

# CANSO Standard of Excellence in Cybersecurity

Thursday 3 December 2020

14:00 – 15:30 CET

# Speakers



*Moderator:*  
Shayne Campbell  
Safety Programme Manager  
CANSO



Richard Derrett-Smith  
Principal Consultant  
Helios



Morten Fruensgaard  
Head of Security, Safety and  
Crisis Management  
Avinor ANS



Andreas Gerstinger  
Safety Manager  
Frequentis AG




# **Richard Derrett-Smith**

## **Principal Consultant**

**Helios**


# Polling Question

**Do you and your leadership team know your current level of cybersecurity maturity?**

- a) Yes, we have used the CANSO SoE maturity model
  - b) Yes, we have used a different maturity model
  - c) We have a rough idea based on expert judgement
  - d) No, but we plan to assess our maturity soon
  - e) Don't know
- 

# Polling Question

**For you as an organisation, how important is the level of cybersecurity maturity of your suppliers for supplier selection?**

- a) It is an essential criterion
  - b) It is one of many criteria
  - c) Not important as our own cybersecurity processes are mature
  - d) Don't know
- 

CANSO Academy



# Standard of Excellence Maturity Model

CANSO Cyber Safety Task Force

3 December 2020

14:00 – 15:30 CET





## Cybersecurity Culture

Development of a positive and proactive cybersecurity culture

### CANSO Emergency Response Planning Guide

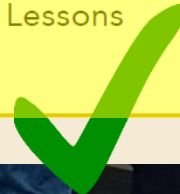
- Planning Guide
- Contingency Procedures
- Lessons Learned

2019

### CANSO Standard of Excellence in Cybersecurity

- Maturity Model
- Advice and Lessons Learned

Sep 2020



### CANSO Cyber Risk Assessment Guide

- Risk Assessment Guide
- Risk Matrix
- Threat Landscape

# Need for Cybersecurity

- Increased sharing of information in an open systems ATM architecture
- Use of commercially available IT and network infrastructure products, transition away from legacy systems
- Greater attack surface and consequences are significant
  - Safety
  - Financial
  - Reputational
  - Regulatory Compliance



# Potential Threat Sources

- Unintentional
  - Human behaviour
  - Weaknesses in processes (operating and maintenance)
  - Equipment Failure
- Intentional
  - Targeted attacks (insider led)
  - Non-targeted attacks (virus/worm/malware)

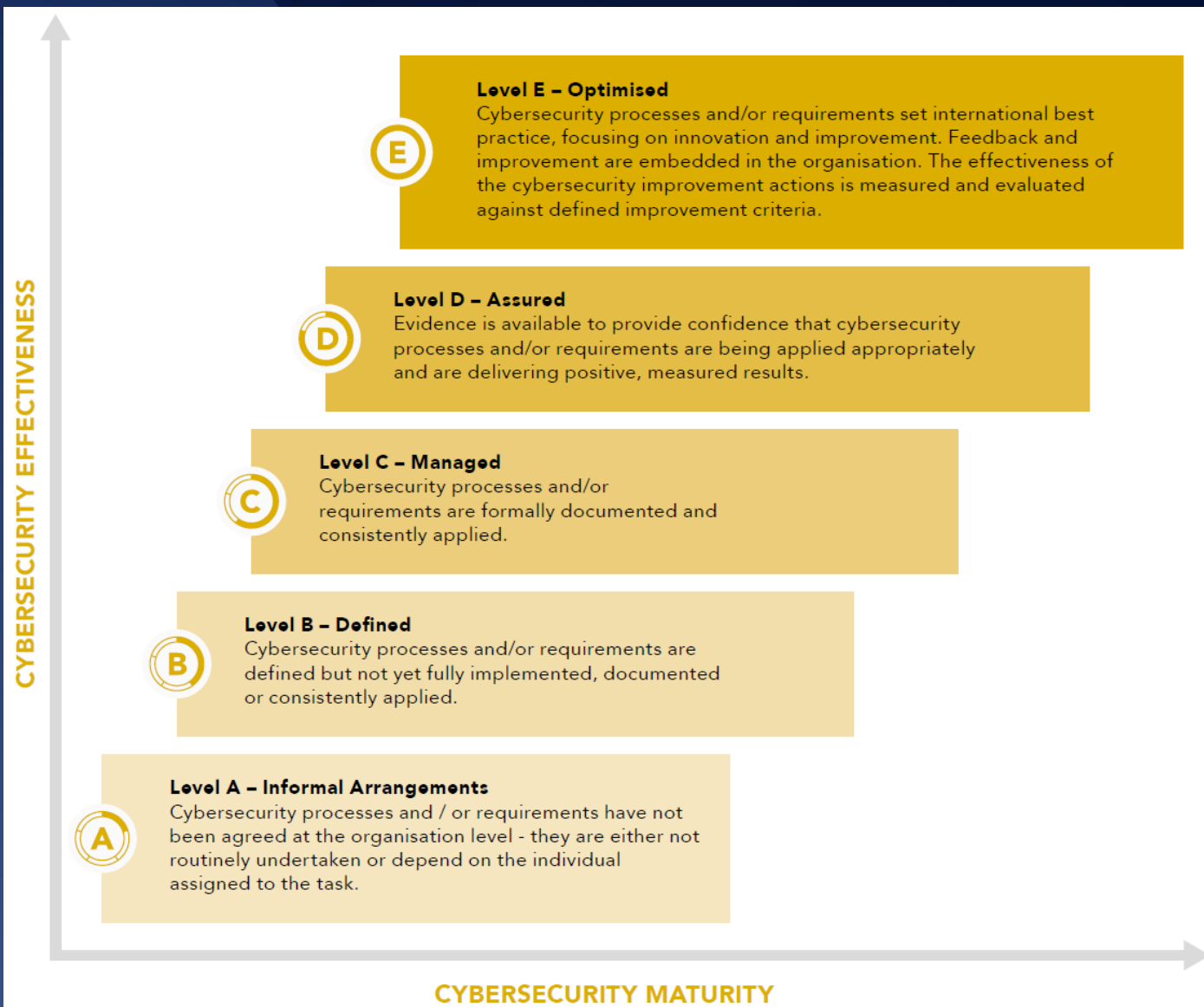
# Excellence in Cybersecurity

- What
  - Maturity model based approach focusing on key functions and elements within each function critical to cybersecurity
- Who is it for
  - Senior management including Chief Information Security Officers (CISOs) and/or cybersecurity managers
- Benefits
  - Highlights the critical elements of cybersecurity based on industry expertise specific to ATM
  - Allows comparison
  - Non-prescriptive and is flexible to accommodate different levels of cybersecurity risk exposure
  - Broad basis from across safety-critical industries not just ATM

# SoE Maturity Levels




## CANSO Standard of Excellence in Cybersecurity



# Polling Question

**What are the key area(s) of concern from a cybersecurity perspective within your organisation?**

- a) Lack of leadership and governance
  - b) Level of cybersecurity maturity within our supply chain
  - c) Weak identity management and access control
  - d) Ability of our staff to detect and respond to cyber threats
  - e) None of the above – please add to question pane
- 

# What are the key elements?

Leadership and Governance

Information Security Management System

Asset Management

Risk Assessment

Information Sharing

Supply Chain Risk Management

Identity Management and Access Control

Human-Centred Security

Anomalies and Events

Protective Technology

Response Planning

Mitigation

Recovery Planning



# Some more detail

## Leadership and Governance

- Demonstrate leadership and commitment
- Clear understanding of cybersecurity vulnerabilities
- Management of cybersecurity risks and setting objectives/priorities

## Supply Chain Risk Management

- Appropriate processes and policies in place to manage supply chain risk
- Appropriate levels of trust between commercial partners
- Applies to commercially acquired information and technologies

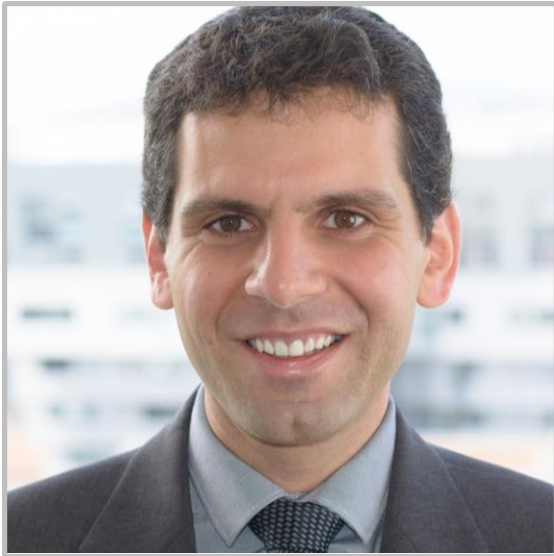
# Some more detail

## Identity Management and Access Control

- Identification, authentication and authorisation
- Access to physical and logical assets is limited to authorised users only
- Access is managed consistent with the risk of unauthorised access
- Proper separation of duties is key to ensure that conflicts of interest don't arise

## Human-Centred Security

- Development of positive security culture (attitudes, behaviours and set by example)
- Provision of appropriate cybersecurity awareness and training
- Recognition that people form a key defence against cybersecurity threats from both a prevention and recovery perspective



**Andreas Gerstinger**

**Safety Manager**

**Frequentis AG**

# Leadership and Governance

- Assessment of maturity level against each element is supported by probing questions for ANSPs and suppliers

Element	Description	 <b>A</b> Informal Arrangements	 <b>B</b> Defined	 <b>C</b> Managed	 <b>D</b> Assured	 <b>E</b> Optimised
<b>Leadership and Governance</b>	Senior management demonstrate leadership and commitment to cybersecurity. The policies needed to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	No overarching policy, strategy or plan	Policy established, together with parts of a strategy or plan; roles & responsibilities are established but no or weak link with top management	Policy supported by a strategy and plan approved by top management; key risks are accepted by top management	Plan is funded and, with visible top management commitment, delivering intended improvements across the organisation	Updated regularly to reflect progress, threats and risks

Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
<b>Leadership and Governance</b>				<ul style="list-style-type: none"> <li>Do you have an approved policy, strategy, plan and budget?</li> <li>How is the whole organisation aligned with them?</li> <li>Who is responsible for what?</li> <li>How do you ensure that security is integrated into all operational processes?</li> </ul>	<ul style="list-style-type: none"> <li>Do you have an approved policy, strategy, plan and budget for securing the product/service?</li> <li>How is the whole organisation aligned with them?</li> <li>Who is responsible for what?</li> <li>How do you ensure that security is integrated into all processes that deliver the product/service?</li> </ul>

# Supply Chain Risk Management

Element	Description	 <b>A</b> Informal Arrangements	 <b>B</b> Defined	 <b>C</b> Managed	 <b>D</b> Assured	 <b>E</b> Optimised
<b>Supply Chain Risk Management</b>	The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has in place the processes to identify, assess and manage supply chain risks. Appropriate levels of trust are established with data exchange partners.	No complete overview of all suppliers / partners	Some requirements placed on some suppliers and agreements with some partners; partial and informal understanding of supplier/partner cybersecurity maturity	Minimum set of requirements placed on all critical suppliers and agreements with partners, with mostly self-assessment for compliance	Requirements placed on suppliers with proportionate compliance checks and processes / penalties / measures for non-compliance	Independent reviews / audits / assessments supporting regular updates of requirements against new good practices

Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
<b>Supply Chain Risk Management</b>				<ul style="list-style-type: none"> <li>How do you determine the level of trust you have with different suppliers / partners?</li> <li>How do you ensure the right requirements are placed on suppliers?</li> <li>How do you ensure the right supplier/partner behaviours?</li> </ul>	<ul style="list-style-type: none"> <li>How do you determine the level of trust you have with different sub-contractors / partners in delivering the product/service?</li> <li>How do you ensure the right requirements are placed on sub-contractors?</li> <li>How do you ensure the right sub-contractors/partner behaviours?</li> </ul>



# Human-Centred Security

Element	Description	 Informal Arrangements	 Defined	 Managed	 Assured	 Optimised
<b>Human-Centred Security</b>	The organisation's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Security is part of the organisation's culture.	No awareness/training programme	Ad hoc activities to inform and educate	Coherent programme in place that addresses whole organisation, including addressing human factors and organisational culture	Sustained activities with follow-ups, differentiated for different roles, leading to increasing compliance and performance	State of the art syllabus, with systematic testing, leading to routine and proactive cybersecurity risk reporting from staff

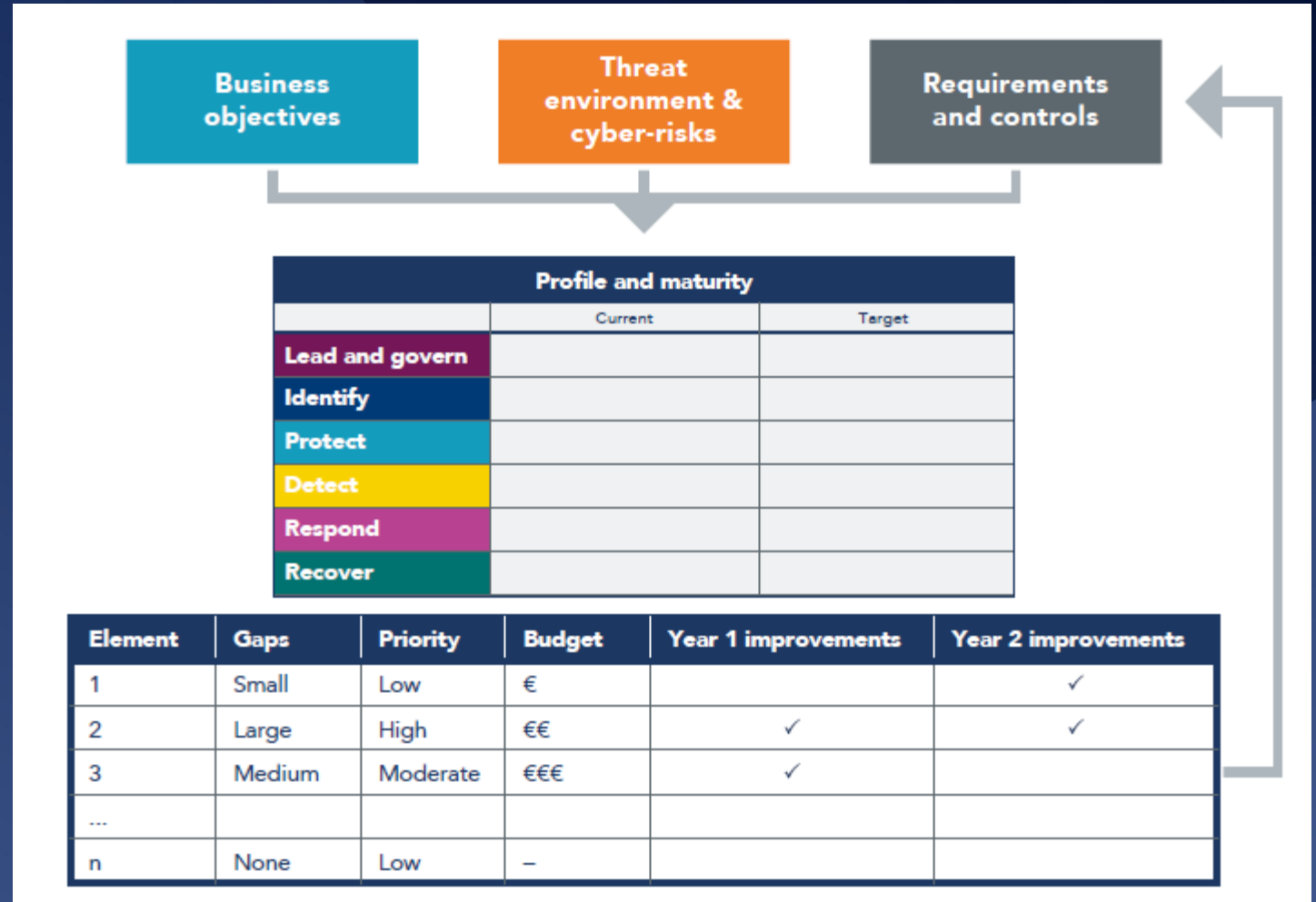
Element	Level score? (A-E)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
<b>Human-Centred Security</b>				<ul style="list-style-type: none"> <li>How do you ensure that awareness leads to the right behaviours?</li> <li>What indicators do you use to predict who will later be detected violating security policy?</li> </ul>	<ul style="list-style-type: none"> <li>How do you ensure that awareness leads to the right behaviours?</li> <li>What indicators do you use to predict who will later be detected violating security policy?</li> </ul>

# Example Assessment Results

Function	Capability	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
Lead and Govern	Leadership and Governance	D	D	D	C	B	B
	Information Security Management System	C	D	C	C	C	B
Identify	Asset Management	E	E	D	C	C	B
	Risk Assessment	B	D	D	B	C	B
	Information Sharing	C	D	C	B	B	A
	Supply Chain Risk Management	C	D	D	C	B	A
Protect	Identity Management and Access Control	D	E	C	C	D	C
	Human - Centred Security	B	D	D	C	C	A
	Protective Technology	D	E	C	D	B	B
Detect	Anomalies and Events	D	C	C	C	C	A
Respond	Response Planning	C	D	D	D	A	A
	Mitigation	D	D	C	C	A	B
Recover	Recovery Planning	D	D	D	B	C	B

# How to Use the Results

- Identify gaps
- Set priorities
- Build a roadmap for improvement



# Yet Another Maturity Model?

- Yes, but
  - It is aimed at ATM – so it is relevant for us it aims to focus on security in a safety-related context
  - It provides an end-to-end cybersecurity assessment of your organisation including your supply chain
  - It is very simple and a self-assessment should be possible in less than a day
  - It contains lessons learned from our industry

# Lessons Learned

- Leadership and Governance
  - Combine safety and security, stress that security vulnerabilities can undermine the safety of operations,...
- Supply Chain Risk Assessment
  - Educate purchasing department, evaluate suppliers, be aware of costs, adapt requirements for suppliers, let cybersec professionals communicate directly,...
- Human-Centred Security
  - Draw lessons from a more mature group, e.g. safety, add cybersecurity training to onboarding, regularly refresh training,...



# Questions and Answers



*Moderator:*  
Shayne Campbell  
Safety Programme Manager  
CANSO



Richard Derrett-Smith  
Principal Consultant  
Helios




Morten Fruensgaard  
Head of Security, Safety and  
Crisis Management  
Avinor ANS



Andreas Gerstinger  
Safety Manager  
Frequentis AG


# Polling Question

**Do you think you will apply this SoE to your own organisation?**

- a) No, we have already applied another model or approach
  - b) It would require clear management endorsement
  - c) Yes, as it seems simple and effective
  - d) Don't know
- 


# Polling Question

**Do you think you will apply the SoE to your suppliers?**

- a) No, we rate our suppliers based on other criteria
  - b) It would require clear management endorsement
  - c) Yes, but we would let them self-assess themselves
  - d) Yes, but we would probably assess them ourselves
  - e) Don't know
- 

# Polling Question

**The Cyber Risk Assessment Guide was last published in 2014. In your opinion, what should the scope of update be:**

- a) I am not aware of/I have not read the document
  - b) It is acceptable in its current form
  - c) It is too high-level and requires more detailed guidance
  - d) None of the above, please add comments to question pane
- 

# Questions and Answers



*Moderator:*  
Shayne Campbell  
Safety Programme Manager  
CANSO



Richard Derrett-Smith  
Principal Consultant  
Helios



Morten Fruensgaard  
Head of Security, Safety and  
Crisis Management  
Avinor ANS



Andreas Gerstinger  
Safety Manager  
Frequentis AG



# Thank you

Visit us:  
**canso.org**

