# PART - Information Security

Seminář pro provozovatele OLD 2025

Michal Parýzek

# Úvod

1. Safety vs. Security
2. PART – IS
3. Požadavky na organizace
4. Legislativní prostředí
5. Implementace
6. Dotazy

# IS – Information Security

Dvě různé novinky – mají společné téma:

1. Evropská směrnice NIS 2 a nový národní zákon o kybernetické bezpečnosti

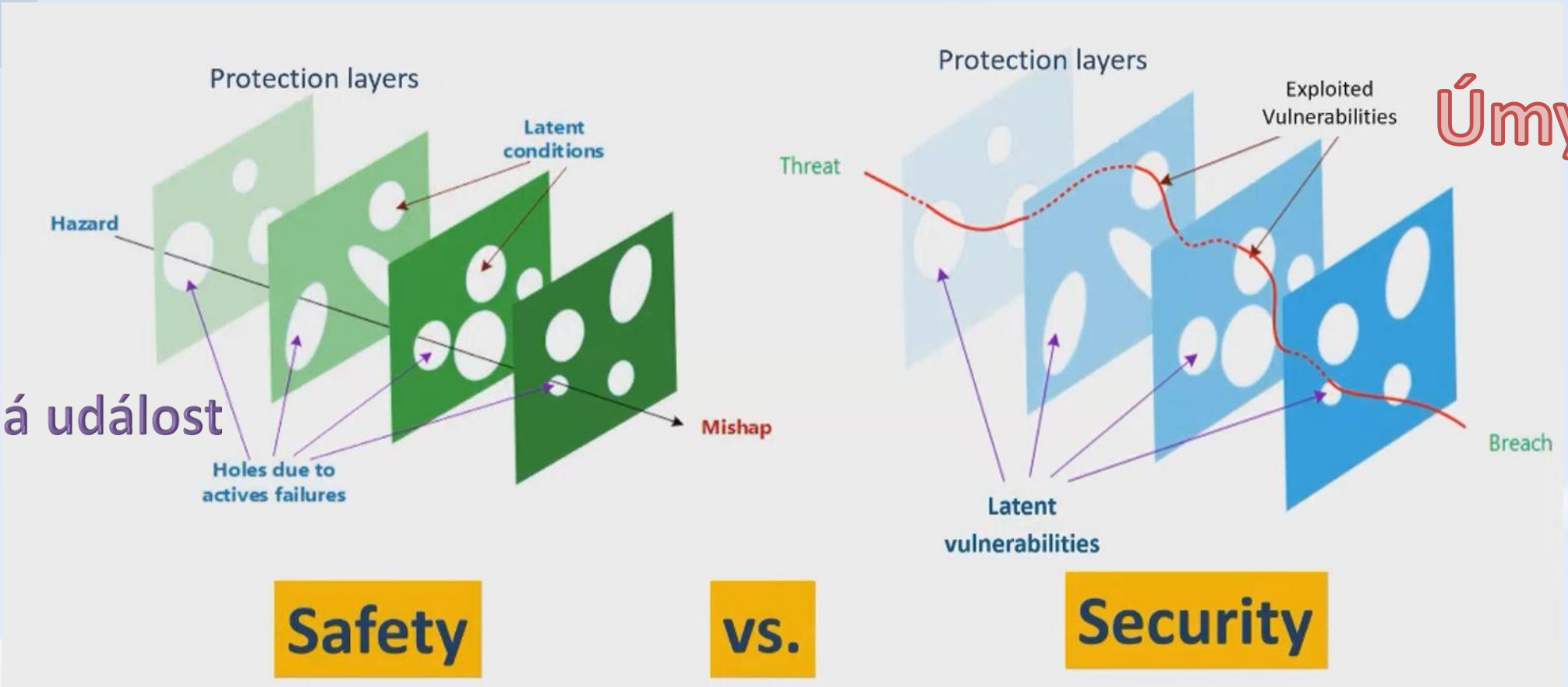
SECURITY

2. Part-IS – Prováděcí nařízení Komise (EU) 2023/203 a související AMC a GM

AVIATION SAFETY

# Safety x Security

Nahodilá událost

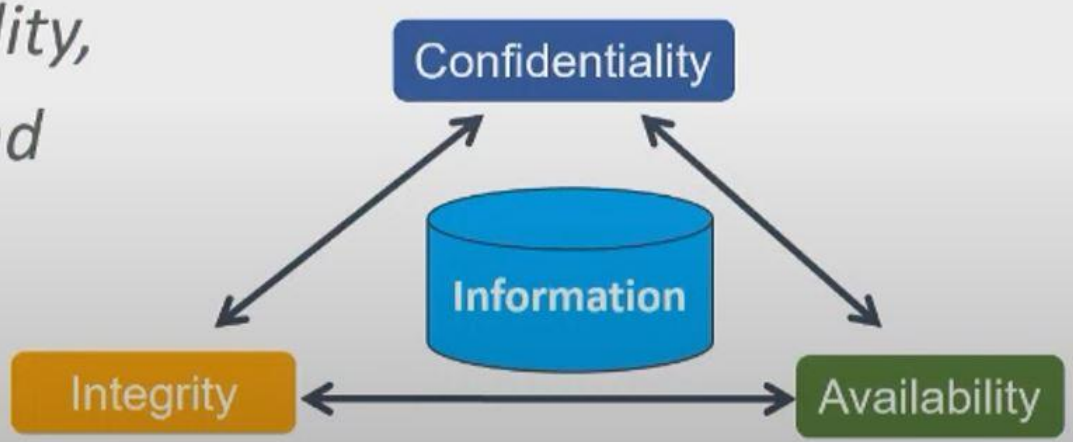



Úmysl

# Safety x Security

## What is Information Security Management?

- ISO 27000 states that ***Information Security Management*** *is a top-down, business driven approach to the management of an organization's physical and electronic information assets in order to preserve their*
  - *Confidentiality,*
  - *Integrity, and*
  - *Availability.*



# ISMS - definice

## ISO 27001

An ISMS is the means by which management monitors and controls information security, minimizing the residual **business risk** and ensuring that information security continues to fulfill corporate, customer and legal requirements.

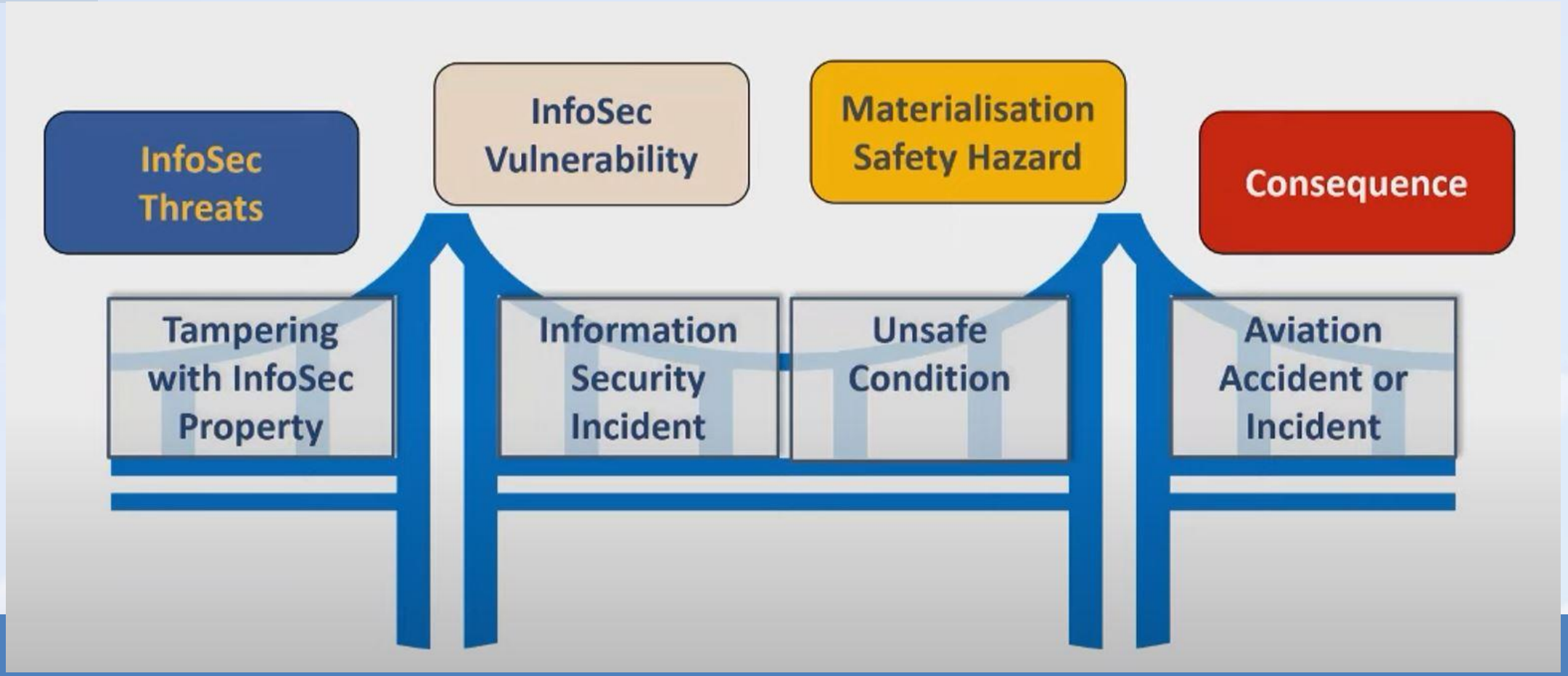
## Part-IS

An ISMS is the means by which management monitors and controls information security, minimizing the residual business **safety risk** and ensuring that information security continues to fulfill ~~corporate, customer and~~ legal requirements and societal expectations.

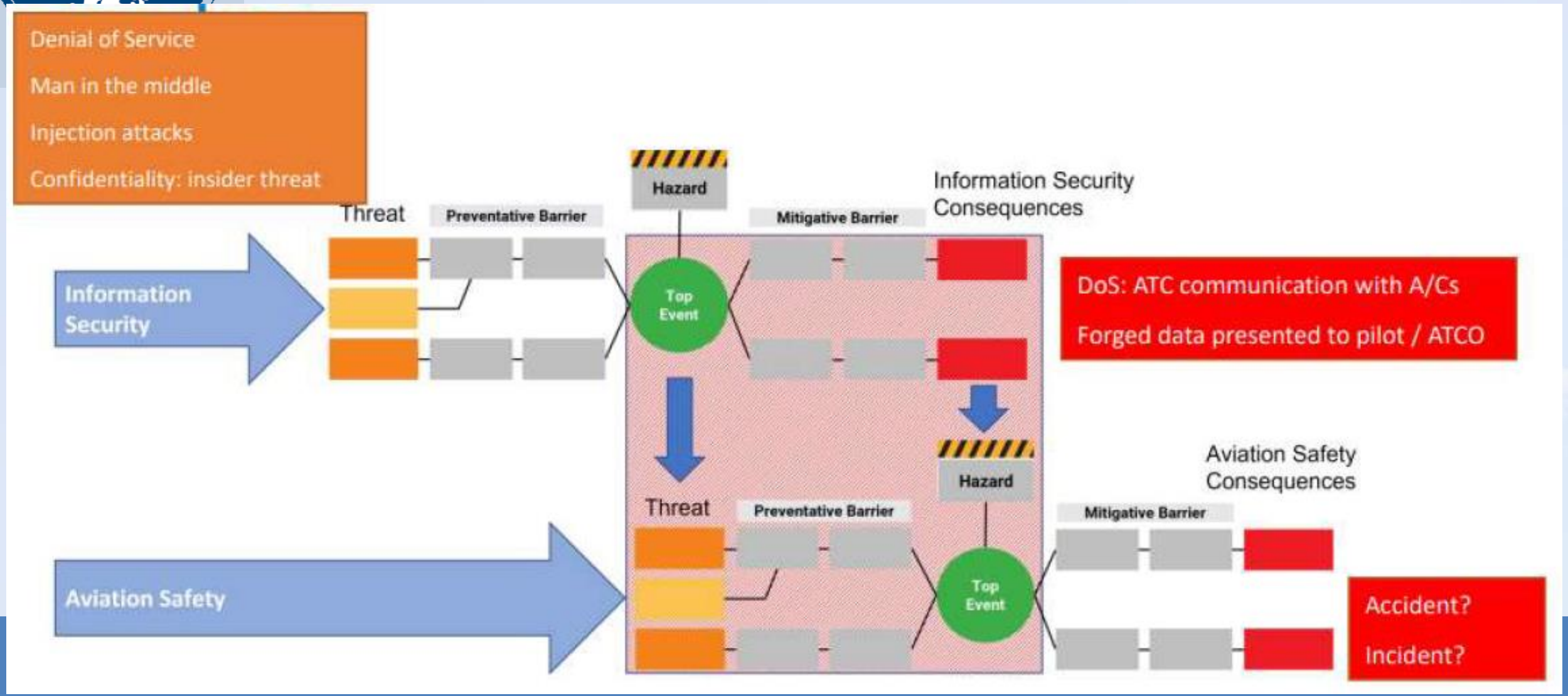
# PART-IS

| | |
|---|---|
| **Objective** | Protect the aviation system from information security risks **with potential impact on aviation safety** |
| **Scope** | Information and communication technology systems and data used by Approved Organisations and Authorities for civil aviation purposes |
| **Activity** | - **identify and manage** information security risks related to information and communication technology systems and data used for civil aviation purposes;<br>- **detect** information security events, identifying those which are considered information security incidents; and<br>- **respond** to, and **recover** from, those information security incidents |

# PART-IS – most mezi SECURITY a SAFETY



# PART-IS – most mezi SECURITY a SAFETY



# PART-IS – předpisová základna

## Implementing Rules (IRs) (Commission Regulations)

| Incorporated Regulation | Regulation amendment | Applicability date[1] |
|---|---|---|
| Regulation (EU) 2023/203 | Initial issue | 22/2/2026[2] |
| Regulation (EU) 2023/1769 | n/a | 5/10/2023 |
| Regulation (EU) 2024/1109 | n/a | 1/5/2024 |

## Delegated Rules (DRs) (Commission Regulations)

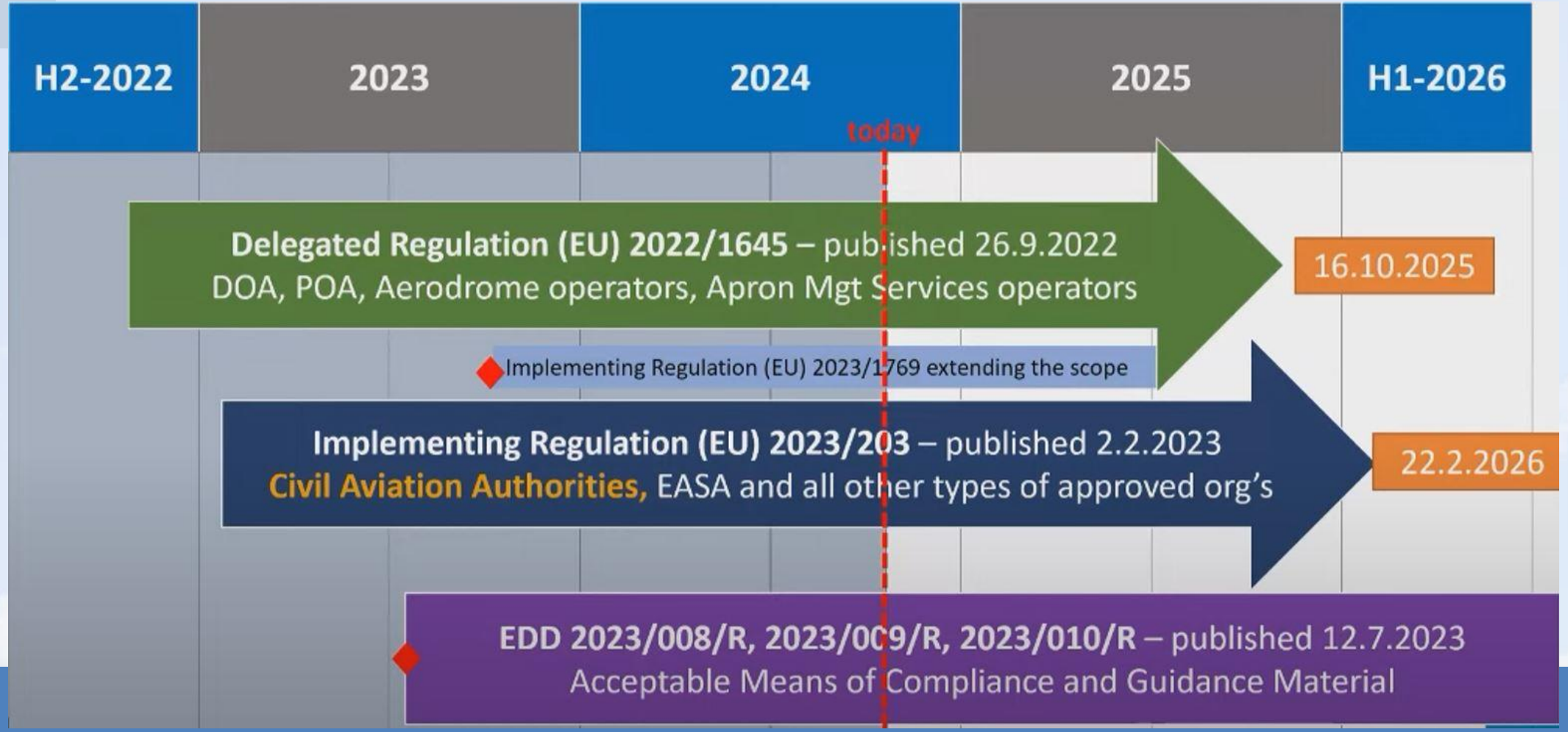
| Incorporated Regulation | Regulation amendment | Applicability date |
|---|---|---|
| Regulation (EU) 2022/1645 | Initial issue | 16/10/2025 |

## AMC & GM to IRs (ED Decisions)

| Incorporated ED Decisions | AMC/GM Issue No, Amendment No | Applicability date |
|---|---|---|
| ED Decision 2023/008/R | Issue 1 | 22/2/2026 |
| ED Decision 2023/009/R | Issue 1 | 22/2/2026 |
| ED Decision 2023/010/R | Issue 1 | 22/2/2026 |


easa.europa.eu/en/document-library/easy-access-rules

# PART-IS – časová osa



# PART-IS - obsah

- Obsah – vlastní nařízení
- Annex I – požadavky na úřady IS.AR.xxx
- Annex II – požadavky na organizace IS.I.OR.xxx
- Annex III – Part-ARA a Part –ORA k nařízení 1178/2011 (FCL)

  .
  .
  .
- Annex V – Part-ARO a Part-ORO k nařízení 965/2012 (OPS)

# PART-IS - obsah

- Ob
- An
- An
- An CL)
- An )


ANNEX III — INFORMATION SECURITY — ANNEXES VI (Part-ARA) and VII (Part-ORA) to Regulation (EU) No 1178/2011 ..... 179

ANNEX IV — INFORMATION SECURITY — Annex I (Part 21) to Regulation (EU) No 748/2012 ..... 180

ANNEX V — INFORMATION SECURITY — Annexes II (Part-ARO) and III (Part-ORO) to Regulation (EU) No 965/2012 ..... 181

ANNEX VI — INFORMATION SECURITY — Annex II (Part-ADR.AR) to Regulation (EU) No 139/2014 ..... 182

ANNEX VII — INFORMATION SECURITY — Annexes II (Part-145), III (Part-66) and Vc (Part-CAMO) to Regulation (EU) No 1321/2014 ..... 183

ANNEX VIII — INFORMATION SECURITY — Annexes II (Part ATCO.AR) and III (Part ATCO.OR) to Regulation (EU) 2015/340 ..... 184

ANNEX IX — INFORMATION SECURITY — Annexes II (Part-ATM/ANS.AR) and III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 ..... 185

# PART-IS – Annex V

EASA

*First Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645)*

*Implementing Regulation (EU) 2023/203*

## ANNEX V — INFORMATION SECURITY — ANNEXES II (PART-ARO) AND III (PART-ORO) TO REGULATION (EU) NO 965/2012

For the consolidated version of Part-ARO and Part-ORO, please refer to the Easy Access Rules for Air Operations (Regulation (EU) No 965/2012).

# PART-IS vs. (EU) 965/2012

## ORO.GEN.200A Information security management system

*Regulation (EU) 2023/203*

In addition to the management system referred to in point ORO.GEN.200, the operator shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.

*[applicable from 22 February 2026 — Implementing Regulation (EU) 2023/203]*

# Dopady do jednotlivých Nařízení

| Area \ Part | Reg. 1178 ORA | Reg. 748 21 | Reg. 965 ORO | Reg. 139 ADR | Reg. 340 ATCO | Reg. 373 ATM/ANS | Reg. 1321 CAMO | Reg. 1321 145 |
|---|---|---|---|---|---|---|---|---|
| Hook to ISMS | .GEN.200A | .A.139A<br>.A.239A | .GEN.200A | .OR.D.005A<br>.OR.D.007<br>.OR.F.045A | .OR.C.001A | .OR.B.005A<br>.OR.D.010 | .A.200A | .A.200A |

| Area \ Part | Reg. 1178 ARA | Reg. 748 21 | Reg. 965 ARO | Reg. 139 ADR | Reg. 340 ATCO | Reg. 373 ATM/ANS | Reg. 1321 CAMO | Reg. 1321 145 | Reg. 1321 66 |
|---|---|---|---|---|---|---|---|---|---|
| Hook to ISMS | .GEN.200 | .B.25 | .GEN.200 | .AR.B.005 | .AR.B.001 | .AR.B.001 | .B.200 | .B.200 | .B.15 |
| Imm. React. to IS Reports | .GEN.125<br>.GEN.135A | .B.15<br>.B.20A | .GEN.125<br>.GEN.135.A | .AR.A.025<br>.AR.A.030A | .AR.A.020<br>.AR.A.025A | .AR.A.020<br>.AR.A.025A | .B.125<br>.B.135A | .B.125<br>.B.135A | N/A |
| Oversight | .GEN.300<br>.GEN.330A | .B.221<br>.B.240A<br>.B.431<br>.B.435A | .GEN.300<br>.GEN.330A | .AR.C.005<br>.AR.C.040A | .AR.C.001<br>.AR.E.010A | .AR.C.010<br>.AR.C.025A | .B.300<br>.B.330A | .B.300<br>.B.330A | N/A |
| Allocation of tasks | .GEN.205 | .B.30 | .GEN.205 | .AR.B.010 | .AR.B.005 | .AR.B.005 | .B.205 | .B.205 | N/A |

# PART-IS - Předmět

*Článek 1*

**Předmět**

Toto nařízení stanoví požadavky, které musí organizace a příslušné orgány splnit s cílem:

a) identifikovat a řídit rizika v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví, která by mohla ovlivnit systémy a údaje informačních a komunikačních technologií používaných pro účely civilního letectví;

b) zjistit události v oblasti bezpečnosti informací a určit ty, které jsou považovány za incidenty v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví;

c) reagovat na tyto incidenty v oblasti bezpečnosti informací a zotavit se z nich.

# PART-IS – oblast působnosti

c) letečtí provozovatelé, na které se vztahuje příloha III (část ORO) nařízení (EU) č. 965/2012, s výjimkou těch, kteří se podílejí výhradně na provozu některého z následujících letadel:

i) letadlo ELA2 podle definice v čl. 1 odst. 2 písm. j) nařízení (EU) č. 748/2012;

ii) jednomotorové vrtulové letouny s maximální provozní konfigurací sedadel pro cestující 5 nebo méně, které nejsou klasifikovány jako složitá motorová letadla, při vzletu a přistání na stejném letišti nebo provozním místě a při provozu podle pravidel letu za viditelnosti ve dne;

iii) jednomotorové vrtulníky s maximální provozní konfigurací sedadel pro cestující 5 nebo méně, které nejsou klasifikovány jako složitá motorová letadla, při vzletu a přistání na stejném letišti nebo provozním místě a při provozu podle pravidel letu za viditelnosti ve dne;

d) schválené organizace pro výcvik, na které se vztahuje příloha VII (část ORA) nařízení (EU) č. 1178/2011, s výjimkou těch, které se zabývají výhradně výcvikovými činnostmi u letadel ELA2 podle definice v čl. 1 odst. 2 písm. j) nařízení (EU) č. 748/2012 nebo se zabývají výhradně teoretickým výcvikem;

# PART-IS – IS.I.OR.200(e) - zmírnění

e) Aniž je dotčena povinnost dodržovat požadavky týkající se hlášení uvedené v nařízení (EU) č. 376/2014 a požadavky bodu IS.I.OR.200 písm. a) bodu 13, může příslušný úřad organizaci udělit oprávnění neprovádět požadavky uvedené v písmenech a) až d) a související požadavky uvedené v bodech IS.I.OR.205 až IS.I.OR.260, pokud ke spokojenosti uvedeného úřadu prokáže, že její činnosti, zařízení a zdroje, jakož i služby, které provozuje, poskytuje, přijímá a udržuje, nepředstavují ani pro ni, ani pro jiné organizace žádná rizika bezpečnosti informací s potenciálním dopadem na bezpečnost letectví. Schválení musí vycházet z dokumentovaného posouzení rizik bezpečnosti informací, které provede organizace nebo třetí strana v souladu s bodem IS.I.OR.205 a které přezkoumá a schválí její příslušný orgán.

Platnost tohoto schválení bude přezkoumána příslušným orgánem v návaznosti na příslušný cyklus dozorových auditů a vždy, když dojde ke změnám v rozsahu činnosti organizace.

# PART-IS – IS.I.OR.200(e)

## GM1 IS.I.OR.200(e) Information security management system (ISMS)

*ED Decision 2023/009/R*

Any organisation that believes that it does not pose any information security risk with a potential impact on aviation safety, either to itself or to other organisations, may consider requesting an approval for a derogation by the competent authority following the procedure outlined in AMC1 IS.I.OR.200(e).

Some examples of organisations that may consider asking for a derogation might include:

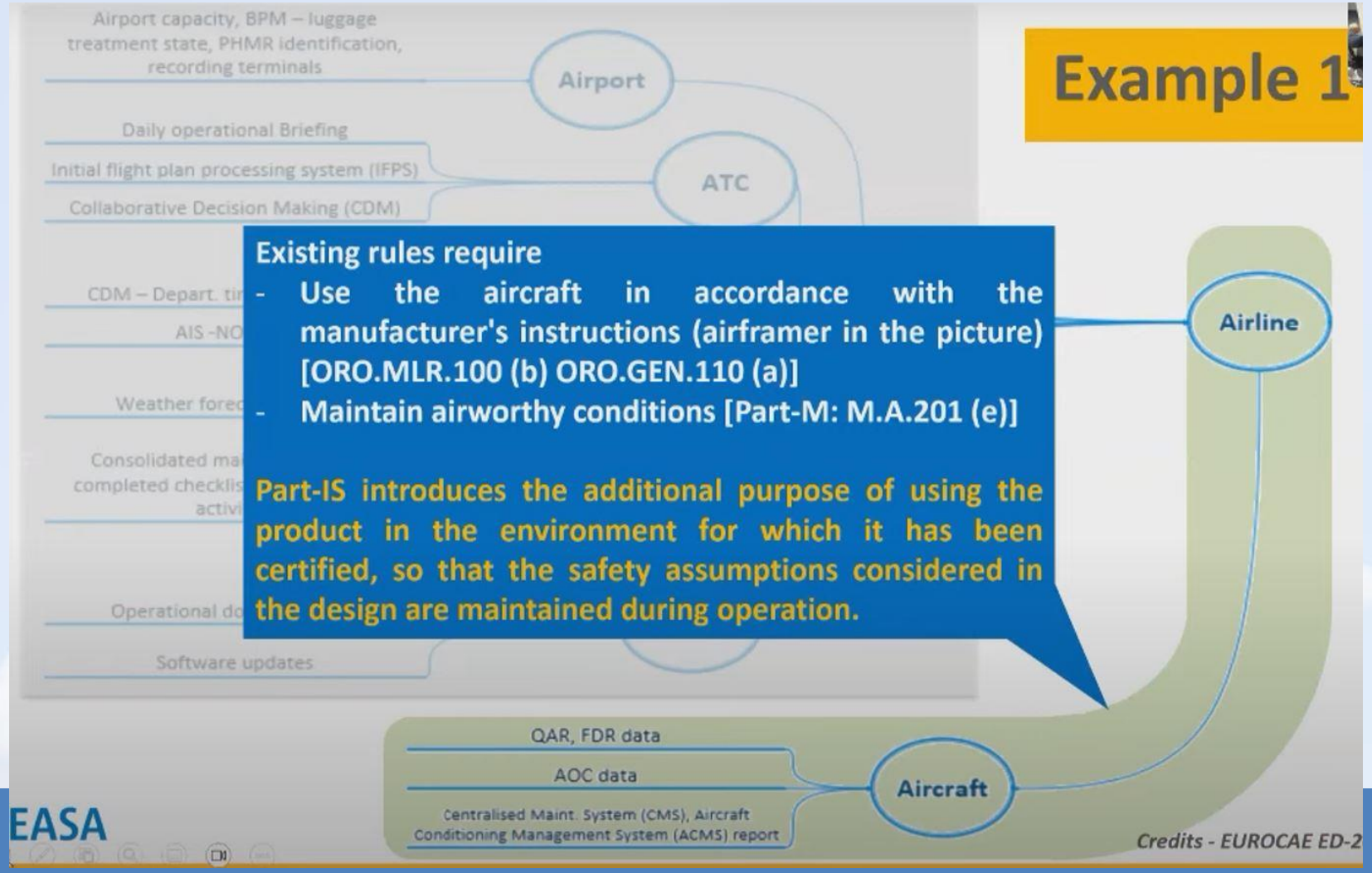
— An air operator that performs non-high-risk commercial specialised operations (SPO) with non-complex aircraft, if the nature of the operations justifies the grounds for a derogation.

— An air operator that operates ELA2 aircraft as defined in Article 1(2)(j) of Regulation (EU) No 748/2012 with the exception of one aircraft that is operated in predefined operational conditions or under certain operational limitations.

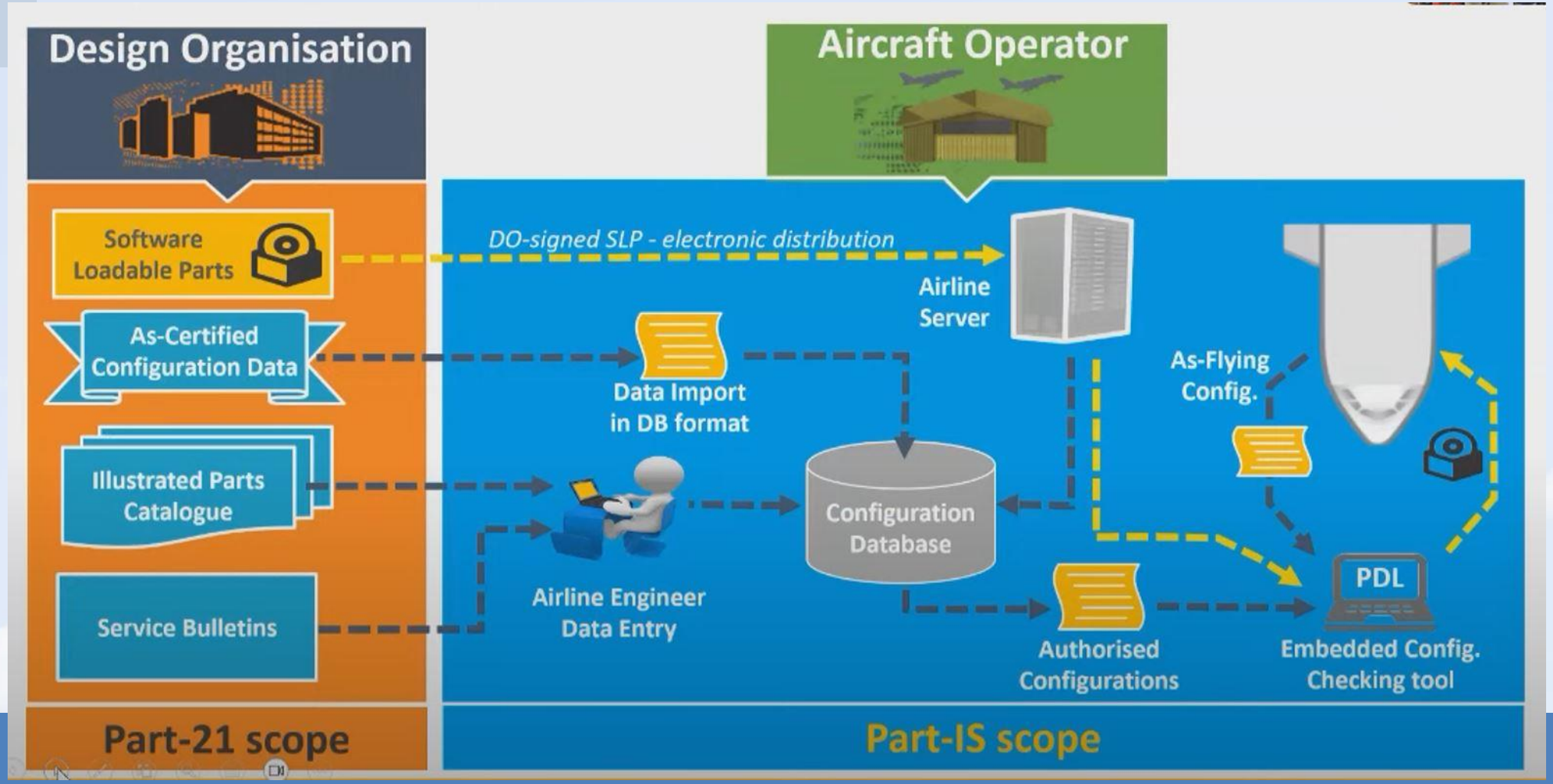
— A maintenance organisation approved under Part-145 dealing only with maintenance of components or maintenance activities that do not contribute to ensuring the structural integrity of the aircraft nor any major safety-related functionalities — for instance, undertaking activities such as washing, removing coatings, painting, etc.

The aforementioned examples are not exhaustive and are only indicative of potential scenarios that might provide an initial basis for the preparation of an information security risk assessment that justifies the exclusion of all elements of an organisation from the scope of the ISMS.

# PART-IS - příklad



# PART-IS - příklad



# PART-IS - požadavky

| ORGANISATION | Description | AUTHORITY |
|---|---|---|
| IS.I.OR.100 | Scope | IS.AR.100 |
| IS.I.OR.200 | Information security management system (ISMS) | IS.AR.200 |
| IS.I.OR.205 | Information security risk assessment | IS.AR.205 |
| IS.I.OR.210 | Information security risk treatment | IS.AR.210 |
| IS.I.OR.215 | Information security internal reporting scheme | |
| IS.I.OR.220 | Information security incidents — detection, response, and recovery | IS.AR.215 |
| IS.I.OR.225 | Response to findings notified by the competent authority | |
| IS.I.OR.230 | Information security external reporting scheme | ✓ |
| IS.I.OR.235 | Contracting of information security management activities | IS.AR.220 |
| IS.I.OR.240 | Personnel requirements | IS.AR.225 |
| IS.I.OR.245 | Record-keeping | IS.AR.230 |
| IS.I.OR.250 | Information security management manual (ISMM) | |
| IS.I.OR.255 | Changes to the information security management system | |
| IS.I.OR.260 | Continuous improvement | IS.AR.235 |

# IS.OR.200 Systém řízení IS (ISMS)

Za účelem dosažení cílů stanovených v článku 1 organizace vytvoří, zavede a udržuje systém řízení bezpečnosti informací (ISMS), který zajistí, že organizace:

1) ***stanoví politiku bezpečnosti informací***
2) ***identifikuje a přezkoumává rizika*** bezpečnosti informací
3) ***definuje a provádí opatření k řešení rizik*** bezpečnosti informací
4) ***zavede systém interního hlášení*** v oblasti bezpečnosti informací
5) ***definuje a provede opatření*** potřebná k odhalování událostí v oblasti bezpečnosti informací, určuje události, které jsou považovány za incidenty s možným dopadem na bezpečnost letectví, reaguje na tyto incidenty v oblasti bezpečnosti informací a odstraňuje jejich následky;
6) ***provádí opatření***, která příslušný orgán oznámil *jako* ***okamžitou reakci*** na incident nebo zranitelnost v oblasti bezpečnosti informací s dopadem na bezpečnost letectví
7) ***přijme vhodná opatření*** k řešení zjištění oznámených příslušným orgánem

# IS.OR.200 Systém řízení IS (ISMS)

Za účelem dosažení cílů stanovených v článku 1 organizace vytvoří, zavede a udržuje systém řízení bezpečnosti informací (ISMS), který zajistí, že organizace:

***8)*** ***zavede systém externího hlášení***, aby mohl příslušný orgán přijmout vhodná opatření;
9) dodržuje požadavky obsažené v bodě IS.I.OR.235, pokud zadává jakoukoliv část činností uvedených v bod IS.I.OR.200 jiným organizacím
***10)*** ***splňuje požadavky na zaměstnance*** stanovené v bodě IS.I.OR.240;
***11)*** ***splňuje požadavky na vedení záznamů*** stanovené v bodě IS.I.OR.245;
***12)*** ***sleduje, jak organizace plní požadavky tohoto nařízení a poskytuje zpětnou vazbu o zjištěních odpovědnému vedoucímu pracovníkovi, aby zajistil účinné provádění nápravných opatření;***
***13)*** ***chrání,*** aniž by byly dotčeny platné požadavky na hlášení incidentů**,** ***důvěrnost všech informací,*** které organizace mohla obdržet od jiných organizací, a to podle úrovně jejich citlivosti

Za účelem dosažení cílů informací
(ISMS), který zajistí, že o

***8) zavede systém exte***
9) dodržuje požadavky .I.OR.200
jiným organizacím
***10) splňuje požadavky***
***11) splňuje požadavky***
***12) sleduje, jak organiz mu***
***vedoucímu pracovn***
***13) chrání,*** aniž by byly izace mohla
obdržet od jiných or

## ORO.GEN.200 Management system

*Regulation (EU) No 965/2012*

(a) The operator shall establish, implement and maintain a management system that includes:

(1) clearly defined lines of responsibility and accountability throughout the operator, including a direct safety accountability of the accountable manager;

(2) a description of the overall philosophies and principles of the operator with regard to safety, referred to as the safety policy;

(3) the identification of aviation safety hazards entailed by the activities of the operator, their evaluation and the management of associated risks, including taking actions to mitigate the risk and verify their effectiveness;

(4) maintaining personnel trained and competent to perform their tasks;

(5) documentation of all management system key processes, including a process for making personnel aware of their responsibilities and the procedure for amending this documentation;

(6) a function to monitor compliance of the operator with the relevant requirements. Compliance monitoring shall include a feedback system of findings to the accountable manager to ensure effective implementation of corrective actions as necessary; and

(7) any additional requirements that are prescribed in the relevant Subparts of this Annex or other applicable Annexes.

(b) The management system shall correspond to the size of the operator and the nature and complexity of its activities, taking into account the hazards and associated risks inherent in these activities.

# IS.OR.205 Posouzení rizik IS

**a)** *Organizace identifikuje všechny své prvky*, které by mohly být vystaveny rizikům bezpečnosti informací. Patří sem:
1. činnosti, zařízení a zdroje organizace, jakož i služby, které organizace provozuje, poskytuje, přijímá nebo udržuje;
2. vybavení, systémy, údaje a informace, které přispívají k fungování prvků uvedených v bodě 1.

**b)** *Organizace identifikuje rozhraní*, která má s jinými organizacemi a která by mohla vést k vzájemné expozici rizikům v oblasti bezpečnosti informací

**c)** S ohledem na prvky a rozhraní uvedené v písmenech a) a b) organizace identifikuje rizika v oblasti bezpečnosti informací, která mohou mít možný dopad na bezpečnost letectví.

**d)** Organizace přezkoumá a aktualizuje posouzení rizik

# IS.OR.205 Posouzení rizik IS

Na základě Na základě novelizace Prováděcího nařízení komise EU 2015/1998 ve znění Prováděcího nařízení komise EU 2019/1583 a Prováděcího nařízení komise EU 2020/910, které posouvá platnost Prováděcího nařízení komise EU o rok, jsou od 1. 1. 2022 pro oblast kybernetické bezpečnosti vyžadovány nové povinnosti u subjektů a školitelů podílejících se na ochraně civilního letectví před protiprávními činy (dále jen „subjekty“):

**a)** *O*
1. či
2. vy

**b)** *Organizace identifikuje rozhraní,* která má s jinými organizacemi a která by mohla vést k vzájemné expozici rizikům v obl

1. Subjekty jsou povinny provést identifikaci kritických informačních a komunikačních systémů (IKS) za účelem určení, zda by narušení důvěrnosti, integrity nebo dostupnosti informací, uložených a používaných v těchto systémech, jejich funkcích a komponentech mohlo mít vliv na ochranu civilního letectví před protiprávními činy a na jeho základě stanovit rozsah zaváděných opatření v oblasti kybernetické bezpečnosti.

**c)** S
kte

**d)**

# IS.OR.205 Posouzení rizik IS

## GM3 ORO.GEN.200(a)(3) Management system

*ED Decision 2014/017/R*

**SAFETY RISK ASSESSMENT — RISK REGISTER**

The results of the assessment of the potential adverse consequences or outcome of each hazard may be recorded by the operator in a risk register, an example of which is provided below.

| Hazard | | Incident Sequence Description | Existing Controls | Outcome (Pre-Mitigation) | | | Additional Mitigation required | Outcome (Post-Mitigation) | | | Actions and Owners | Monitoring and Review Requirements |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| No. | Description | | | Severity | Likelihood | Risk | | Severity | Likelihood | Risk | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

# IS.OR.210 Řešení rizik IS

**a)** Organizace vypracuje opatření k řešení nepřijatelných rizik zjištěných v souladu s bodem IS.I.OR.205, včas je provede a kontroluje jejich trvalou účinnost. Tato opatření musí organizaci umožnit:

1)*kontrolovat okolnosti*, které přispívají ke skutečnému výskytu scénáře hrozeb;

2) *snížit důsledky* pro bezpečnost letectví spojené s naplněním scénáře hrozeb;

3) *vyhnout se rizikům*. Tato opatření nesmí přinést žádná nová možná nepřijatelná rizika pro bezpečnost letectví.

**b)** AM a ostatní dotčení pracovníci organizace musí být informováni o výsledku posouzení rizik provedeného v souladu s bodem IS.I.OR.205, o odpovídajících scénářích hrozeb a o opatřeních, která mají být provedena. Organizace rovněž informuje organizace, s nimiž má rozhraní v souladu s bodem IS.I.OR.205 písm. b), o všech rizicích sdílených mezi oběma organizacemi

# IS.OR.210 Řešení rizik IS

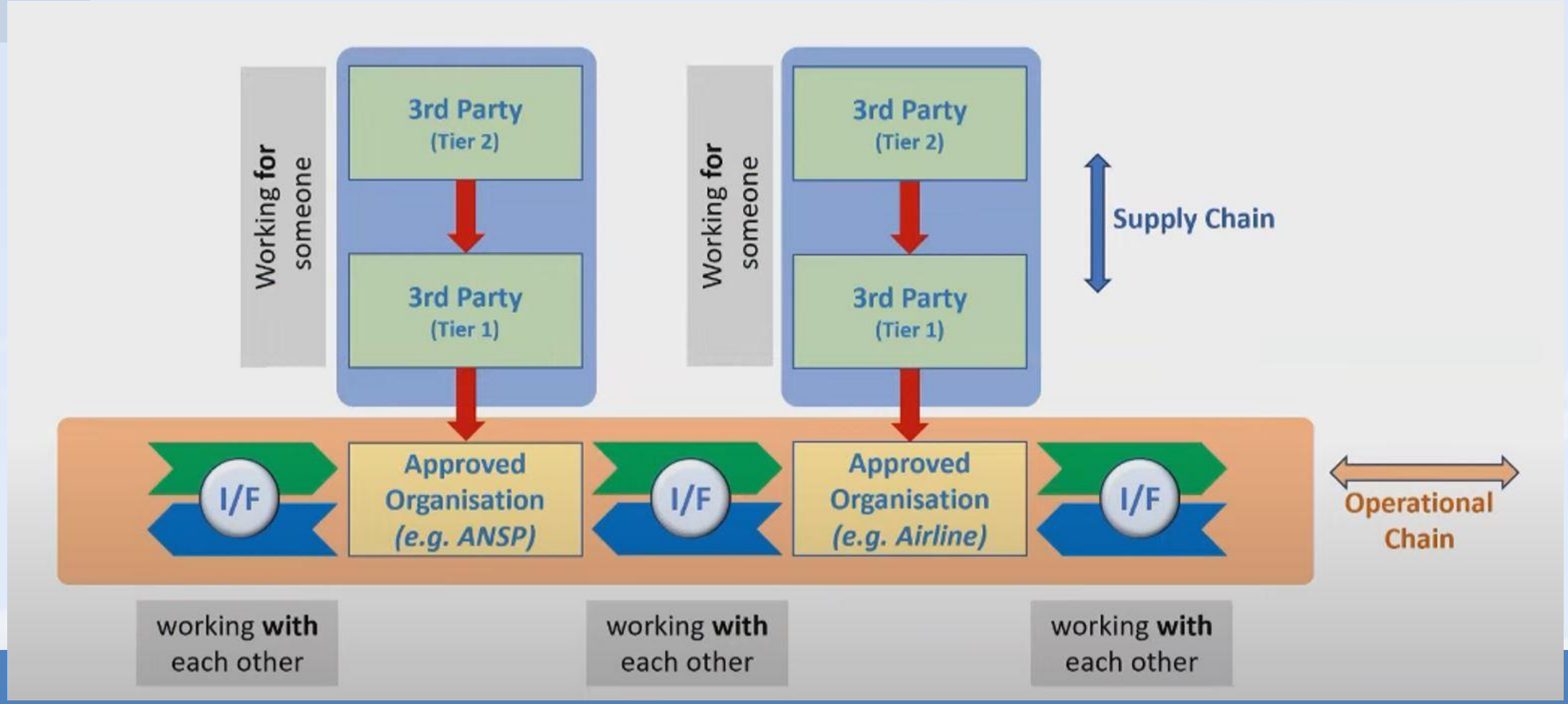
**a)** C
kon
1)
2)
3)

3. Na základě identifikace IKS je potřeba tyto systémy a informace v nich obsažené zabezpečit především proti neoprávněnému přístupu, změně a použití, zabránit narušení integrity nebo nedostupnosti, změně konfigurace IKS a zabránit neoprávněné manipulaci se systémy a jejich daty. Pro systematické nastavení zabezpečení u subjektů, které nespadají do působnosti zákona o kybernetické bezpečnosti, doporučujeme využít jako pomocný dokument „ Minimální bezpečnostní standard “, připravený Národním úřadem pro kybernetickou a informační bezpečnost (dále jen NÚKIB“). Konkrétní opatření je nutno aplikovat na základě identifikace IKS a vyhodnocení rizik.

**b)** A
bodem IS.I.OR.205, o odpovídajících scénářích hrozeb a o opatřeních, která mají být provedena. Organizace rovněž informuje
organizace, s nimiž má rozhraní v souladu s bodem IS.I.OR.205 písm. b), o všech rizicích sdílených mezi oběma organizacemi

Pro hodnocení aktiv, rizik, zranitelností a hrozeb lze využít Přílohy 1 – 3, Vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat č. 82/2018.

# PART-IS - řetězce



# IS.OR.215 Systém interního hlášení IS

*Organizace vytvoří systém interního hlášení*, který umožní shromažďování a vyhodnocování událostí v oblasti bezpečnosti informací.

*Každá smluvní organizace*, která může organizaci vystavit rizikům v oblasti bezpečnosti informací s možným dopadem na bezpečnost letectví*, je povinna této organizaci hlásit události v oblasti bezpečnosti informací.*

*Organizace spolupracuje při vyšetřování s jakoukoli jinou organizací*, která významně přispívá k bezpečnosti informací v rámci své vlastní činnosti.

*Organizace může tento systém podávání hlášení integrovat* s jinými systémy podávání hlášení, které již zavedla

# IS.OR.215 Systém interního hlášení IS

*Organizac* …nosti informací…

*Každá sm…* …n na bezpečno…

*Organizac* …cí v rámci své vlastn…

*Organizac*…

## GM1 ORO.GEN.200(a)(3) Management system

*ED Decision 2017/007/R*

**INTERNAL SAFETY REPORTING SCHEME**

(a) The overall purpose of the internal safety reporting scheme is to use reported information to improve the level of the safety performance of the operator and not to attribute blame.

(b) The objectives of the scheme are to:

(1) enable an assessment to be made of the safety implications of each relevant incident and accident, including previous similar occurrences, so that any necessary action can be initiated; and

(2) ensure that knowledge of relevant incidents and accidents is disseminated, so that other

# IS.OR.220 Incidenty IS – odhalení, reakce a zotavení

**a)** Na základě výsledku posouzení rizik provedeného podle bodu IS.I.OR.205 a výsledku ošetření rizik provedeného podle bodu IS.I.OR.210 organizace provede *opatření k odhalování incidentů a zranitelností*, které naznačují možné naplnění nepřijatelných rizik a které mohou mít možný dopad na bezpečnost letectví.

**b)** Organizace zavede *opatření, která reagují na všechny podmínky* události zjištěné v souladu s písmenem a), které se mohou rozvinout nebo se rozvinuly do incidentu v oblasti bezpečnosti informací.

**c)** Organizace zavede *opatření zaměřená na obnovu po incidentech* v oblasti bezpečnosti informací, včetně případných mimořádných opatření.

# IS.OR.220 Incidenty IS – odhalení, reakce a zotavení

**a)** Na základě výsledku posouzení rizik provedeného podle bodu IS.I.OR.205 a výsledku ošetření rizik provedeného podle bodu IS.I.OR.210 organizace provede *opatření k odhalování incidentů a zranitelností*, které naznačují možné naplnění nepřijatelných rizik a které mohou mít možný dopad na bezpečnost letectví.

**b)** ro

**c)** m

4. V bezpečnostních programech subjektů nebo v jiném relevantním dokumentu zaštiťujícím kybernetickou bezpečnost u subjektu, na který se bezpečnostní program odkazuje, se na základě posouzení rizik, která si zpracoval daný subjekt, **podrobně stanoví opatření k zajištění ochrany před kybernetickými útoky, jejich odhalování a reakce na ně.**

# IS.OR.225 Reakce na zjištění oznámená příslušným orgánem (ÚCL, NÚKIB)

a) Po obdržení oznámení o zjištěních předloženého příslušným orgánem organizace:
   1) zjistí hlavní příčinu nebo příčiny nesouladu a faktory, které k němu přispěly;
   2) vytvoří plán nápravných opatření;
   3) prokáže nápravu nesouladu ke spokojenosti příslušného orgánu

**b)** Opatření uvedená v písmenu a) se provedou ve lhůtě dohodnuté s příslušným orgánem

# IS.OR.225 Reakce na zjištění oznámená příslušným orgánem (ÚCL, NÚKIB)

## ORO.GEN.150 Findings

*Regulation (EU) No 965/2012*

After receipt of notification of findings, the operator shall:

(a) identify the root cause of the non-compliance;

(b) define a corrective action plan; and

(c) demonstrate corrective action implementation to the satisfaction of the competent authority within a period agreed with that authority as defined in ARO.GEN.350(d).

# IS.OR.230 Systém externího hlášení v oblasti IS

**a)** Organizace zavede systém podávání hlášení o bezpečnosti informací, který splňuje požadavky stanovené v nařízení (EU) č. 376/2014 a jeho aktech v přenesené pravomoci a prováděcích aktech, pokud se toto nařízení na organizaci vztahuje.

**b)** Aniž jsou dotčeny povinnosti vyplývající z nařízení (EU) č. 376/2014, organizace zajistí, aby každý incident nebo zranitelnost v oblasti bezpečnosti informací, které mohou představovat významné riziko pro bezpečnost letectví, byly oznámeny jejich příslušnému orgánu.

## ORO.GEN.160 Occurrence reporting

*Regulation (EU) 2019/1384*

(a) The operator shall report to the competent authority, and to any other organisation required to be informed by the State of the operator, any accident, serious incident and occurrence as defined in Regulation (EU) No 996/2010 of the European Parliament and of the Council[1] and Regulation (EU) No 376/2014.

(b) Without prejudice to point (a) the operator shall report to the competent authority and to the organisation responsible for the design of the aircraft any incident, malfunction, technical defect, exceeding of technical limitations or occurrence that would highlight inaccurate, incomplete or ambiguous information contained in the operational suitability data established in accordance with Regulation (EU) No 748/2012 or other irregular circumstance that has or may have endangered the safe operation of the aircraft and that has not resulted in an accident or serious incident.

(c) Without prejudice to Regulation (EU) No 996/2010 and Regulation (EU) No 376/2014, the reports referred in points (a) and (b) shall be made in a form and manner established by the competent authority and shall contain all pertinent information about the conditions known to the operator.

(d) Reports shall be made as soon as practicable, but in any case within 72 hours of the operator identifying the condition to which the report relates, unless exceptional circumstances prevent this.

(e) Where relevant, the operator shall produce a follow-up report to provide details of actions it intends to take to prevent similar occurrences in the future, as soon as these actions have been identified. This report shall be produced in a form and manner established by the competent authority.

**a)** Organizace
stanovené v r
pokud se toto

**b)** Aniž jsou d
incident nebo
riziko pro bez

# PART-IS – systém hlášení

## PART-IS
## ANNEX I
**Authority Requirements (AR)**

**IS.AR.200**
**ISMS**

**External Reporting**

Organisations subject to its oversight & information received through **IS.I.OR.230**

## PART-IS
## ANNEX II
**Organisations Requirements (OR)**

**IS.OR.215**
**Internal Reporting**

**Internal Reporting**

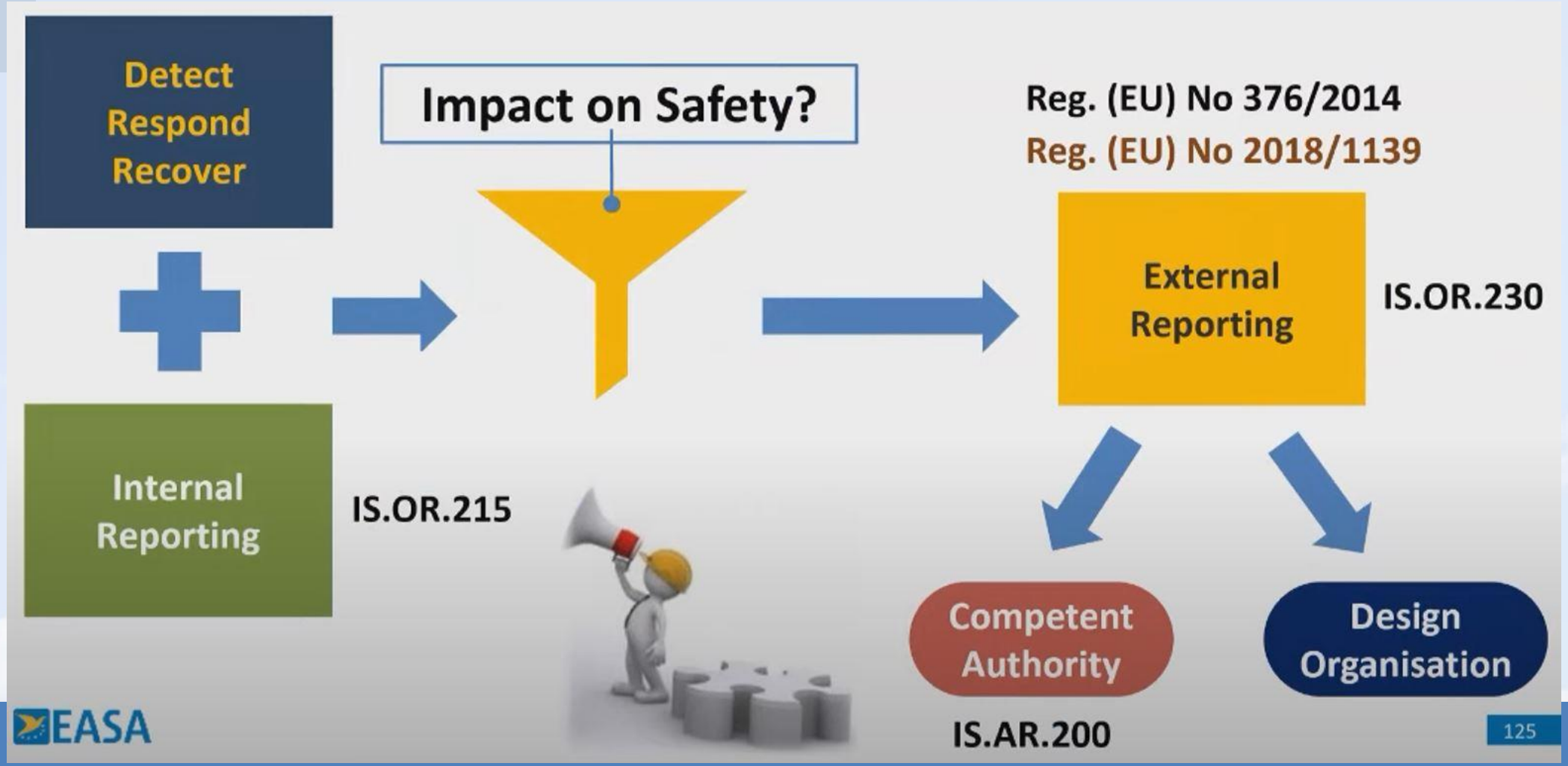
Cyber incidents & Vulnerabilities with a potential **impact on aviation safety**

**IS.OR.230**
**External Reporting**

**External Reporting**

Reg (EU) 376/2014
**Reg (EU) 2018/1139**
Report to:
- Competent Authority
- Design Approval Holder
- Design of system/ constituent
**- Not exceeding 72 h**

# PART-IS – systém hlášení



# PART-IS – systém hlášení

Detect
Respond
Recover

Impact on Safety?

Reg. (EU) No 376/2014
Reg. (EU) No 2018/1139

**RELATIONSHIP BETWEEN INTERNAL AND EXTERNAL REPORTING**

Organisations should collect and report internally incidents and vulnerabilities aiming at covering all items within the scope of this Regulation. Both internal and external reporting are necessary for a complete and effective reporting system. Internal reports should be assessed in a timely manner and where the potential impact on safety is an unsafe condition, organisations should initiate reporting of these internal reports according to IS.I.OR.230.

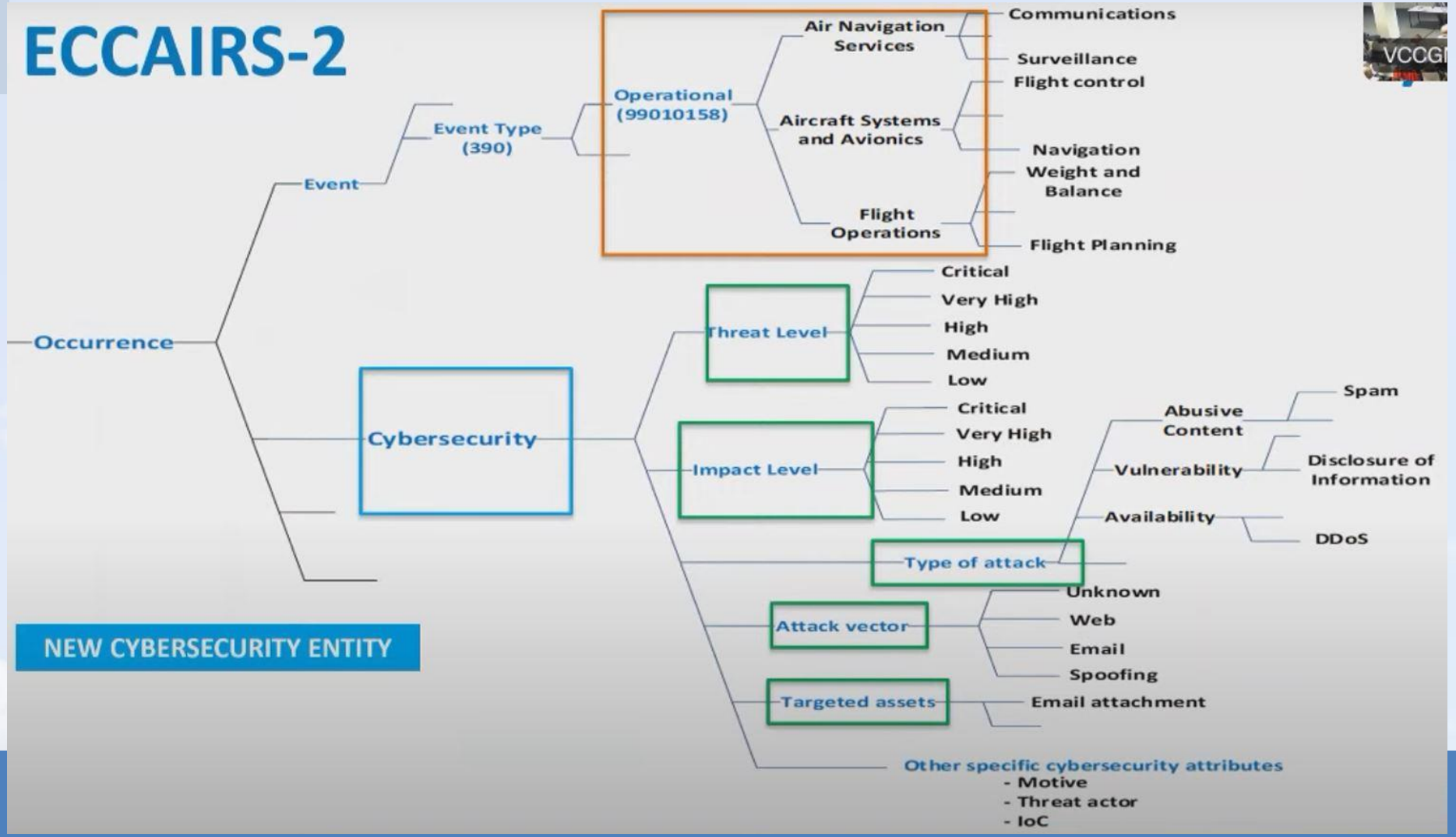
Competent Authority

Design Organisation

EASA

IS.AR.200

# Připravovaná změna ECCAIRS



# IS.OR.235 Uzavírání smluv na činnosti týkající se řízení informací

Organizace zajistí, aby při zadávání jakékoli části činností jiným organizacím byly zadané činnosti v souladu s požadavky tohoto nařízení a aby organizace provádějící zadání *pracovala pod jejím dozorem a rizika spojená se smluvními činnostmi byla náležitě řízena.*

Organizace zajistí, aby příslušný orgán mohl mít na požádání přístup do smluvní organizace, a mohl tak zjistit, zda jsou nadále plněny příslušné požadavky stanovené v tomto nařízení

# IS.OR.235 Uzavírání smluv na činnosti týkající se řízení informací

## ORO.GEN.205 Contracted activities

*Regulation (EU) 2019/1384*

(a) When contracting or purchasing any services or products as a part of its activities, the operator shall ensure all of the following:

(1) that the contracted or purchased services or products comply with the applicable requirements;

(2) that any aviation safety hazards associated with contracted or purchased services or products are considered by the operator's management system.

(b) When the certified operator or the SPO authorisation holder contracts any part of its activity to

# IS.OR.240 Požadavky na personál

**AM -**

1) zajistí, aby byly k dispozici veškeré zdroje nezbytné ke splnění požadavků tohoto nařízení;
2) zavede a podporuje politiku bezpečnosti informací
3) prokáže základní porozumění tomuto nařízení.

- jmenuje osobu nebo skupinu osob, které zajistí, aby organizace splňovala požadavky tohoto nařízení, a vymezí rozsah jejich pravomoci. Tato osoba (nebo skupina osob) je podřízena přímo odpovědnému vedoucímu a má odpovídající znalosti, kvalifikaci a zkušenosti k plnění svých povinností. V postupech je určeno, kdo zastupuje určitou osobu v případě její dlouhodobé nepřítomnosti.

- jmenuje osobu nebo skupinu osob s odpovědností za řízení funkce sledování souladu uvedené v bodě IS.I.OR.200 písm. a) bodě 12.

# IS.OR.240 Požadavky na personál

AM

- Po
info
neb

-V t
spol
rám

- Or
prac
k pl
a dů

## ORO.GEN.210 Personnel requirements

*Regulation (EU) No 965/2012*

(a) The operator shall appoint an accountable manager, who has the authority for ensuring that all activities can be financed and carried out in accordance with the applicable requirements. The accountable manager shall be responsible for establishing and maintaining an effective management system.

(b) A person or group of persons shall be nominated by the operator, with the responsibility of ensuring that the operator remains in compliance with the applicable requirements. Such person(s) shall be ultimately responsible to the accountable manager.

(c) The operator shall have sufficient qualified personnel for the planned tasks and activities to be performed in accordance with the applicable requirements.

(d) The operator shall maintain appropriate experience, qualification and training records to show compliance with point (c).

(e) The operator shall ensure that all personnel are aware of the rules and procedures relevant to the exercise of their duties.

# Možnost sloučení organizací

# IS.OR.245 Vedení záznamů

a) Organizace vede záznamy o svých činnostech v oblasti řízení bezpečnosti informací a archivuje nejméně 5 let

b) Organizace vede záznamy o kvalifikaci a zkušenostech vlastních zaměstnanců zapojených do činností řízení bezpečnosti informací (uchovává záznamy po dobu činnosti zaměstnanců a archivuje 3 roky po ukončení jejich činnosti)

c) Formát záznamů je upřesněn v postupech organizace.

d) Záznamy jsou uchovávány způsobem zajišťujícím jejich ochranu před poškozením, pozměňováním a krádeží, přičemž informace se, je-li to vyžadováno, identifikují podle svého stupně utajení. Organizace zajistí, aby záznamy byly uchovávány za použití prostředků, které zajistí integritu, pravost a oprávněný přístup.

## ORO.GEN.220 Record-keeping

*Regulation (EU) No 965/2012*

(a) The operator shall establish a system of record-keeping that allows adequate storage and reliable traceability of all activities developed, covering in particular all the elements indicated in ORO.GEN.200.

(b) The format of the records shall be specified in the operator's procedures.

(c) Records shall be stored in a manner that ensures protection from damage, alteration and theft.

## AMC1 ORO.GEN.220(b) Record-keeping

*ED Decision 2014/017/R*

**GENERAL**

(a) The record-keeping system should ensure that all records are accessible whenever needed within a reasonable time. These records should be organised in a way that ensures traceability and retrievability throughout the required retention period.

(b) Records should be kept in paper form or in electronic format or a combination of both. Records stored on microfilm or optical disc format are also acceptable. The records should remain legible throughout the required retention period. The retention period starts when the record has been created or last amended.

(c) Paper systems should use robust material which can withstand normal handling and filing. Computer systems should have at least one backup system which should be updated within 24 hours of any new entry. Computer systems should include safeguards against the ability of unauthorised personnel to alter the data.

(d) All computer hardware used to ensure data backup should be stored in a different location from that containing the working data and in an environment that ensures they remain in good condition. When hardware or software changes take place, special care should be taken that all necessary data continues to be accessible at least through the full period specified in the relevant subpart. In the absence of such indication, all records should be kept for a minimum period of 5 years.

a) Organizace v … ivuje nejméně 5 let

b) Organizace v … do činností řízení l … rchivuje 3 roky po ukonče

c) Formát zázn…

d) Záznamy jso … ňováním a krádeží, přiče… Organizace zaji… , pravost a oprávněný př…

# IS.OR.250 Příručka pro řízení IS (ISMM)

**a)** Organizace vydá příručku pro řízení bezpečnosti informací (ISMM) která obsahuje:
1) prohlášení podepsané AM, kterým se potvrzuje, že organizace bude svou činnost vždy vykonávat v souladu s touto přílohou a příručkou ISMM. Pokud AM není statutárním organizace, musí prohlášení spolupodepsat statutární zástupce;
2) funkci (funkce), jméno (jména), úkoly, odpovědnosti, povinnosti a pravomoci osoby či osob uvedených v bodě IS.I.OR.240 písm. b) a c);
3) v příslušných případech funkci, jméno, úkoly, odpovědnosti, povinnosti a pravomoc společné odpovědné osoby definované v bodě IS.I.OR.240 písm. d);
4) politiku bezpečnosti informací organizace uvedenou v bodě IS.I.OR.200 písm.a) bodě 1;
5) obecný popis počtu a kategorií pracovníků a zavedeného systému plánování dostupnosti pracovníků, jak je požadováno v bodě IS.I.OR.240;
6) funkci (funkce), jméno (jména), úkoly, odpovědnosti, povinnosti a pravomoci klíčových osob odpovědných za provádění bodu IS.I.OR.200, včetně osoby nebo osob odpovědných za funkci sledování souladu
7) organizační schéma znázorňující související odpovědnostní vztahy mezi osobami
8) popis systému interního hlášení
9) postupy upřesňující jak organizace zajišťuje soulad s Částí IS
10) podrobnosti o aktuálně schválených alternativních způsobech plnění předpisů.

# IS.OR.250 Příručka pro řízení IS (ISMM)

**a)** Organizace vydá příručku pro řízení bezpečnosti informací (ISMM) která obsahuje:

## AMC2 ORO.GEN.200(a)(5) Management system

*ED Decision 2014/017/R*

**COMPLEX OPERATORS — SAFETY MANAGEMENT MANUAL**

(a) The safety management manual (SMM) should be the key instrument for communicating the approach to safety for the whole of the operator. The SMM should document all aspects of safety management, including the safety policy, objectives, procedures and individual safety responsibilities.

(b) The contents of the safety management manual should include all of the following:

(1) scope of the safety management system;

(2) safety policy and objectives;

(3) safety accountability of the accountable manager;

(4) safety responsibilities of key safety personnel;

(5) documentation control procedures;

(6) hazard identification and risk management schemes;

# IS.OR.250 Příručka pro řízení IS (ISMM)

**b)** První vydání příručky řízení bezpečnosti informací schvaluje a kopii si ponechá ÚCL. Příručka řízení bezpečnosti informací se mění podle potřeby tak, aby byla vždy aktuálním popisem systému ISMS organizace. Kopie všech změn příručky ISMM se poskytne ÚCL.

**c)** Změny příručky ISMM se řídí postupem stanoveným organizací. Změny, které nespadají do oblasti působnosti tohoto postupu, a změny týkající se změn uvedených v bodě IS.I.OR.255 písm. b) schvaluje ÚCL.

**d)** Organizace může integrovat příručku ISMM s jinými výklady organizace nebo příručkami managementu, které má k dispozici, za předpokladu, že existuje jasný křížový odkaz, který uvádí, které části výkladu nebo příručky managementu odpovídají jednotlivým požadavkům obsaženým v příloze II, Části IS.

# IS.OR.255 Změny systému řízení IS

a) Změny systému ISMS mohou být řízeny a oznamovány ÚCL postupem, který organizace vypracuje. Tento postup schvaluje ÚCL.

b) Pokud jde o změny systému ISMS, na které se nevztahuje postup uvedený v písmenu a), musí organizace požádat o schválení vydané ÚCL a získat ho. Pokud jde o tyto změny potom platí:

1) Žádost o provedení změny musí být podána předtím, než k jakýmkoli takovým změnám dojde, aby příslušný orgán mohl určit, zda budou i nadále dodrženy požadavky tohoto nařízení a aby v případě potřeby mohl změnit osvědčení organizace a s ním spojené podmínky schválení;
2) organizace poskytne příslušnému orgánu veškeré informace, které si vyžádá k posouzení změny;
3) změna se provede až po získání formálního schválení příslušným orgánem;
4) během provádění těchto změn bude organizace svou činnost provozovat v souladu s platnými podmínkami, které jí příslušný orgán stanovil.

# IS.OR.255 Změny systému řízení IS

a) Z
Ten

b) F
org
1

2
3
4

## ORO.GEN.130 Changes related to an AOC holder

*Regulation (EU) No 379/2014*

(a) Any change affecting:

(1) the scope of the certificate or the operations specifications of an operator; or

(2) any of the elements of the operator's management system as required in ORO.GEN.200(a)(1) and (a)(2),

shall require prior approval by the competent authority.

(b) For any changes requiring prior approval in accordance with Regulation (EC) No 216/2008 and its Implementing Rules, the operator shall apply for and obtain an approval issued by the competent authority. The application shall be submitted before any such change takes place, in order to enable the competent authority to determine continued compliance with Regulation (EC) No 216/2008 and its Implementing Rules and to amend, if necessary, the operator certificate and related terms of approval attached to it.

The operator shall provide the competent authority with any relevant documentation.

# IS.OR.260 Soustavné zlepšování

a) Organizace musí pomocí vhodných ukazatelů výkonnosti hodnotit účinnost a vyspělost systému ISMS. Toto hodnocení se provádí na kalendářním základě předem stanoveném organizací nebo po incidentu v oblasti bezpečnosti informací.

**b)** Pokud jsou po posouzení provedeném podle písmene a) zjištěny nedostatky, přijme organizace nezbytná opatření ke zlepšení, aby zajistila, že systém ISMS bude i nadále splňovat platné požadavky a udrží rizika bezpečnosti informací na přijatelné úrovni. Kromě toho organizace přehodnotí ty prvky systému ISMS, které jsou přijatými opatřeními ovlivněny.

# Požadavky na úřad

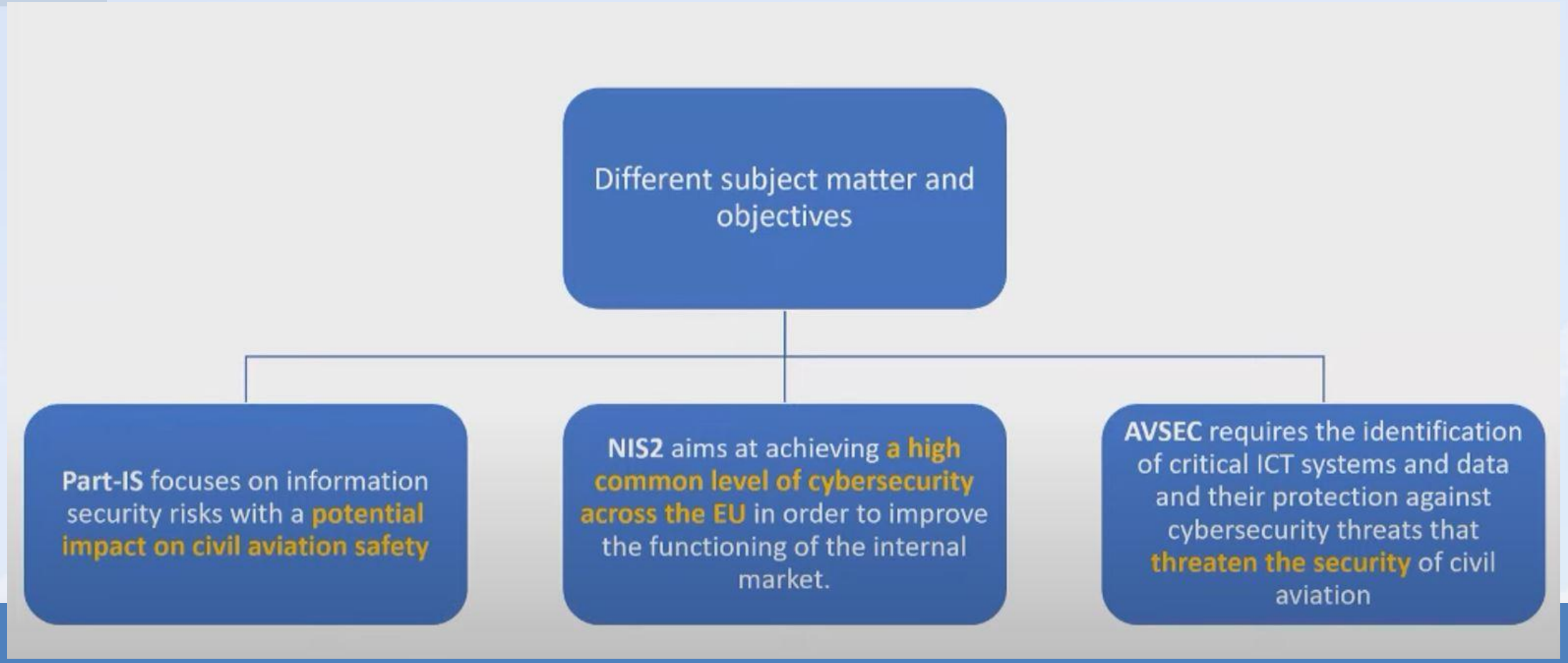
## Organisation Requirements

1. **Provisions** to establish, implement and maintain an **ISMS** as per **IS.OR requirements**.

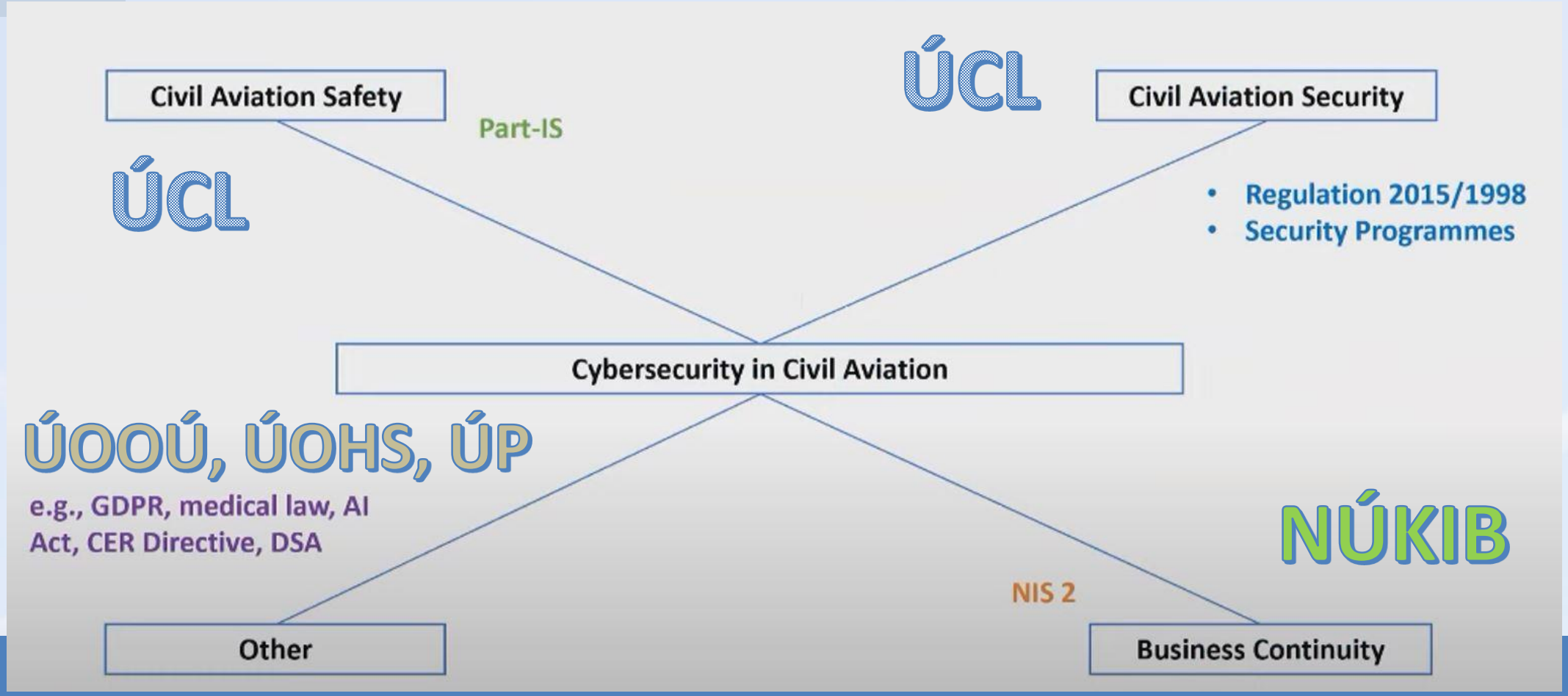
## Authority Requirements

1. **Provisions** to establish, implement and maintain an **ISMS** as per **IS.AR requirements**.
2. **Provisions** to manage and **immediately react** to information security reports received by Organisation under IS.D/I.OR.230.
3. **Provisions** to **oversee Part-IS** implementation and **derogations** granted to Organisations as well as **changes** to the ISMS during the oversight audit cycle.
4. **Possibility** to **allocate oversight tasks** to qualified entities or relevant authority responsible for information security in the Member State.

# Legislativní prostředí



# Legislativní prostředí



# Legislativní prostředí - porovnání

## Key common points and differences


| NIS 2 | Part-IS | AvSec |
|---|---|---|
| Needs to be transposed to the national law of the MS | Directly applicable to concerned organisations & authorities | Same as Part-IS |
| Size of entity is important for applicability | Size is not important – risk is | Same as Part-IS |
| Type of entity is important for applicability | Type of entity is how applicability is defined | Type of entity is how applicability is defined |
| Applicable to smaller entities under conditions* | N/A | N/A |
| Applicability defined by type of organisation (business units) | Applicability defined by approval (organisations = approval holders) | Applicability defined by type of organisation (business units) |
| Flexibility on transposition of the rule | Rule has to be applied as such | Rule has to be applied as such |
| As a Directive, requirements are of a higher level | As a Regulation, there are more granular requirements. | Requirements on cybersecurity are in general of a higher level than in Part-IS |
| ISMS is not necessary | An ISMS is needed | ISMS is not necessary |

# Legislativní prostředí - zápočty

**Reg. 2022/1645, article 4.2 & Reg. 2023/203, article 5.2**

*"Where an organisation referred to in Article 2 complies with security requirements laid down in Article 14 of Directive (EU) 2016/1148 of the European Parliament and of the Council that are equivalent to the requirements laid down in this Regulation, compliance with those security requirements shall be considered to constitute compliance with the requirements laid down in this Regulation"*

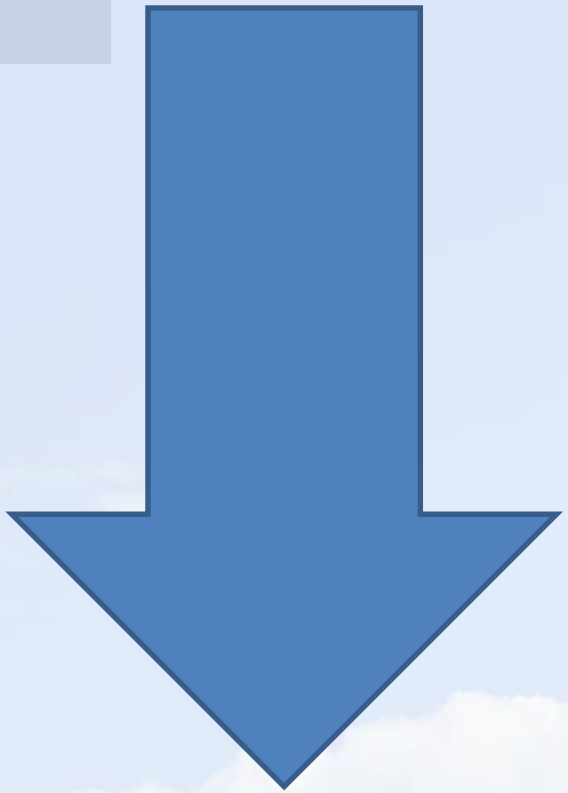
→ **NIS2: ~~A~~ credit towards everything in Part-IS**

*"Where an organisation referred to in Article 2 is an operator or an entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (EC) No 300/2008 of the European Parliament and of the Council, the cybersecurity requirements contained in point 1.7 of the Annex to Implementing Regulation (EU) 2015/1998 shall be considered to be equivalent with the requirements laid down in this Regulation, except as regards point IS.D.OR.230 of the Annex to this Regulation that shall be complied with"*

→ **AVSEC: Automatic credit towards everything in Part-IS except IS.I/D.OR.230 Information security external reporting scheme**

EASA

# Implementace



| | |
|---|---|
| Existence | Uvedeno v příručce |
| Dostatečnost | Posouzeno ÚCL |
| 22. 2. 2026 | |
| Funkčnost | Zavedeno do provozu |
| Efektivita | Dlouhodobé vyhodnocení |

# Existence

Organizace může integrovat příručku ISMM s jinými výklady organizace nebo příručkami managementu, které má k dispozici, za předpokladu, že existuje jasný křížový odkaz, který uvádí, které části výkladu nebo příručky managementu odpovídají jednotlivým požadavkům obsaženým v příloze II ‚Části IS.

# Existence

Doporučení ÚCL:

1) Do SMS manuálu doplnit křížové odkazy na příslušné kapitoly bezpečnostního programu nebo dalších manuálů;
2) Do SMS manuálu doplnit rozšíření externích hlášení o události v souvislosti s IS, které mají potenciál ohrozit letovou bezpečnost;
3) Stanovit osobu odpovědnou za IS;
4) Upravit aplikace pro systém hlášení;
5) Doplnit knihovnu rizik o rizika spojená s IS včetně vyhodnocení a zmírňujících opatření;
6) Rozšířit SPI o indikátory související s IS
7) Předložit ÚCL SMS manuál (nebo jinou příručku) formou oznámení o změně provozní příručky

# Dostatečnost

ÚCL:

1) Vyhodnotí oznámenou změnu provozní příručky a případně zašle protokol s nedostatky

2) V rámci průběžného dozoru (kontrol na základně) provede kontrolu jednotlivých bodů - může nahlédnout do bezpečnostního programu, knihovny rizik, SPI…

# Funkčnost (po 22. 2. 2026)

1) ÚCL v rámci průběžného dozoru (kontrol na základně) provede kontrolu jednotlivých bodů - může nahlédnout do bezpečnostního programu, knihovny rizik, vyhodnocení SPI, archivu interních hlášení, archivu dokumentace, zavedení zmírňujících opatření, výcviku personálu…

2) ÚCL zpracuje hlášení došlá od provozovatelů předepsaným způsobem

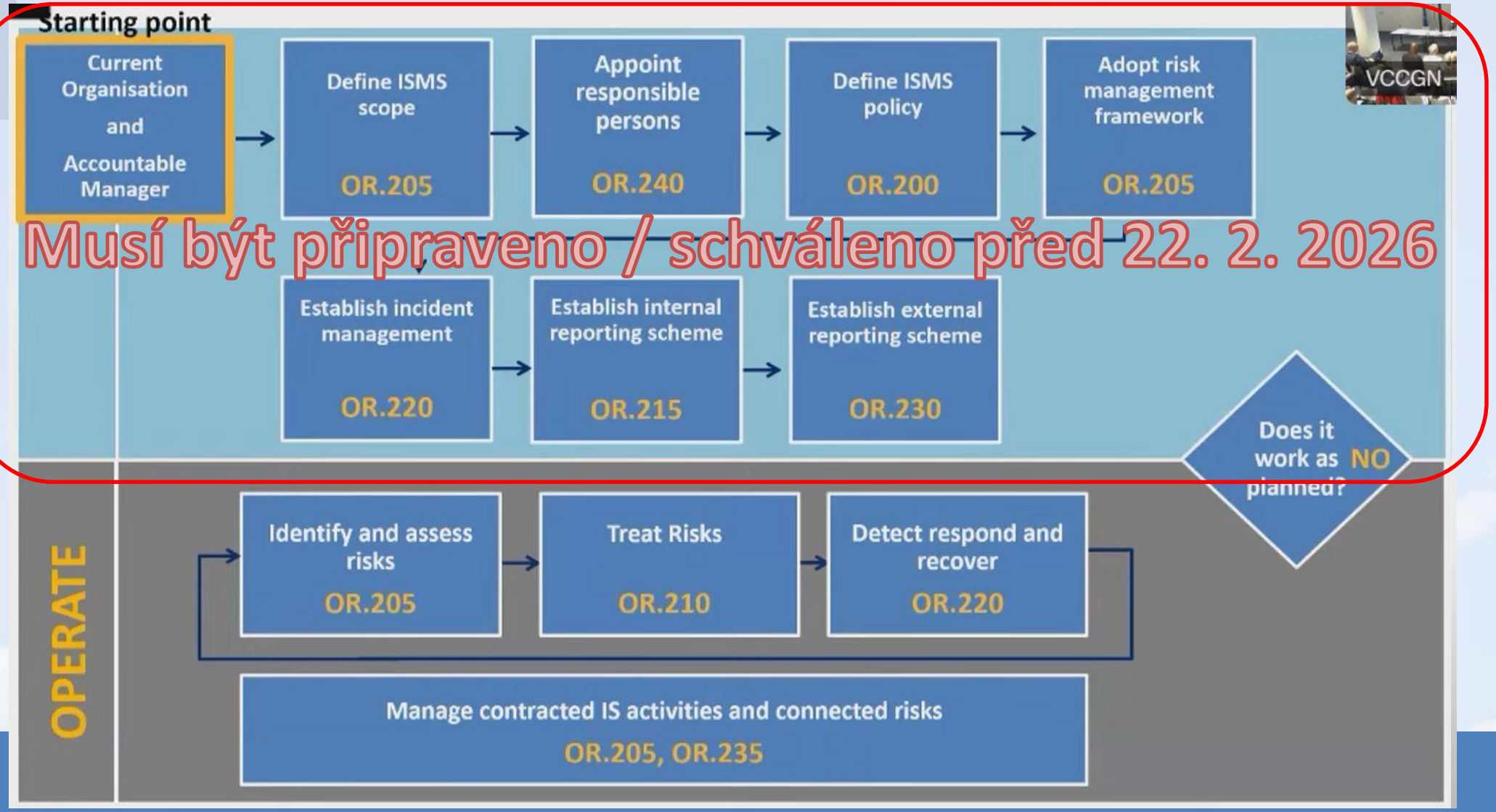
# Efektivita

Proces dlouhodobého hodnocení funkčnosti a efektivity celého systému – budoucnost.

# Věstník ÚCL

Bude vydán věstník s doporučeným postupem pro implementaci PART-IS pro provozovatele obchodní letecké dopravy.

# Kde začít?


Starting point
Current Organisation and Accountable Manager
Define ISMS scope
OR.205
Appoint responsible persons
OR.240
Define ISMS policy
OR.200
Adopt risk management framework
OR.205
Musí být připraveno / schváleno před 22. 2. 2026
Establish incident management
OR.220
Establish internal reporting scheme
OR.215
Establish external reporting scheme
OR.230
Does it work as planned?
NO
OPERATE
Identify and assess risks
OR.205
Treat Risks
OR.210
Detect respond and recover
OR.220
Manage contracted IS activities and connected risks
OR.205, OR.235
VCCGN

# Závěr

PART-IS není o IT ani o Cyber Security, ale inspektor musí být schopen hovořit s IT jejich jazykem.

# Dotazy ?

# Part-IS Implementation Workshop 2025

*Hybrid event (partially online and partially on-site)*

Description

Registration

Get notified via email alerts

Contact

**25 Jun 2025 ▸ 26 Jun 2025**

**Day 1: 25/06/2025**, 09:00 - 17:30 CET (UTC +2)

**Day 2: 26/06/2025**, 09:00 - 17:30 CET (UTC +2)

Add to Calendar

## Location

**EASA Headquarters**

Konrad- Adenauer-Ufer 3

50668 Köln

# Děkuji za pozornost

michal.paryzek@caa.gov.cz