Navigating Cyber Risk in Aviation

Aligning EASA Part-IS and NIS2 through a Risk-Based Approach

April 2026

Dr. Fernando Sevillano
Head of Cyber & Tech Consulting, Western Europe

By **measuring** your **external exposure, maturity level, and existing cyber risk, based on evidence**, you empower yourself to **make informed, strategic decisions** regarding **mitigation and risk transfer.**

You reduce costs and risk.

You will be **aligned with cybersecurity regulations** to **avoid fines.**

The Hybrid Threat - The Evidences

On September 19, 2025, Dublin Airport experienced a major security alert that prompted the evacuation of Terminal 2 after a **suspicious piece of luggage was discovered**.

Following a thorough investigation, authorities confirmed the item was harmless, allowing normal airport operations to resume.

At the same time, a **Europe-wide cyberattack**, specifically the **HardBit Ransomware**, affected major airports including London Heathrow, Brussels, Berlin, as well as **Dublin and Cork**.

The attackers targeted **Collins Aerospace's ARINC cMUSE (Multi-User System Environment)**, a vital infrastructure for check-in and boarding.

As a result, airports were forced to switch to manual passenger processing, leading to significant delays.

Aer Lingus, among other airlines, was particularly impacted by the ransomware attack.

Additionally, **drone incursions** have been observed in similar contexts, contributing to what some European officials describe as **hybrid threats**, **blending physical disruptions with cyber risks to compromise airport security.**

1. https://economictimes.com/news/international/us/dublin-airport-evacuated-thousands-cleared-from-terminal-2-after-suspicious-luggage-scare-is-it-safe-to-travel-now/articleshow/124017326.cms
2. https://www.bbc.com/news/articles/cz7rp35gjpzo
3. https://www.irishexaminer.com/business/companies/arid-41711888.html
4. https://brandsit.pl/en/cyber-attack-on-software-provider-paralyses-key-european-airports/

Contents

1. EASA Part-IS & NIS2 Regulations.
2. Fundamental concepts you should understand regarding the measurement of cyber risk.
3. Practical application of these concepts within the context of the EASA Part-IS and the NIS2 Directive in Ireland.
4. Adopting a structured roadmap to strengthen resilience while ensuring EASA Part-IS and NIS2 alignment.

1. EASA Part-IS & NIS2 Regulations

EASA Part IS.OR (Information System – Organization Requirements)

European Union Aviation Safety Agency (EASA)
- **Basic Regulation: (EU) 2018/1139 – Establishes EASA & high-level safety objectives**
- **Implementing Rules (IRs)** – Detailed technical requirements
  - **Part-21** (Design/Production/MRO): Aircraft certification
    - **Part-IS.D.OR** ← Inserted here (DOA/POA/Aerodromes) [2022/1645]**
  - **Part-66/145** (Maintenance): Continuing airworthiness
    - **Part-IS.I.OR** ← Inserted here [2023/203]**
  - **Part-ORA/ATO** (Training): Approved Training Orgs
    - **Part-IS.I.OR** ← Inserted here**
  - **Part-CAT/AOC** (Air Operations): Commercial ops
    - **Part-IS.I.OR** ← Inserted here (AOC/CAMO)**
  - **Part-ATS/ANSP** (Air Navigation): ATM/ANS services
    - **Part-IS.I.OR** ← Inserted here**
  - **Part-IS.AR** ← New annex for Aviation Authorities (oversight) [Annex I]
- **Acceptable Means of Compliance (AMC) & Guidance Material (GM)**
  - AMC/GM to Part-IS.AR / Part-IS.I.OR / Part-IS.D.OR
- **Easy Access Rules** – Consolidated publications (all above in one doc)

1. EU has adopted dedicated **information security rules** for civil aviation via **Commission Delegated Regulation (EU) 2022/1645 and Implementing Regulation (EU) 2023/203.**

2. EASA Part-IS.I.OR contains the **core cybersecurity requirements** for operational aviation organizations (AOCs, Part-145, ANSPs, etc.).
   - https://www.easa.europa.eu/sites/default/files/dfu/AMC___GM_to_Part-IS.I.OR__Issue_1.pdf

3. Core elements include: an **Information Security Management System (ISMS), risk assessment and treatment, incident detection/response/recovery, internal and external reporting, defined responsibilities and an ISM manual.**

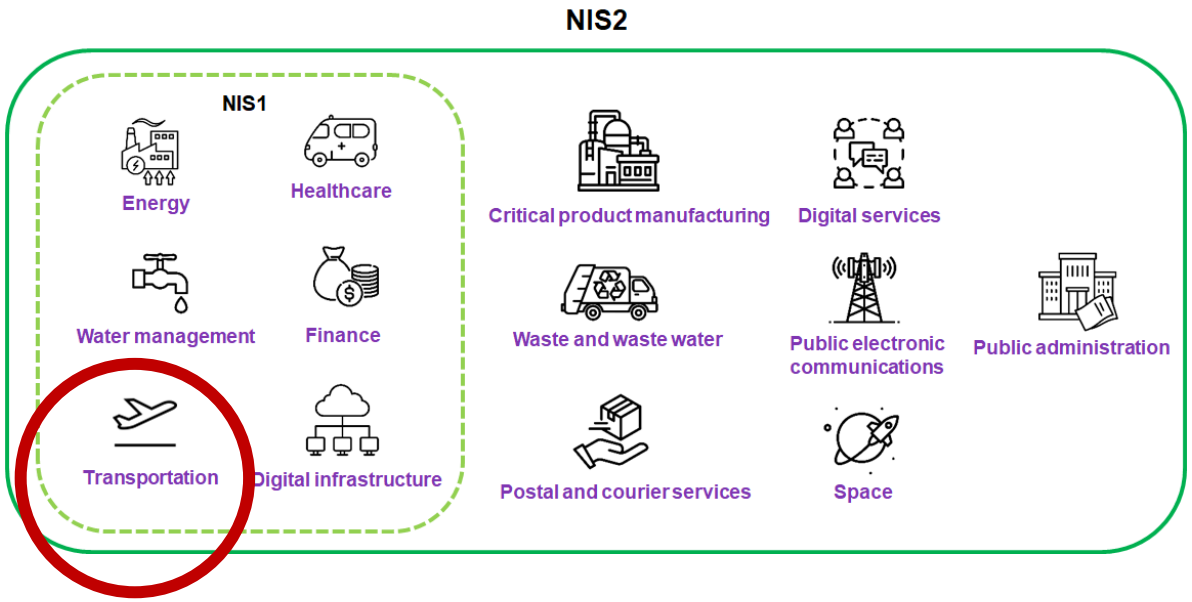
4. EASA Part-IS applies **to EASA-approved aviation organizations** handling safety-critical ICT systems/data: airlines (AOCs/CAMOs), Part-145 maintenance organizations, airports, ANSPs, DOAs/POAs, and ATOs (excl. ELA-European Light Aircraft).

NIS 2 Directive (Network and Information Security 2)

Member States shall ensure that the **management bodies** of essential and important entities **approve the cybersecurity risk-management measures** taken by those entities to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

1. Management obligations.
2. Assess and recognize, notify to authority.
3. Report incidents.

4. Establish and maintain:
   - A systematical approach to manage cyber security.
   - Suitable security measures.
   - Training for management and employees.



(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.

Part-IS.I.OR & NIS2 Mapping

Aligned with regulatory obligations under a risk-based approach

Part-IS.I.OR Code	NIS2 Article
IS.I.OR.100 ISMS	Art. 21(2) Risk management measures
IS.I.OR.105 Policy	Art. 20 Management responsibility
IS.I.OR.110 Roles	Art. 20(2) Management oversight
IS.I.OR.200 Risk ID	Art. 21(2)(a) Risk analysis
IS.I.OR.205 Risk Assessment	Art. 21(2)(a) Risk analysis policies
IS.I.OR.210 Risk Treatment	Art. 21(2) Technical measures
IS.I.OR.215 Internal Reporting	Art. 21(2)(f) Effectiveness assessment
IS.I.OR.220 Incidents	Art. 21(2)(b) Incident handling
IS.I.OR.225 External Reporting	Art. 23 24h CSIRT reporting
IS.I.OR.230 Corrective Actions	Art. 21(2)(f) Effectiveness policies
IS.I.OR.235 Suppliers	Art. 21(2)(d) Supply chain security
IS.I.OR.240 Training	Art. 21(2)(g) Cyber hygiene training
IS.I.OR.250 ISMM	Art. 21(5) Documentation
IS.I.OR.260 Continuous Improvement	Art. 21(2) All measures reviewed

1. Management responsibilities.
2. Training & Awareness.
3. **Evidence-based cyber risk management to make informed decisions. Own and Third Parties.**
4. Incident response and business continuity capabilities and communication.
5. Formal documentation (policies, procedures).

2. Fundamental concepts you should understand regarding the measurement of cyber risk

Don’t confuse **Cybersecurity Maturity Assessments** with **Cyber Risk Management Processes**

Cybersecurity Maturity Assessment

It provides information on **the extent and depth to which IT/OT cybersecurity programs** (controls, policies, procedures, activities) are implemented. It measures current maturity **using a rating scale.**

Others:

- ISO/IEC 27002:2022 - Information security, Cybersecurity and privacy protection
- CIS Critical Security Controls Version 8.1
- NIST SP 800-82 rev.3 - Guide to Operational Technology (OT) Security
- ISA/IEC 62443 series

Cyber Risk Management Processes

It entails the **identification, assessment and treatment** (mitigation or transfer) of cyber risk. We always need to assess two main variables: **Impact and Likelihood (or Frequency).**

Qualitative

- ISO/IEC 27005:2022 - Guidance on managing information security risks
- NIST SP 800-30 - Guide for Conducting Risk Assessments

Quantitative

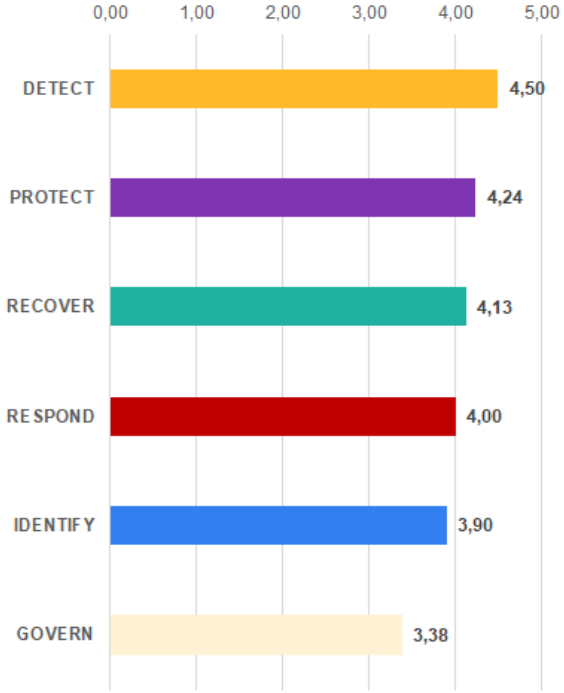
- Applied Information Economics (AIE)
- FAIR Core
- FAIR-CAM (Controls Analytics Model)
- FAIR-MAM (Materiality Assessment Model)
- FAIR TAM
- Open FAIR

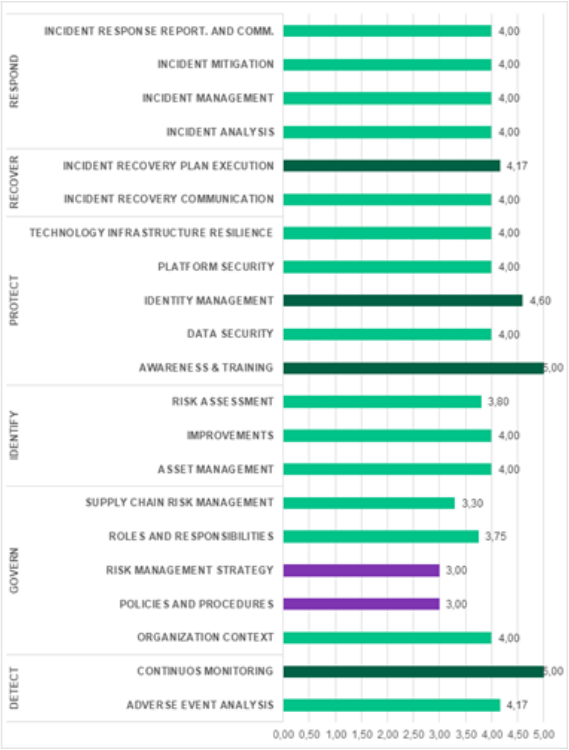
Don’t confuse **Cybersecurity Maturity Assessments** with **Cyber Risk Management Processes**

Cybersecurity Maturity Assessment

1. You measure your risk with a rating (and a peer comparison).
2. It helps you identify gaps and areas for improvement.
3. It´s the basis for designing a cybersecurity roadmap.
4. It´s used to assess the likelihood and impact of risks (as part of a Cyber Risk Management Process).

The Organization´s cybersecurity maturity level (rating) obtained against the **NIST CSF 2.0** is **3,91 out of 5.00**. This result means Organization's IT Cybersecurity Program has a **HIGH** maturity level.

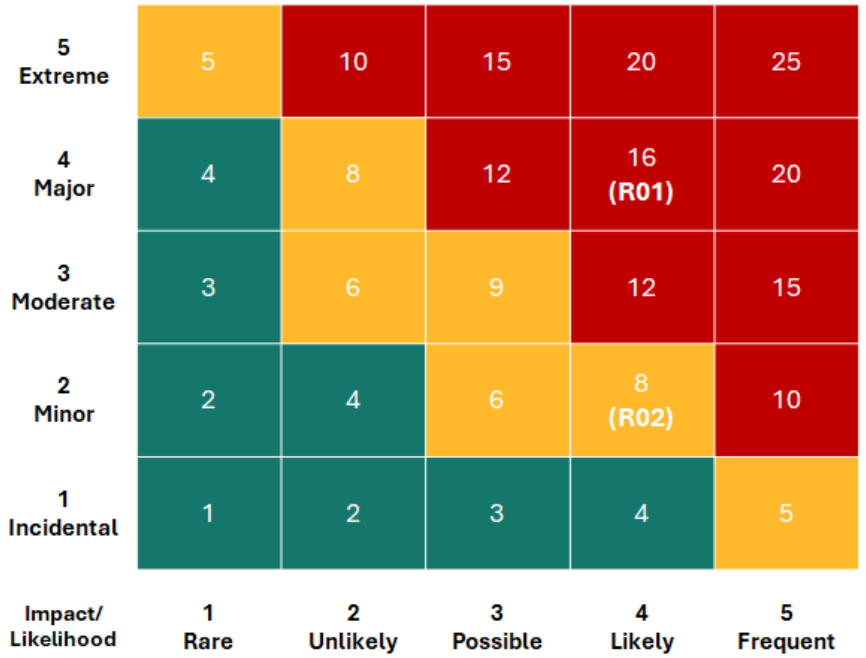




Don’t confuse **Cybersecurity Maturity Assessments** with **Cyber Risk Management Processes**

Cyber Risk Management Processes (Qualitative)

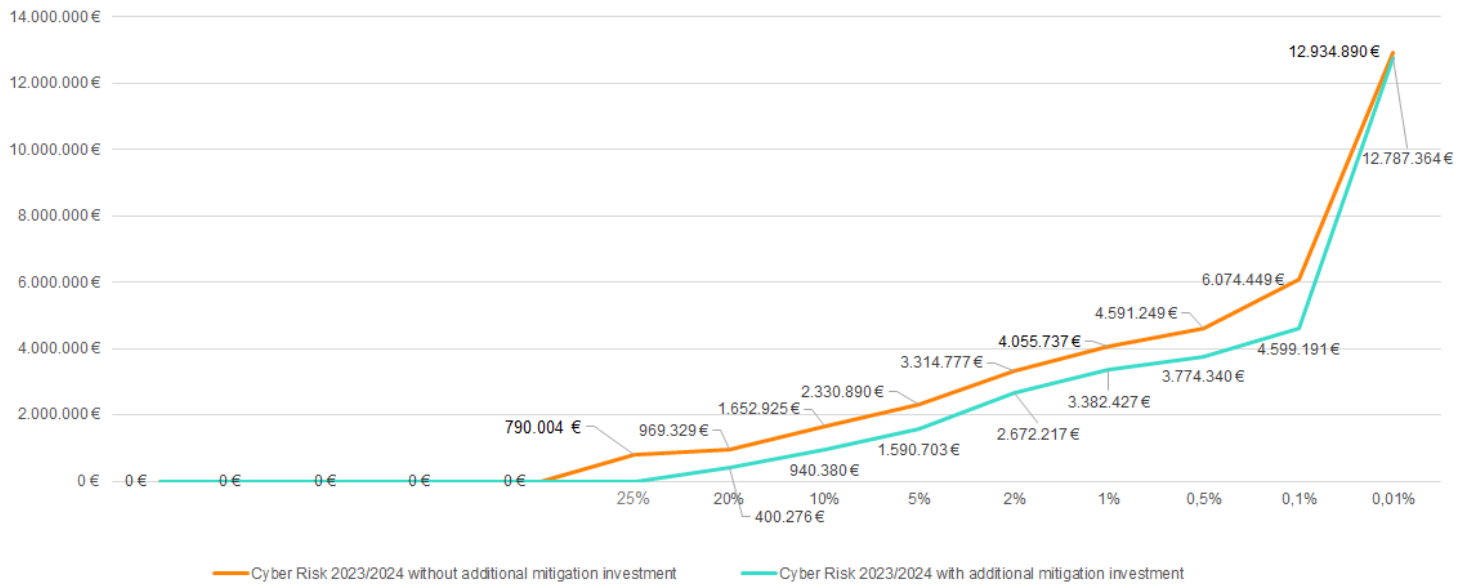
Qualitative
Working with **asset and threat catalogs**
Likelihood estimation with **scales** (1 to 5, or high/medium/low)
Impact estimation, mostly technical, with **scales. For example,** (1 to 5, or high/medium/low)
Deliverable based on **risk map or matrix**



Don’t confuse **Cybersecurity Maturity Assessments** with **Cyber Risk Management Processes**

Cyber Risk Management Processes (Quantitative)

Quantitative
Working with **customized scenarios**
Likelihood estimation (range) based on **historical data, certainty, Bayesian methods, etc.**
Impact estimation (range) based on **cyber loss types** (with a 90% confidence interval)
Deliverable based on **Excess Loss Curve**



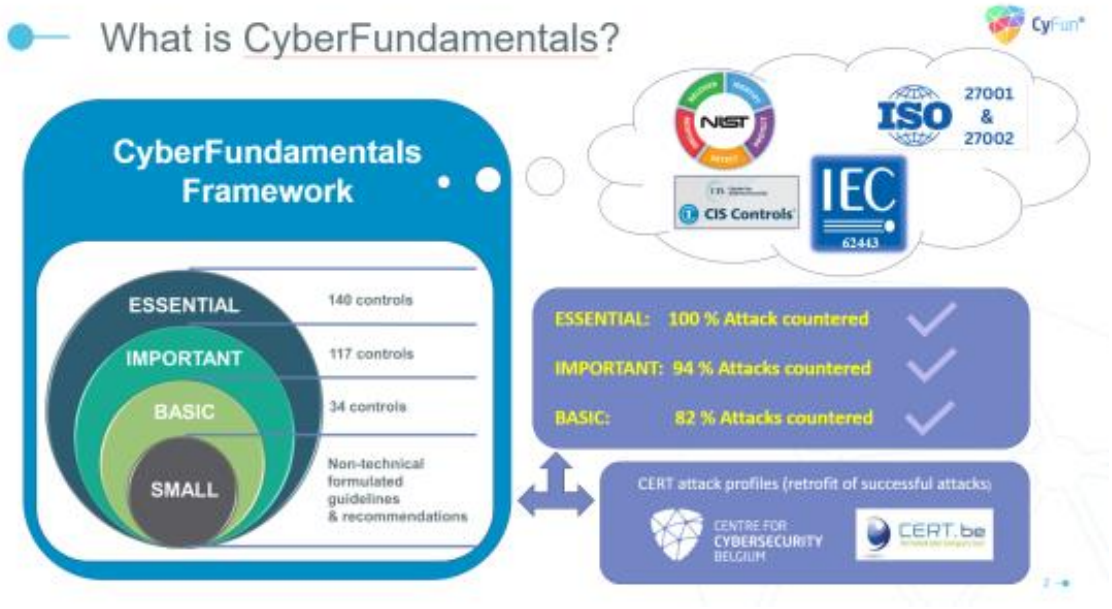
Don’t confuse **Cybersecurity Maturity Assessments** with **Cyber Risk Management Processes**

The EASA Part-IS and the NIS2 Directive (Art.20 and Art. 21.1) asks organizations to conduct both exercises: a **Cybersecurity Maturity Assessment** and a **Cyber Risk Management Process.**

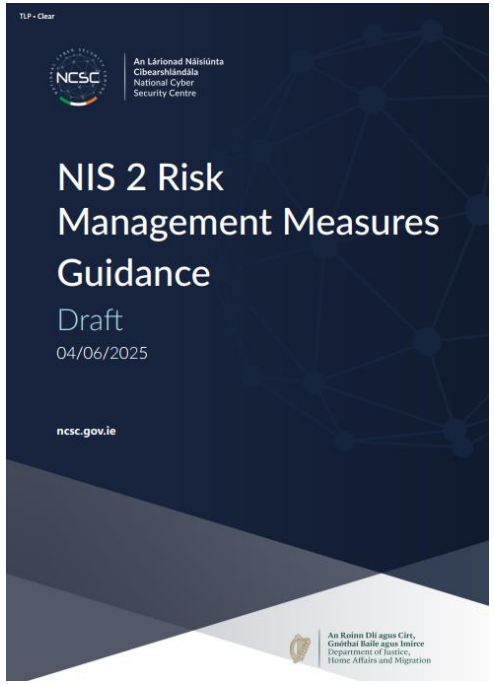
3. Practical application of these concepts within the context of the EASA Part-IS and the NIS2 Directive in Ireland

Cyber Fundamentals Framework (CyFun) & NIS2 RMMG

Conduct a **Cybersecurity Maturity Assessment** to align with EASA Part-IS and mainly the NIS2 requirements, measure your current cyber posture, and establish a foundation for improving resilience.



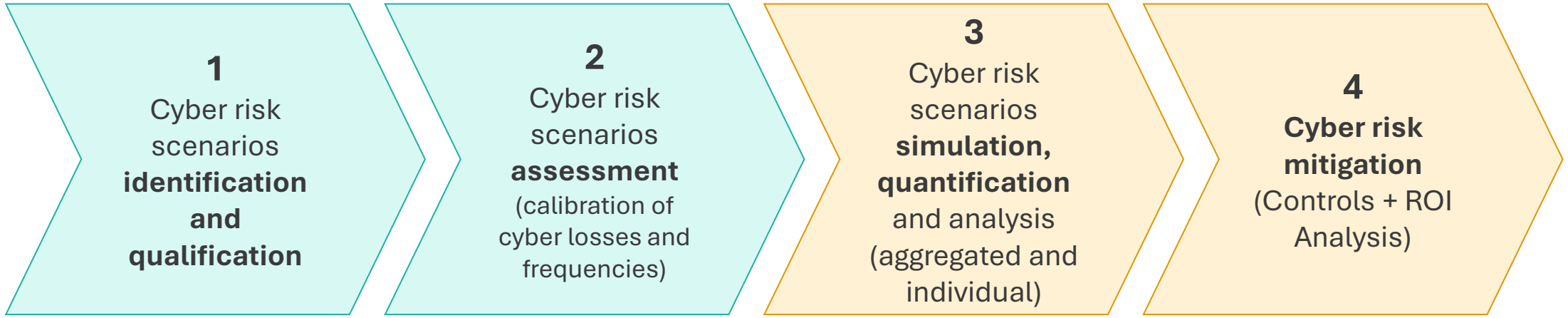
https://cyfun.eu/en/cyfun-2025
https://www.ncsc.gov.ie/CyFun/



NIS2 RMMG

Tailored Quantitative Cyber Risk Management Process

Implement a **Quantitative Cyber Risk Management Process** to align with EASA-Part IS and NIS2 requirements, quantify your current cyber exposure in financial terms, and strategically allocate your mitigation and transfer investments.



Tailored Quantitative Cyber Risk Management Process

The Hybrid Threat - The Evidences

On September 19, 2025, Dublin Airport experienced a major security alert that prompted the evacuation of Terminal 2 after a **suspicious piece of luggage was discovered**.

Following a thorough investigation, authorities confirmed the item was harmless, allowing normal airport operations to resume.

At the same time, a **Europe-wide cyberattack**, specifically the **HardBit Ransomware**, affected major airports including London Heathrow, Brussels, Berlin, as well as **Dublin and Cork**.

The attackers targeted **Collins Aerospace's ARINC cMUSE (Multi-User System Environment)**, a vital infrastructure for check-in and boarding.

As a result, airports were forced to switch to manual passenger processing, leading to significant delays.

Aer Lingus, among other airlines, was particularly impacted by the ransomware attack.

Additionally, **drone incursions** have been observed in similar contexts, contributing to what some European officials describe as **hybrid threats**, **blending physical disruptions with cyber risks to compromise airport security.**

Tailored Quantitative Cyber Risk Management Process

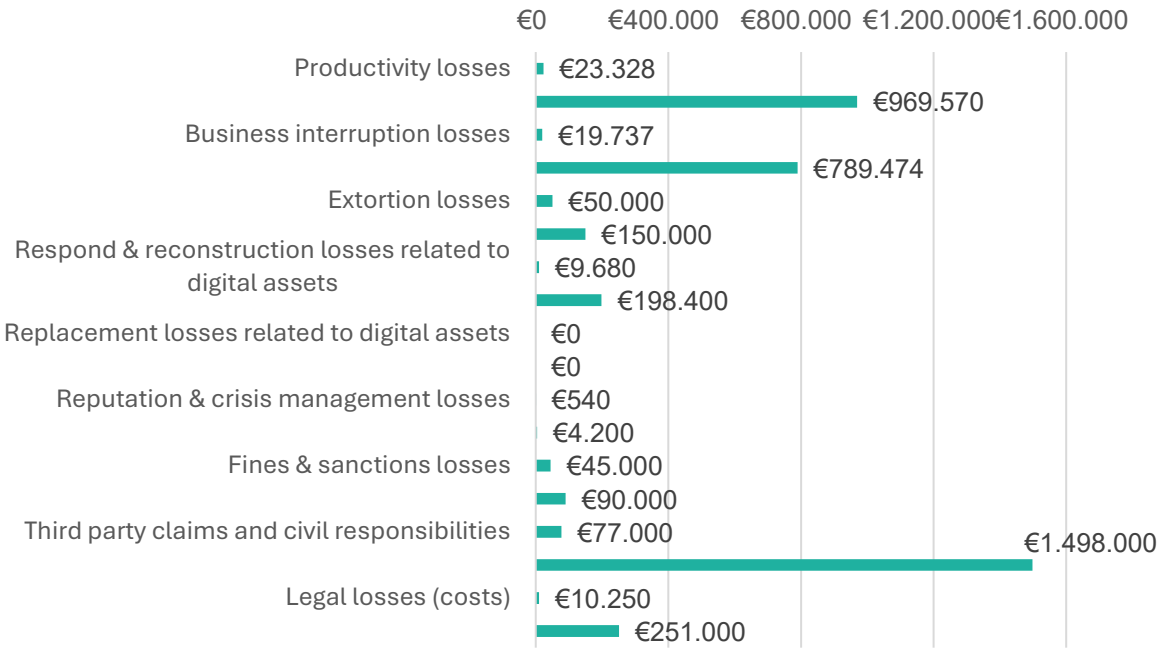
Identifying Cyber Risk Scenarios (based on actual incidents)

ID	Scenario definition	Threat	Assets	Affects	Environment & Deployment	Agents
S01	Ransomware infection on a **critical third-party software** provider cripples the **check-in and baggage handling systems** across the airport. This disruption forces airport staff and airlines to revert to manual operations, causing widespread delays, significant passenger congestion, and operational chaos. The incident results in prolonged **business interruption**, substantial recovery costs, and complex third-party liability claims.	**Ransomware**	**Check-in and baggage handling systems**	Integrity and confidentiality	IT-On Premise (Third Party)	Ransomware Gang / External Agent / APT Group
S02	The attackers escalate their access and **exfiltrate sensitive customer PII data** from the **Customer Service Portal (CSP).** The breach results in reputational damage, regulatory scrutiny, and potential legal consequences.	**Data Breach**	**PII Data (CSP)**	Confidentiality	IT-Cloud (Third Party)	Ransomware Gang / External Agent / APT Group

Tailored Quantitative Cyber Risk Management Process

S02- Data Breach PII Data (Customer Service Portal)

Lower bound (90% CI)	Upper bound (90% CI)
235.535 €	3.950.644 €

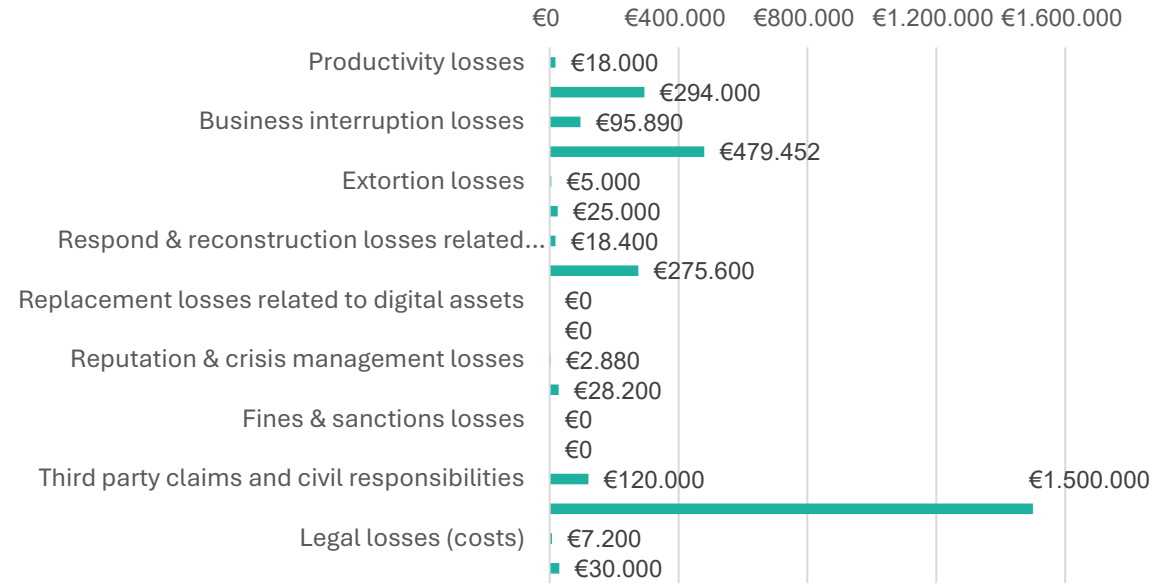


Annual Frequency

Best Case	Most Likely	Worst Case
0,07	0,1	0,25

S01- Ransomware - Check-in and baggage handling systems

Lower bound (90% CI)	Upper bound (90% CI)
267.360 €	2.632.252 €

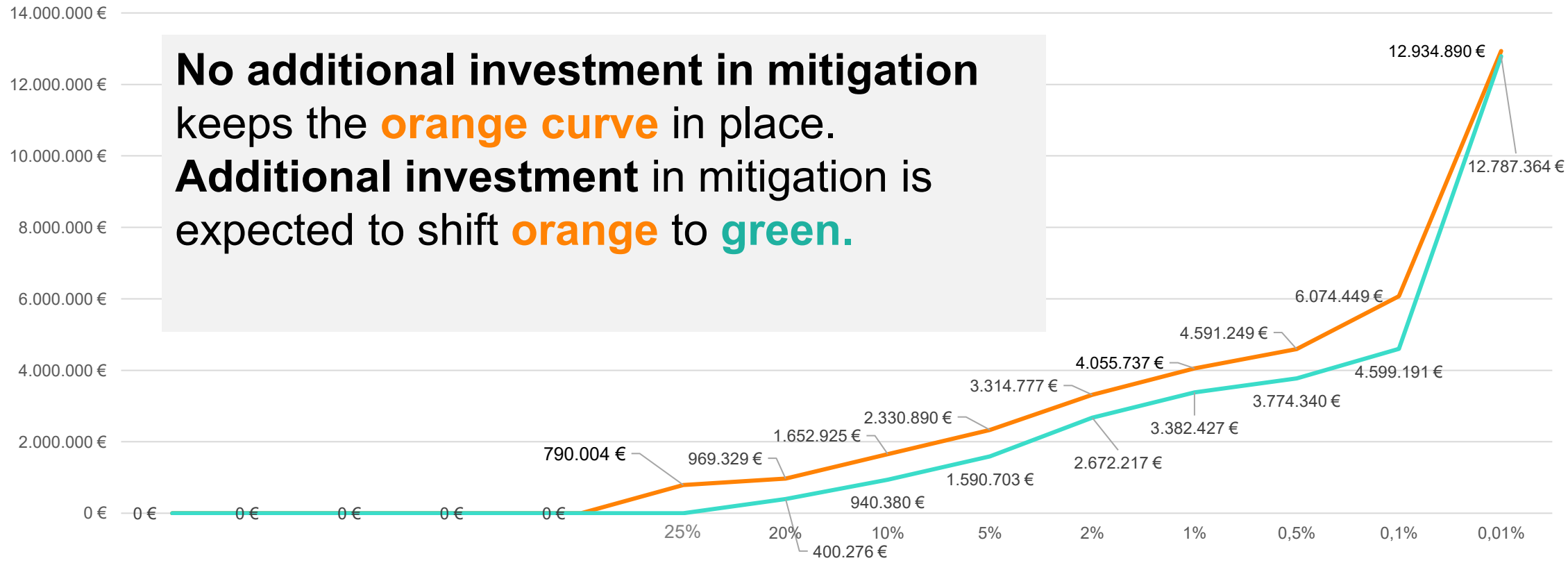


Annual Frequency

Best Case	Most Likely	Worst Case
0,14	0,33	0,5

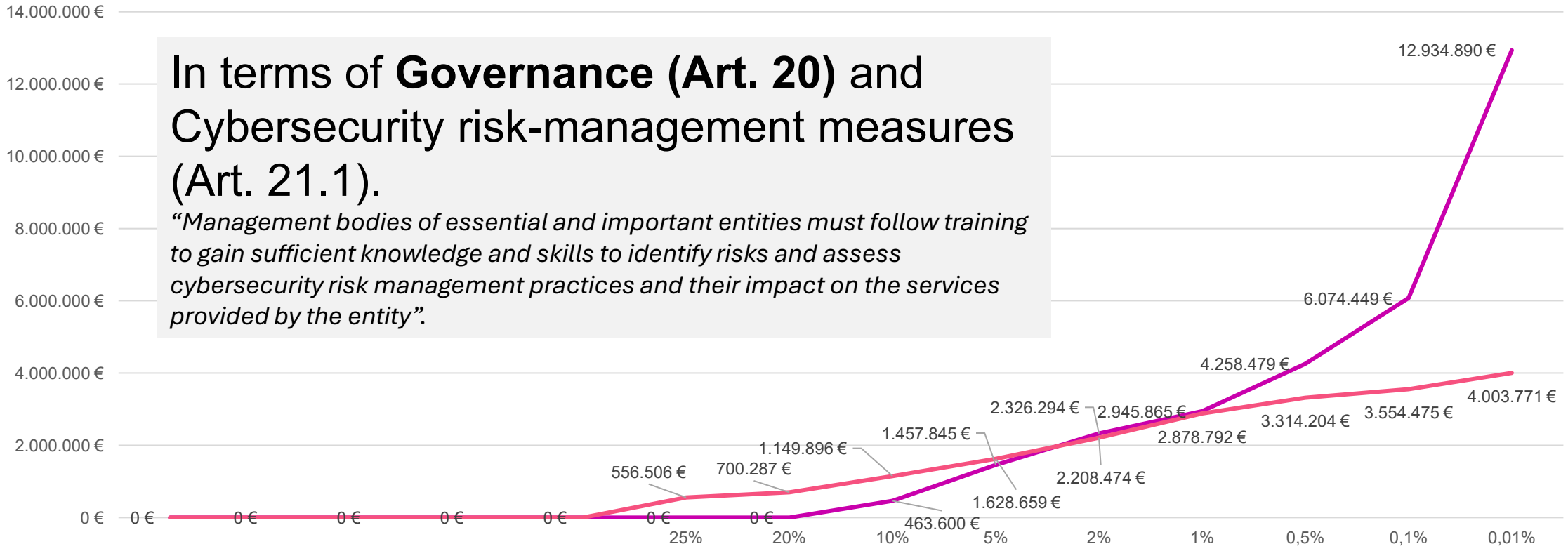
Tailored Quantitative Cyber Risk Management Process

Aggregated results after applying Montecarlo Simulation



Tailored Quantitative Cyber Risk Management Process

Individual results per scenario after applying Montecarlo Simulation



In terms of **Governance (Art. 20)** and Cybersecurity risk-management measures (Art. 21.1).

"Management bodies of essential and important entities must follow training to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity".

S02- Data Breach PII Data (Customer Service Portal)	
Lower bound (90% CI)	Upper bound (90% CI)
235.535 €	3.950.644 €

S01- Ransomware - Check-in and baggage handling systems	
Lower bound (90% CI)	Upper bound (90% CI)
267.360 €	2.632.252 €

4. Adopting a structured roadmap to strengthen resilience while ensuring EASA Part-IS and NIS2 alignment

Whether or not you fall under the EASA Part IS or/and NIS2 scope, measure and understand your cyber risk to make informed decisions

1-Assess **external exposure and pinpoint weaknesses** adversaries could exploit to access your systems.

2-Conduct a **Cybersecurity Maturity Assessment** using a recommended standard. Under EASA Part IS/NIS2 in Ireland, prefer CyFun.

3 -Adopt a **Cyber Risk Management Process** to measure the exposure, likelihood, and impact of incidents (NIS2, Art. 21.1).

4-Define a **cybersecurity roadmap** based on these exercises: identify key gaps, prioritize actions, allocate investment, and ensure NIS2 compliance.

5-**Brief the board on main outcomes**. Management must be trained to assess risks, practices, and impacts (Art. 20 NIS2).

6-**Implement actions**, reassess cyber risk, and establish continuous improvement.

Lean on a **third party to avoid bias**, too "optimistic" outcomes, and an unstructured approach (save time). The outcomes delivered by the third party can be used to communicate your cyber risk posture to customers and stakeholders.

Evidence-based Cyber Risk Measurement

To **understand** your **cyber risk exposure**. To **make informed decisions** on your **mitigation** and **transfer** strategies. To **reduce risk and cost.**

What are your needs and main concerns?		What do we do?	What do you get? Outcomes & Benefits
DISCOVER	Do you have vulnerable exposed IT or OT assets, or public or leaked information, such as credentials or sensitive data, that adversaries could exploit for unauthorized access?	**Cyber Reconnaissance & Initial Access Testing**	✓ Reduce the risk an adversary can cause an incident. ✓ Transform technical evidence into risks and mitigate them. ✓ Avoid false positive information in front of carriers.
ASSESS	Are your IT and OT cybersecurity controls effective? What is your maturity level compared to your peers? How do you prioritize remediation? How do you manage third-party risks?	**Cybersecurity Maturity Assessment & Cybersecurity Roadmap**	✓ Boost your maturity rating, benchmark against peers, and focus on the most impactful risk mitigation actions. ✓ Meet insurer standards for improved cyber coverage.
QUANTIFY	What is the financial impact or economic losses (including Maximum Possible Loss) that different cybersecurity incidents (tailored scenarios) can generate in your organization?	**Tailored Cyber Risk Quantification & Management**	✓ Reduce cost or risk by avoiding being over or under insured. ✓ Reduce cost or risk by optimizing mitigation investment and cyber insurance deductible, limit and premium.
RESPOND	How can you swiftly respond to a cybersecurity incident? Do you have a Cyber Incident Response plan? Have you simulated it? Is everyone aware of what to do?	**Cyber Incident Response Plan & Crisis Simulation**	✓ Reduce downtime, reaction time, data loss, and business interruption impact. ✓ Encourage collaboration across key teams.
ALIGN	Which are the main cybersecurity regulations (NIS2, DORA, AI Act, CRA) that you must comply with? What's your existing GAP to be aligned with the obligations?	**Regulation GAP Assessment & Roadmap**	✓ Minimize the risk of fines and enforcement actions. ✓ Empower your cyber profile in front of insurers and 3rd parties. ✓ Increase operational resilience.

Deep Dive Cybersecurity Consulting & Engineering services to measure emerging risks: AI and Microsoft Entra ID & Azure Risks

AI RISK MANAGEMENT

- AI Risk Management Training
- AI Risk Management Process
- AI Incident Response Plan & Simulation

ENTRA ID & AZURE RISK MANAGEMENT

- The Hidden Risk of Entra ID & Azure (Training)
- Entra ID & Azure Assessment
- Testing your SOC with Entra ID & Azure events

Fernando Sevillano Ph.D.

Head of Cyber & Tech Consulting Team (FINEX, Western Europe)

fernando.sevillano@wtwco.com