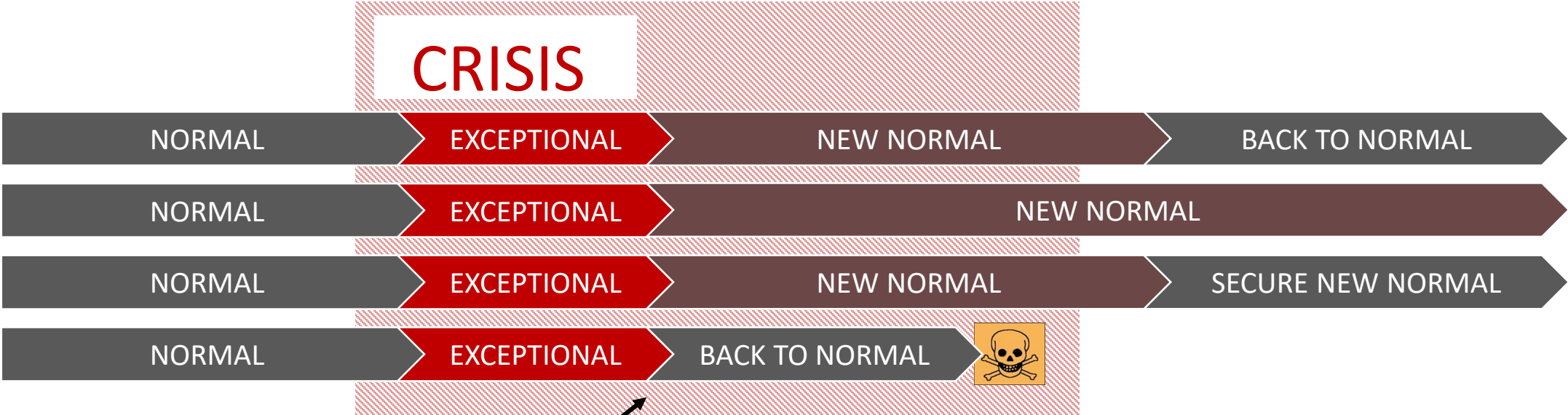
Government restrictions in some countries but not in others

⊕ RISK

“loss of customers”

3

A crisis can be more than a punctual event



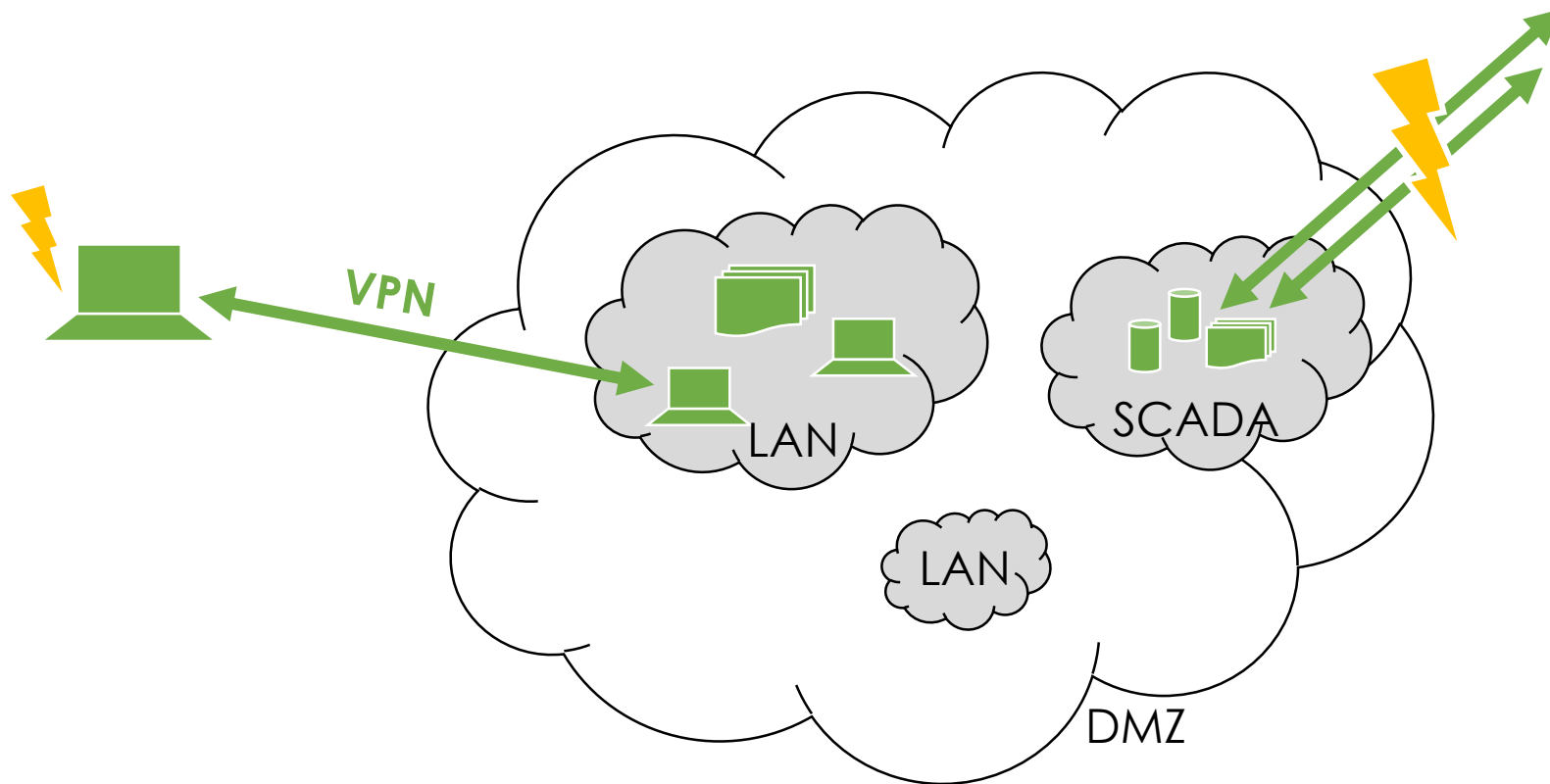
late, despite DRP



3 A crisis can be more than a punctual event

- ^ RISK risk estimation by government may not be accurate
- ^ MEASURE BCP & DRP manageable from remote
- ^ MEASURE review crisis management for long crises
- + MEASURE digitalize
- + MEASURE stress test crisis management
- + MEASURE living space for key personnel (when borders closed)

4 Internal infrastructure has had to be exposed



4 Internal infrastructure has had to be exposed



RISK

increased threat exposure



MEASURE

secure remote access



MEASURE

strong authentication

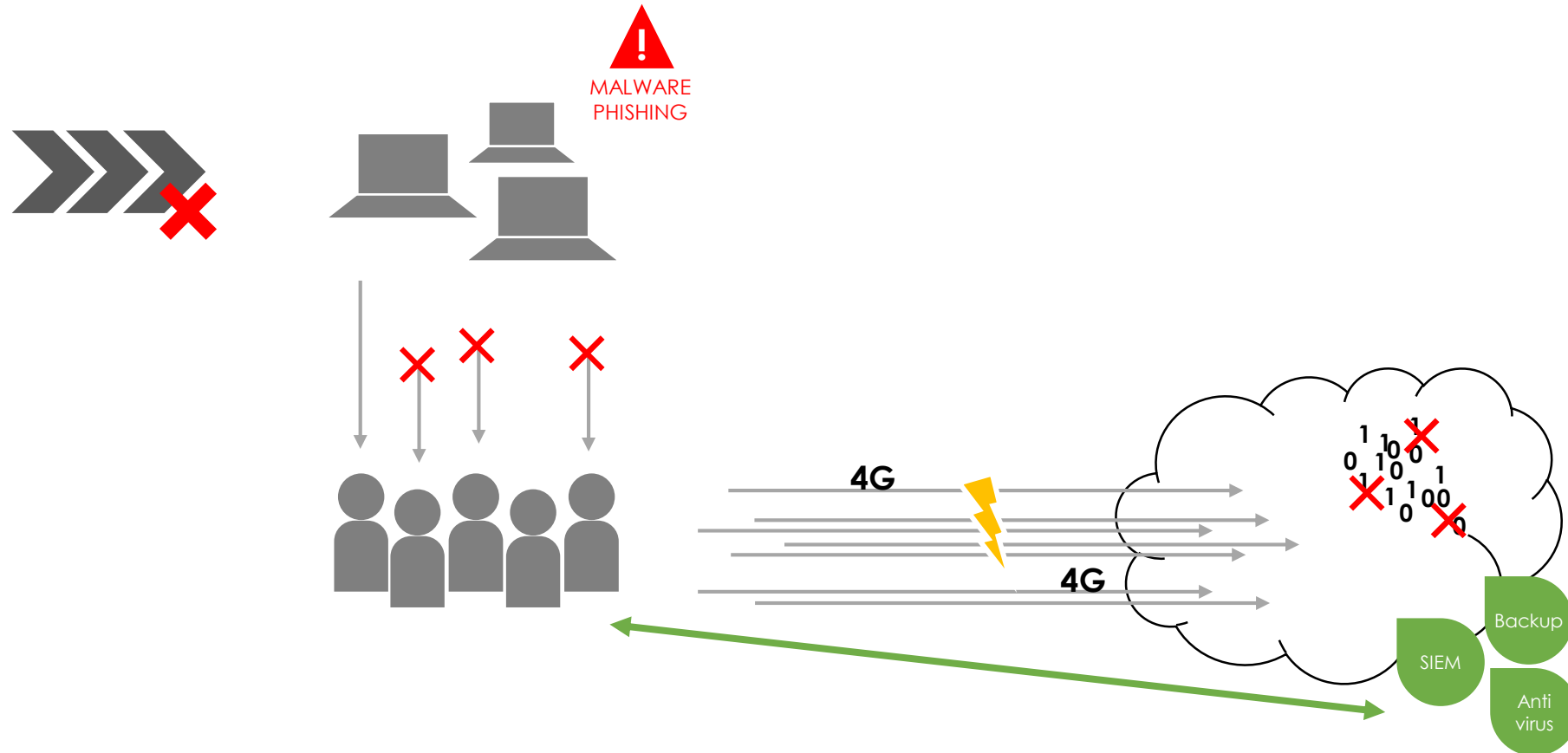


MEASURE

cloud solutions

5

Missing or weak infrastructure for home office



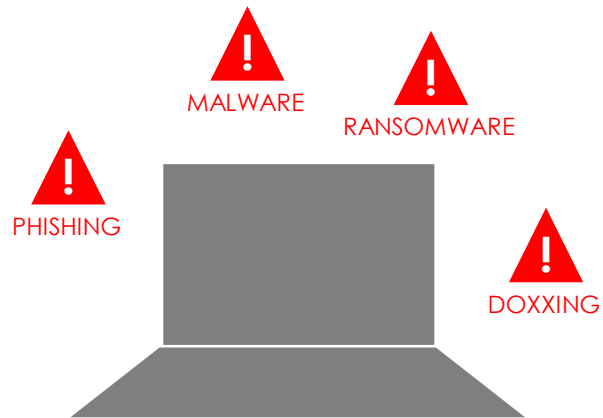
5

Missing or weak infrastructure for home office

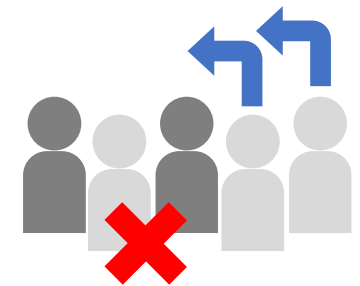
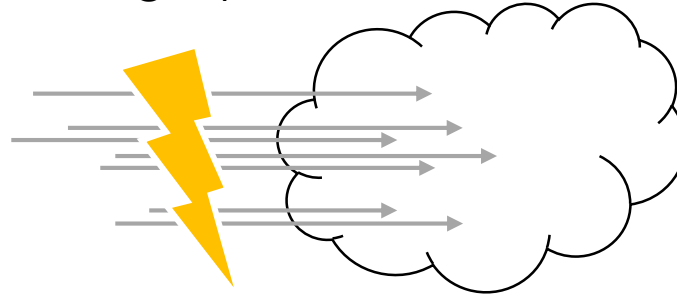
- ^ RISK phishing increased
- ^ RISK leak of information increased (communication via internet)
- ^ RISK data loss increased (no back-ups)
- + RISK communication lines overloaded
- ^ MEASURE security awareness
- ^ MEASURE stress-test infrastructure
- + MEASURE digitalize
- + MEASURE enough home office equipment (+tokens)
- + MEASURE secure communication platforms

6

Threat landscape has changed



VPN = single point of failure



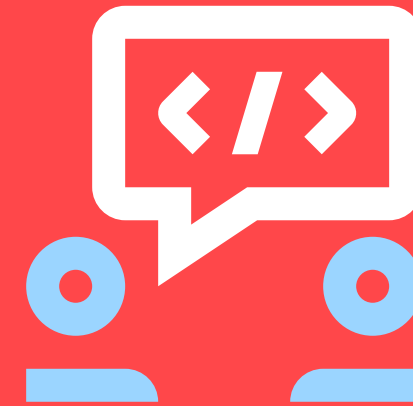
quarantine
social leave

6

Threat landscape has changed

- ^ RISK scam & disinformation (due to insecure situation)
- ^ RISK loss of availability (single point of failure)
- ^ RISK availability of personnel
- ^ MEASURE ensure key personnel is committed and stays available
- ^ MEASURE security awareness training
- + MEASURE provide status information
- + MEASURE DDoS mitigation
- + MEASURE able to handle cyber incident in addition to crisis

ROUND TABLE DISCUSSION



MODERATED BY

*Cédric Mauny,
Co-Chairman, IND-ISAC - Risk Manager,
Proximus Luxembourg*

**WITH
EXPERTS
FROM THE
INDUSTRY**

members of the IND-ISAC

- *Faruk Sari, Assistant CISO, Good Year*
- *Roland Fuhrmann, IT Manager, Faymonville*
- *Cristian Paun, Business CIO EMEA, Du Pont de Nemours*

The background is a solid teal color. In each of the four corners, there are decorative elements consisting of two teal lines meeting at a teal dot, forming a triangular shape pointing towards the center.

CYBERSECURITY DURING THE PANDEMIC TIMES

*Alejandro del Rio,
Data Protection & Privacy – Senior Manager, EY Luxembourg*

“Cybersecurity during the pandemic times”

Conference: Why cybersecurity matters more than ever

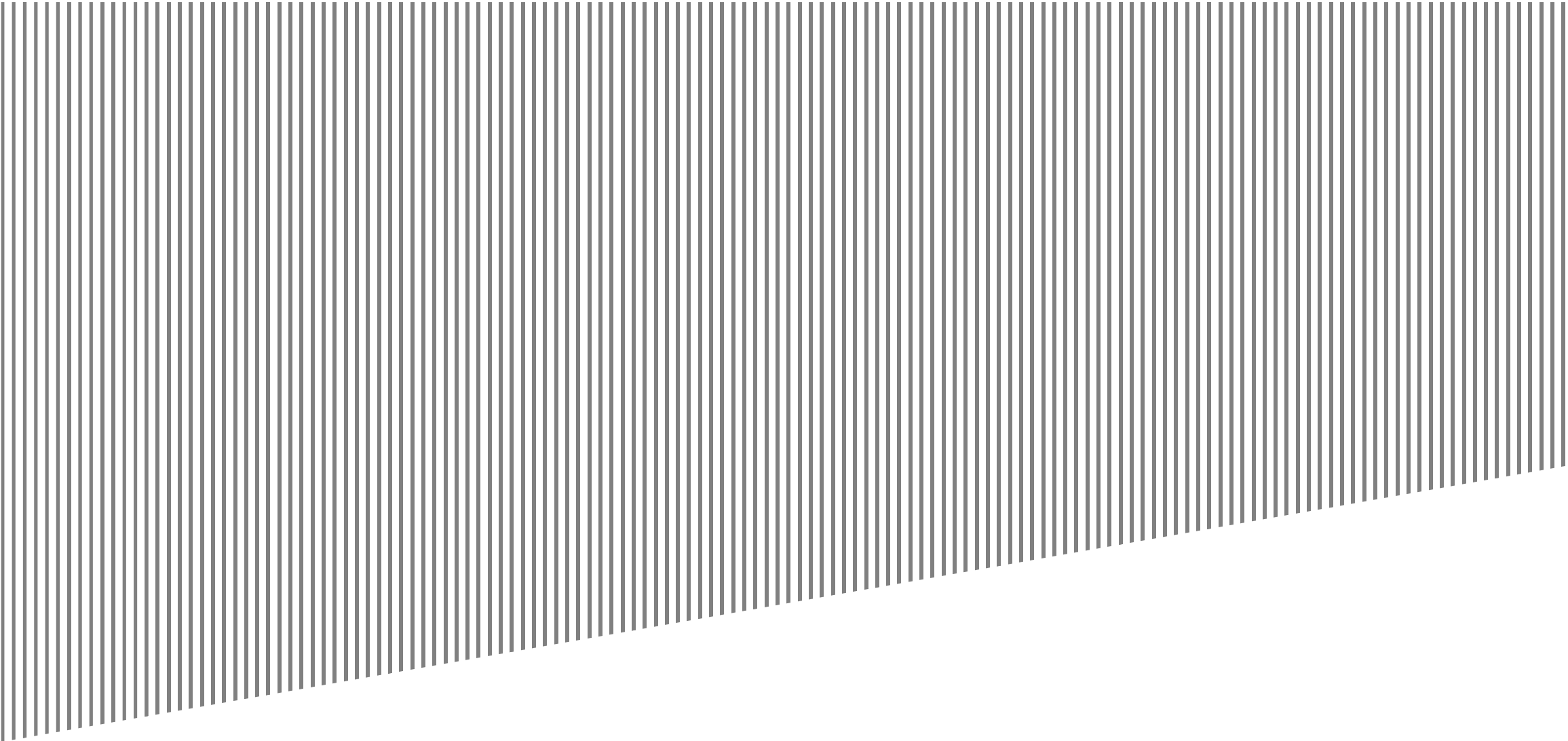
Presentation of Cyber Higiene Rules tool - Thursday 22 October



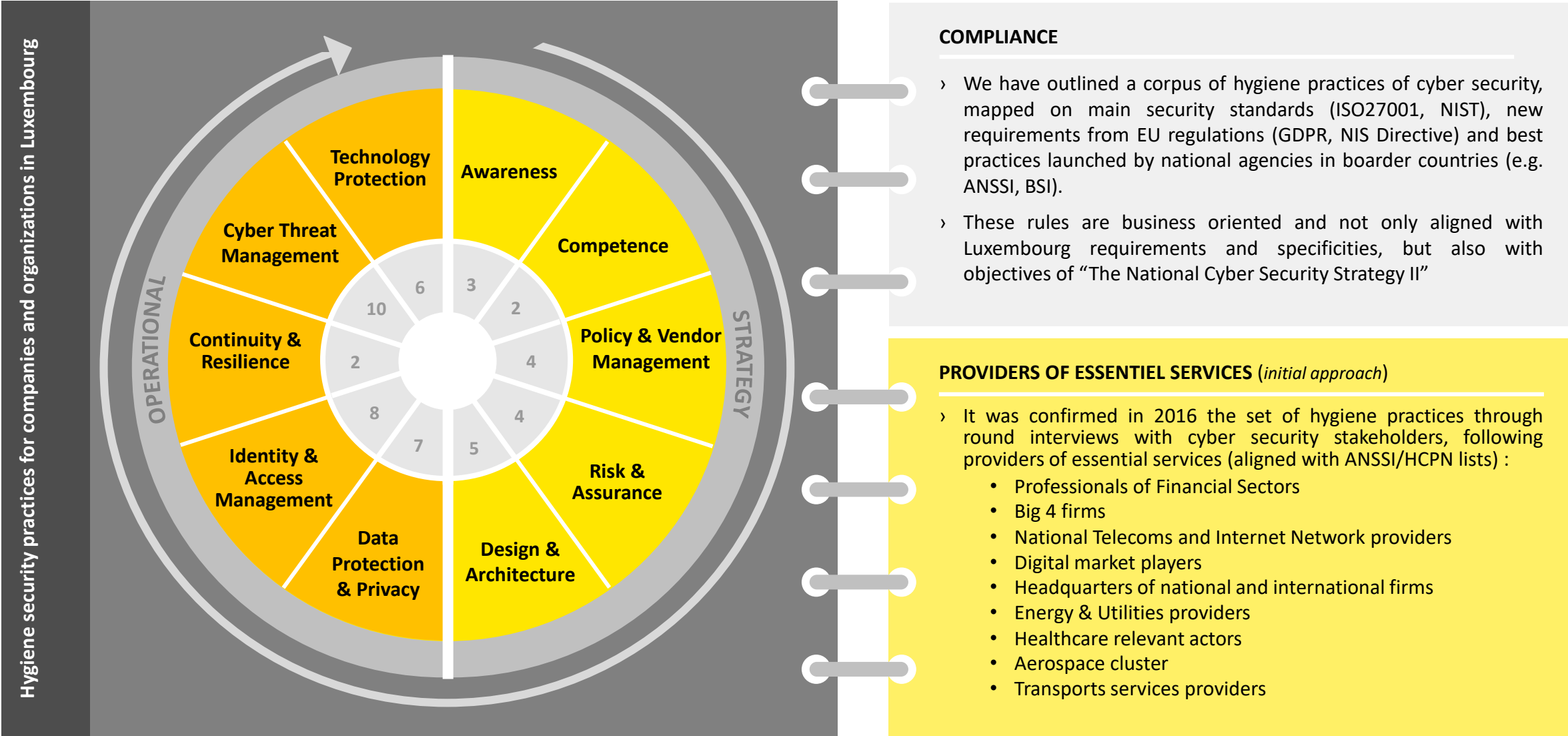
› Mr. Alejandro del Río | Senior Manager | Technology Consulting | Cybersecurity | Data Protection & Privacy



2019 Recap

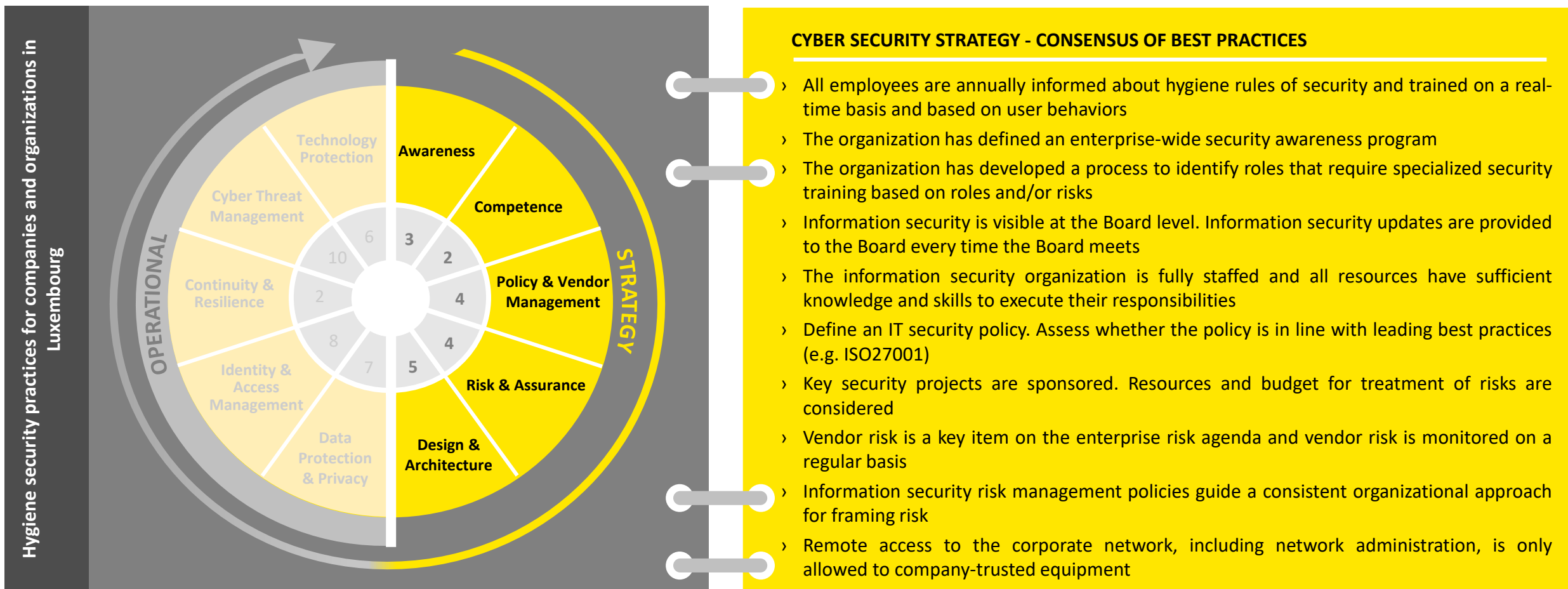


We built in collaboration with companies and organizations a set of security practices, which aimed to strengthen and facilitate the journey towards the protection against new threats



What is the minimum level of standards which should be applied ?

Cyber security strategy

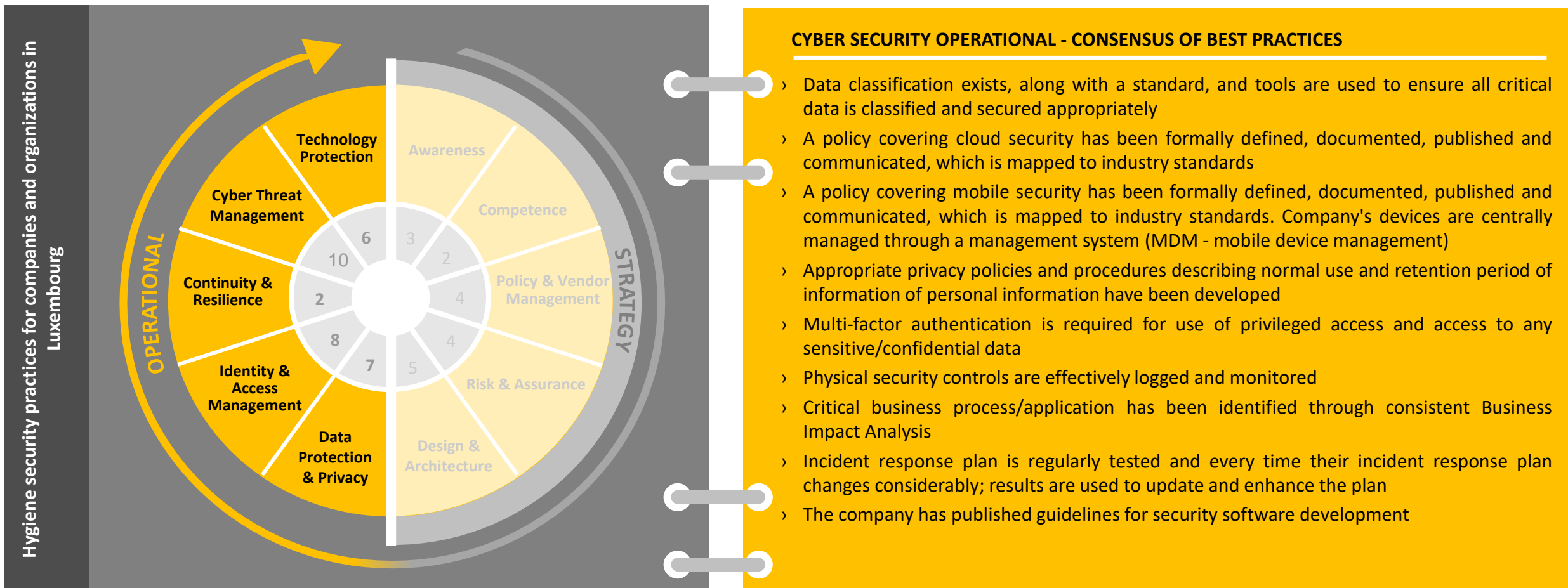


››Based on our first round of interviews, we have identified that some of sectors, such as Healthcare and Aerospace, have already gone further than the consensus according to their risk appetite and level of threats.

››Some actors of Healthcare have adopted advanced data encryption solutions while certain telecommunication players are slightly further the best practices on Business continuity, as business is highly committed to prevent any operational disruption.

What is the minimum level of standards which should be applied ?

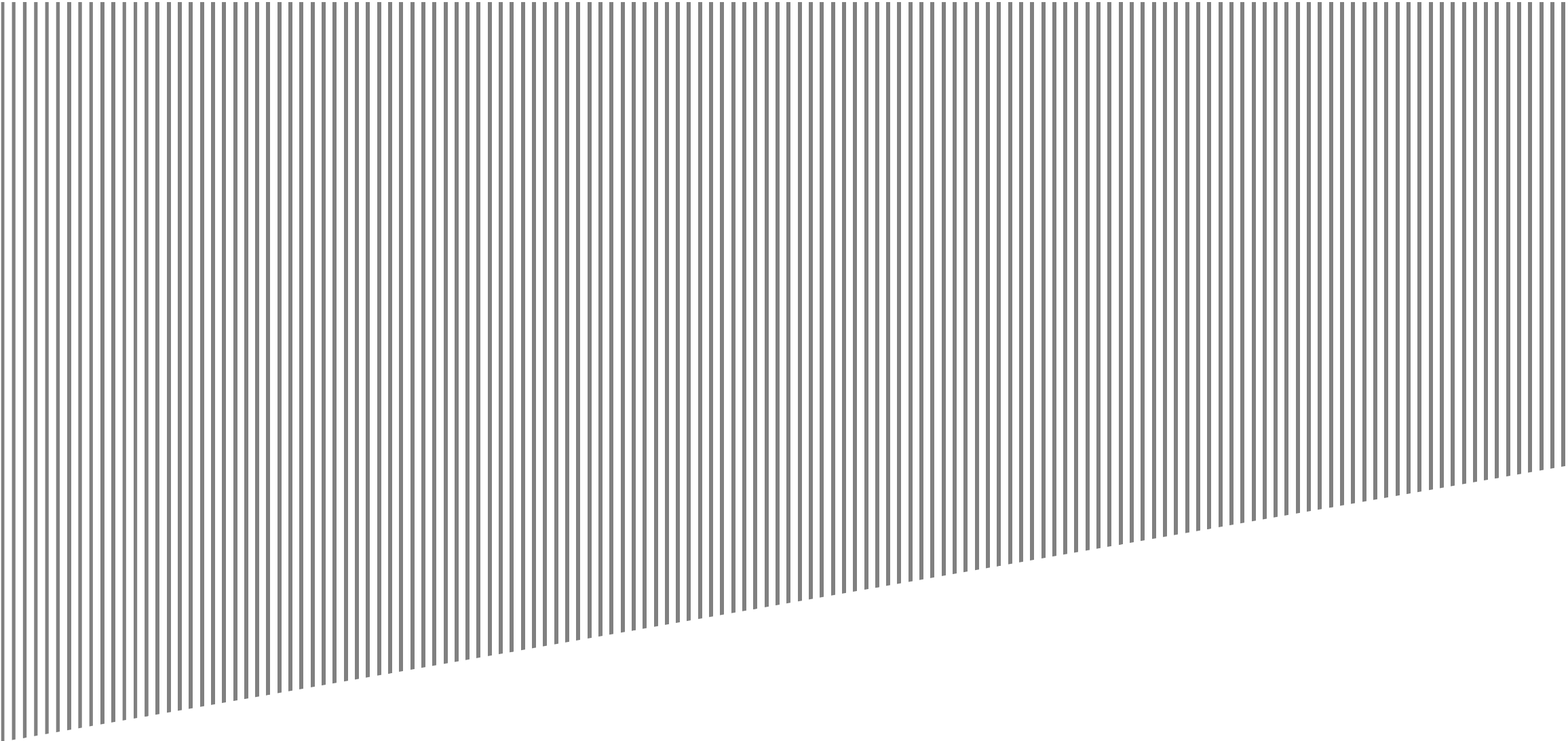
Cyber security operational



››Based on our first round of interviews, we have identified that some of sectors, such as Healthcare and Aerospace, have already gone further than the consensus according to their risk appetite and level of threats.

››Some actors of Healthcare have adopted advanced data encryption solutions while certain telecommunication players are slightly further the best practices on Business continuity, as business is highly committed to prevent any operational disruption.

Adapting Cybersecurity in an Uncertain Environment



Adapting cybersecurity in an uncertain environment

COVID-19 impact on cybersecurity

COVID-19 cyber context

- Threat actors are taking advantage
- Phishing and social engineering attacks targeted at teleworking employees
- Longer term impacts for organizations, as threat actors bury themselves deep within networks
- With staff shortages, reliance on co-sourcing, and outsourcing. Continued trend
- Cybersecurity and privacy functions must stay the course
- Maintain extra vigilance in monitoring for and reacting to cyber risk.

Cyber is adapting to uncertainty...

- Conducting rapid risk assessments and reprioritizing cybersecurity projects.
- Leveraging third parties to provide staff and subject matter resources for emerging cyber risk areas
- Pre-installing and configuring laptops, tablets and encrypted drives for employees to use while working from home
- Developing simple teleworking policies and procedures
- Virtual security awareness training for employees new to teleworking.
- Enabling teleworkers with technology support and expertise on subjects like VPN use or securing personal devices.
- Review data breach insurance and similar policies for coverages and exposures.
- Ensure an adequate bench exists to manage cyber incidents.

How can cyber enable business longer term?

Cyber has a real opportunity to collaborate with the business:

- Are you helping your organization assess and understand new data privacy risks related to operating in a COVID-19 environment ?
- Have you reprioritized patching and upgrading activities to better enable business recovery?
- Have you revisited your sourcing strategy to ensure adequate staff is available as business gears up?
- Assuming we move into a recessionary financial environment, have you begun to revisit cybersecurity strategy and projects for the mid and long-term?

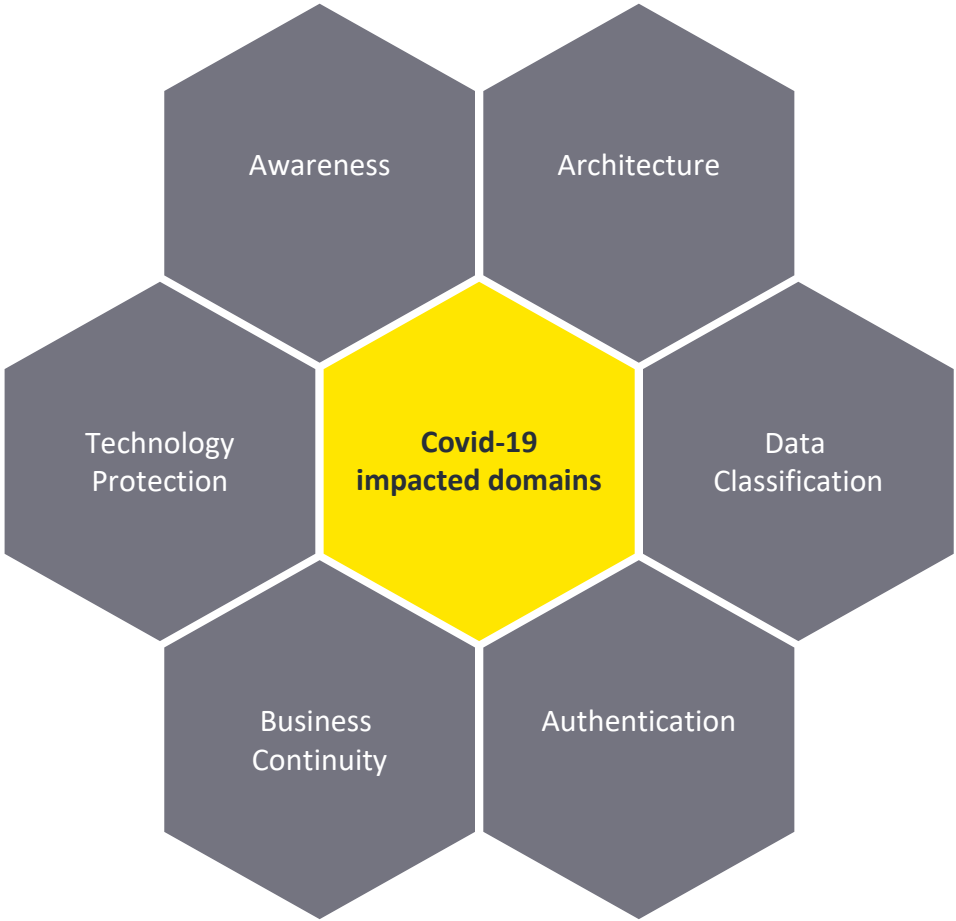
Adapting cybersecurity in an uncertain environment

Update on cyber hygiene rules

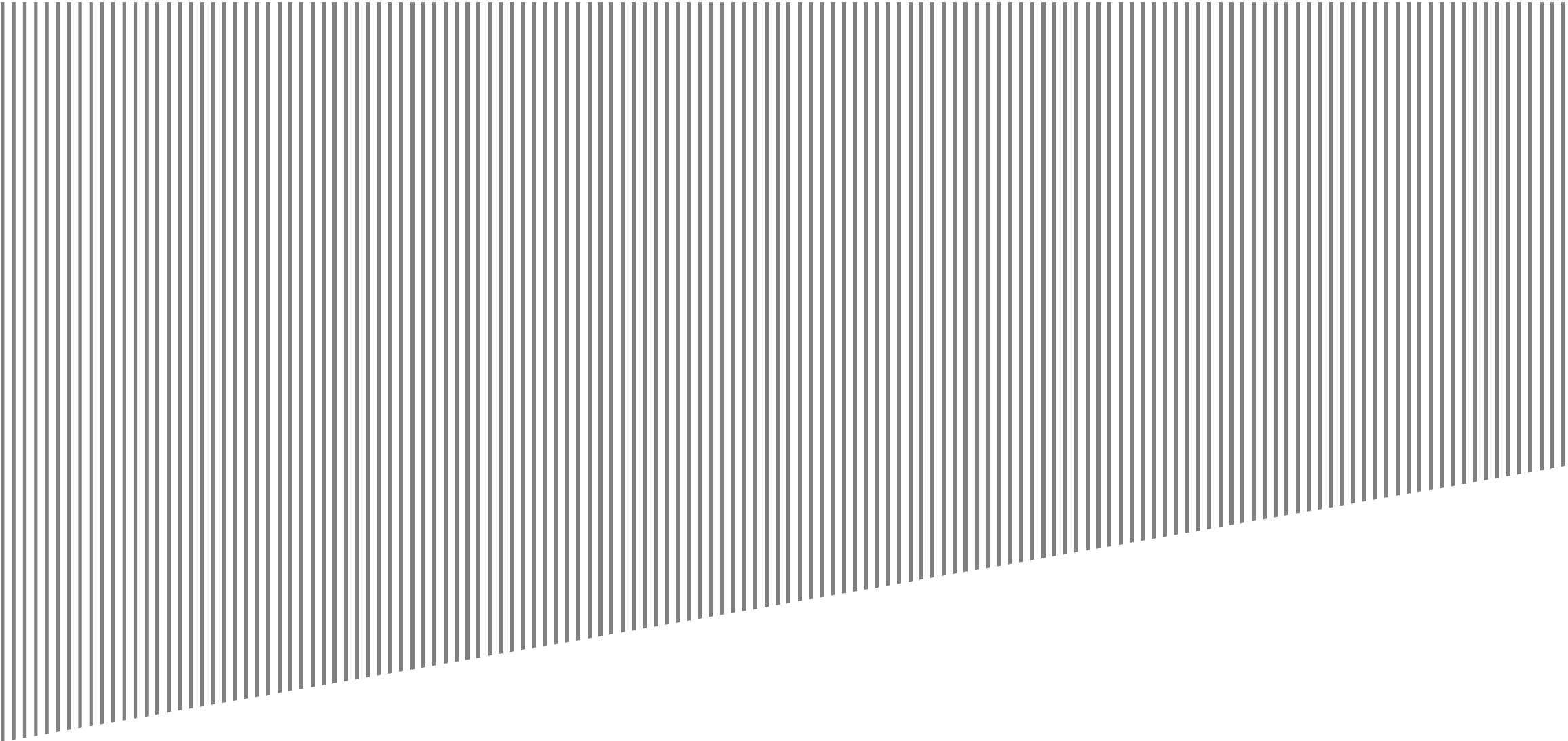
EY Cybersecurity Intelligence has identified an increase in the following opportunistic cybersecurity events among clients and industry research:

STRATEGICAL INSIGHT	
1.1.2	Off-site training
5.1.1	Remote access – VPN test

STRATEGICAL INSIGHT	
6.1.3	Usage of collaboration platforms
7.1.2	Off-site password update
7.1.3	Multi-factor authentication
8.1.2	Crisis management team
10.1.2	Off-site endpoint protection update
10.2.2	Network access control implementation



Access Management Feature



Access management

Improving current capabilities to allow higher control

The new access management features improve mainly three key areas:

- ☐ Username and password using corporate email address to allow continuation of the exercise on the companies
- ☐ Prefilled answers in each new connection to keep as reference last answers
- ☐ Comparison of results from prior assessments

INTRODUCTION

COMPANY DETAILS

STRATEGICAL INSIGHT

AWARENESS

COMPETENCE

POLICY & VENDOR MANAGEMENT

RISK & ASSURANCE

DESIGN & ARCHITECTURE

OPERATIONAL INSIGHT

DATA PROTECTION & PRIVACY

IDENTITY & ACCESS MANAGEMENT

CONTINUITY & RESILIENCE

CYBER THREAT MANAGEMENT

TECHNOLOGY PROTECTION

COMPANY DETAILS

You already did an assessment for your company ? Use your credentials to log into your account to pre-fill the fields with your previous answers.

CONNEXION

NAME

STREET

POSTAL CODE

CITY

EMAIL

PHONE NUMBER

WEB PAGE

TOTAL WORKFORCE

TURNOVER

CONTACT DETAILS

NAME

FIRST NAME

POSITION

EMAIL

PHONE NUMBER

ACCOUNT

PASSWORD

REPEAT PASSWORD

Create an account will allow you to reconnect later and to make a new assessment for your company.

AREA OF ACTIVITY

☐ Aerospace

☐ Healthcare

☐ Public

☐ Aviation

☐ Industry

☐ Telecommunication


☐ Bank

☐ Power and utilities

☐ Start-up

DESCRIPTION OF ACTIVITY

Page 10



FEDIL EY

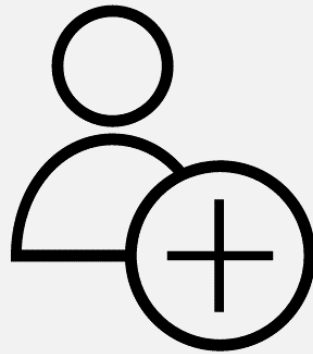
The Voice of Luxembourg's Industry

Next steps (continuation of 2019)

Actions to be considered in next stages in order to keep moving



**For all companies to start
using the [tool](#) as a first
step**



**Increase awareness
towards this tool to have
more participants**



**Strength collaboration
between public bodies
and private sector**

Thank you !



CLOSING WORDS

*Céline Tarraube,
Adviser Digital & Innovation, FEDIL*

FEDIL

The Voice of Luxembourg's Industry



CYBERSECURITY WEEK

19//29 OCTOBER 2020



*with the QR-CODE you
have direct access to the*

**FEDIL
CYBERSECURITY
ASSESSMENT
ONLINE TOOL**

Should you wish to join the ISAC, please contact

*Céline Tarraube
Adviser Digital & Innovation, FEDIL
celine.tarraube@fedil.lu
(+352) 43 53 66 610*

