Part IS Implementation Project :

Introduction to Information Security Management System

October 2023

APAVE / OSAC

Summary

I. EASA Regulatory context - Integration of the Part IS

II. Project Management

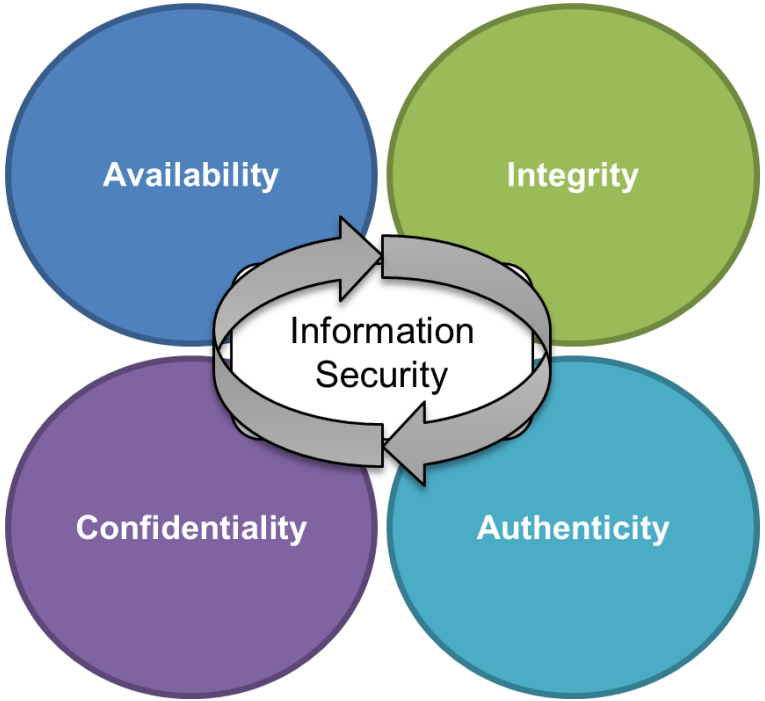
III. Deployment of oversight

IV. User support

Conclusion


PART IS:
INFORMATION SECURITY
osac

I.S. for …



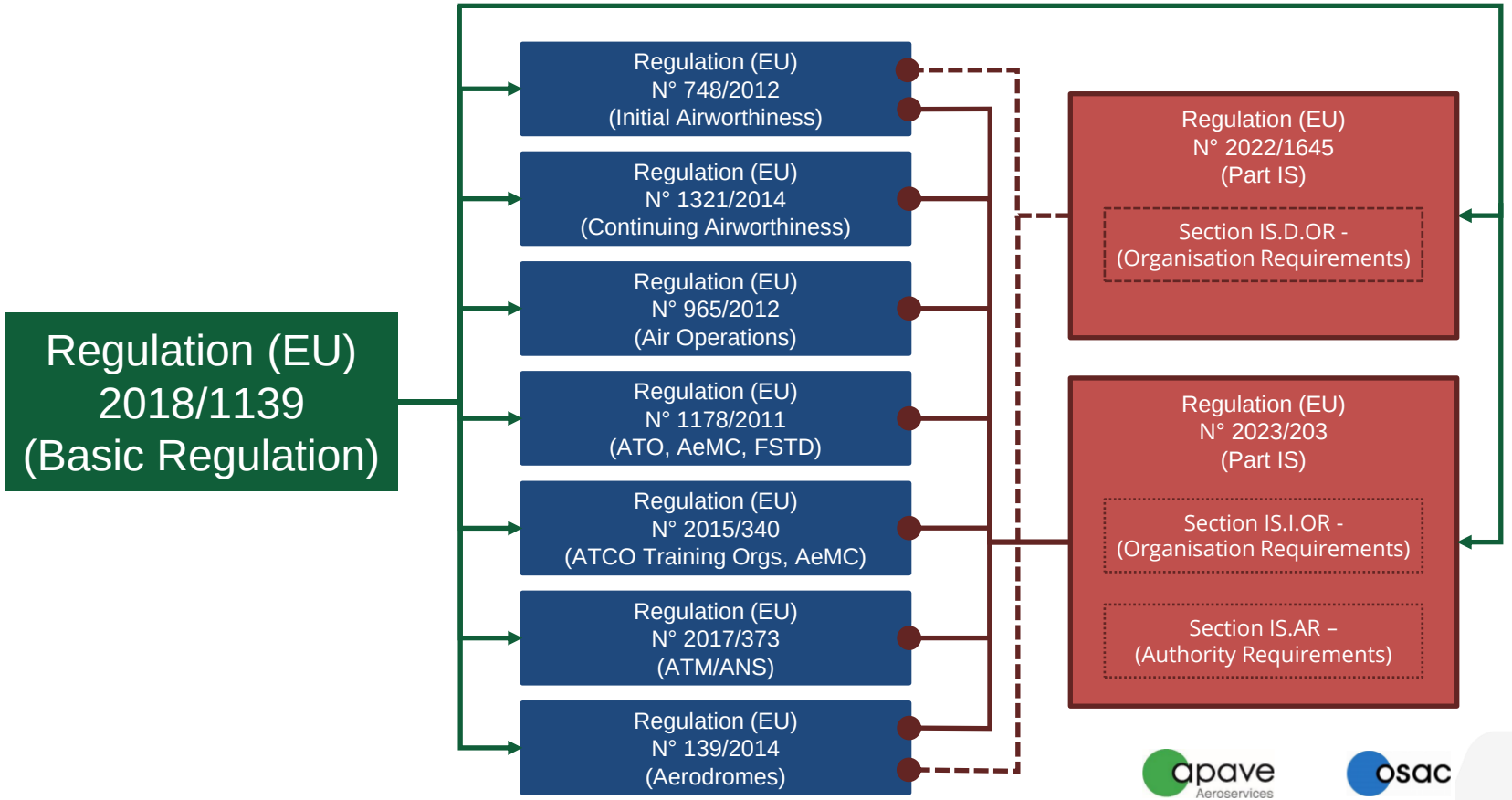
Implementing Regulation (Eu) 2023/203 - Article 3 (1):

« **Information Security** means the preservation of Confidentiality, Integrity, Authenticity and Availability of network and information systems. »

EASA Regulatory context

- **27 May:** NPA 2019-07 Publication
- **11 June**: Opinion 03/2021 Publication
- **16 October**: Delegated Regulation (EU) 2022/1645 coming into force
- **22 February** : Implementing Regulation (EU) 2023/203 coming into force
- **13 July :** Publication of the AMC and GM to support implementation of Part-IS (ED Decision 2023/008/R, ED Decision 2023/009/R and ED Decision 2023/010/R).
- **16 October:** Applicability of the Delegated Regulation (EU) 2022/1645
- **22 February** : Applicability of the Implementing Regulation (EU) 2023/203

Integration in the EASA regulation



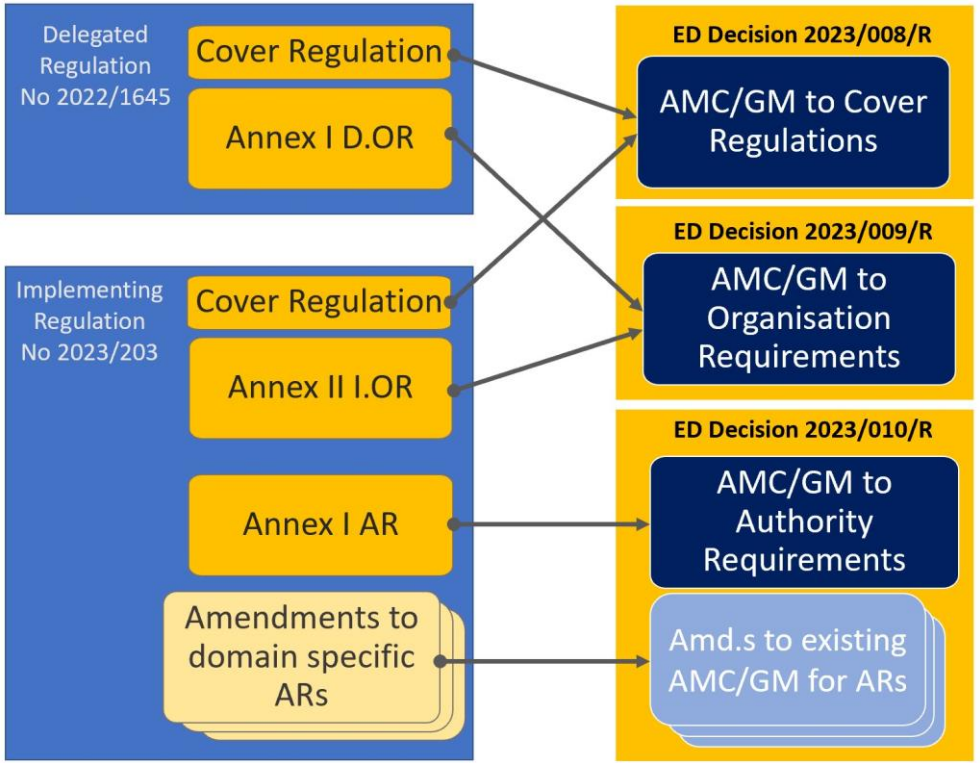


Diagram extracted from the EASA website - ED Decision 2023/010/R

ANNEX I

INFORMATION SECURITY – AUTHORITY REQUIREMENTS

[PART-IS.AR]

IS.AR.100 Scope

IS.AR.200 Information security management system (ISMS)

IS.AR.205 Information security risk assessment

IS.AR.210 Information security risk treatment

IS.AR.215 Information security incidents – detection, response, and recovery

IS.AR.220 Contracting of information security management activities

IS.AR.225 Personnel requirements

IS.AR.230 Record-keeping

IS.AR.235 Continuous improvement

Establishment, implementation and continuing improvement of an Information Security Management System (ISMS)

Risk analysis

Managing information security events

Monitoring IS suppliers

Competency management

Section OR structure

ANNEX II

INFORMATION SECURITY – ORGANISATION REQUIREMENTS

[PART-IS.I.OR]

IS.I.OR.100 Scope

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

IS.I.OR.205 Information security risk assessment

IS.I.OR.210 Information security risk treatment

IS.I.OR.215 Information security internal reporting scheme

IS.I.OR.220 Information security incidents – detection, response, and recovery

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.I.OR.240 Personnel requirements

IS.I.OR.245 Record-keeping

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

Establishment, implementation and continuing improvement of an Information Security Management System (ISMS)

Risk analysis

Managing information security events

Monitoring IS suppliers

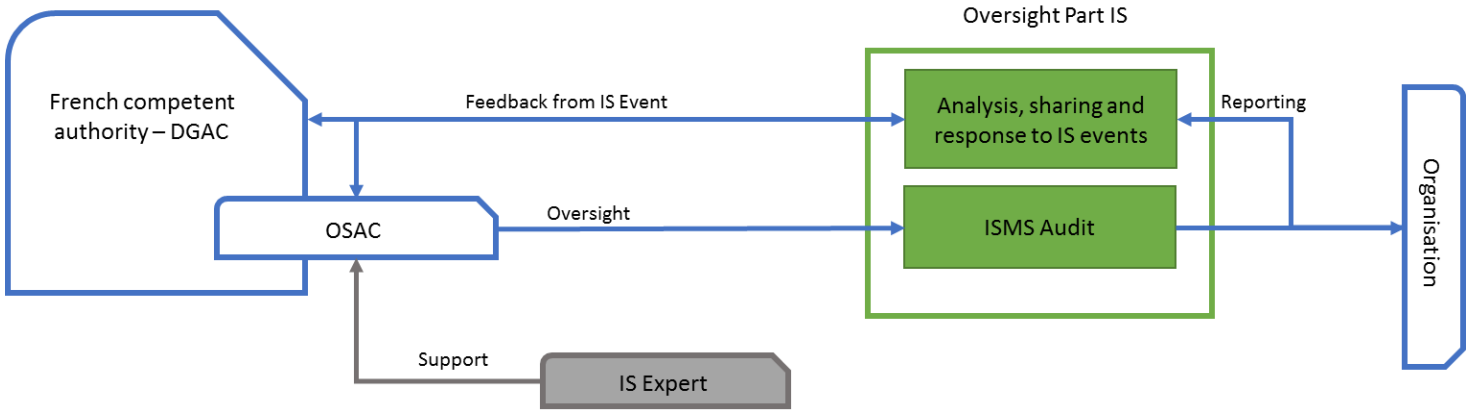
Competency management

ISMS Manuel

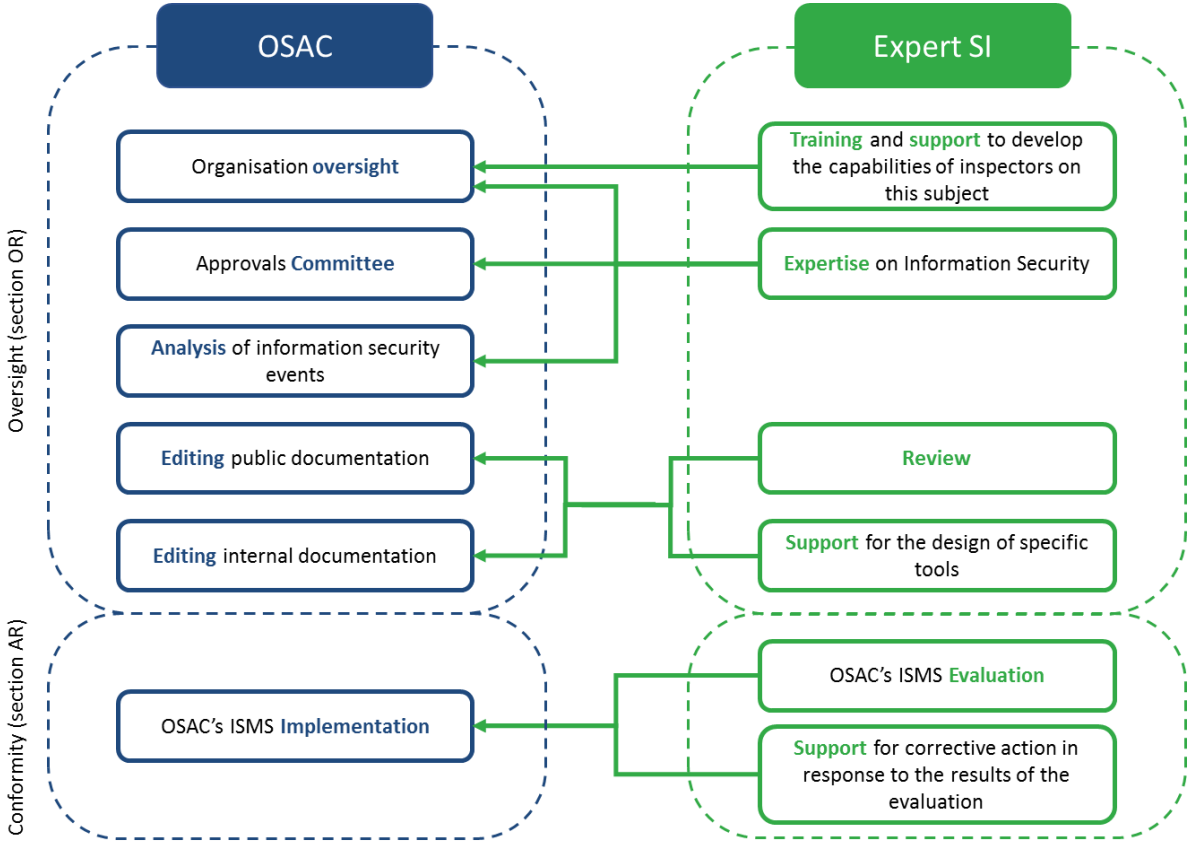
- Integration of Information Security in aviation systems
- Possibility to have one Management system including different subjects

- Some redundancy in reglementary texts
- Some lack of Harmonisation between Part 21, Part 145 or Part CAMO and the Part IS (ex: application dates and AMC/GM's definitions)

Project Management


Oversight Part IS
French competent authority – DGAC
Feedback from IS Event
Analysis, sharing and response to IS events
Reporting
Organisation
OSAC
Oversight
ISMS Audit
Support
IS Expert

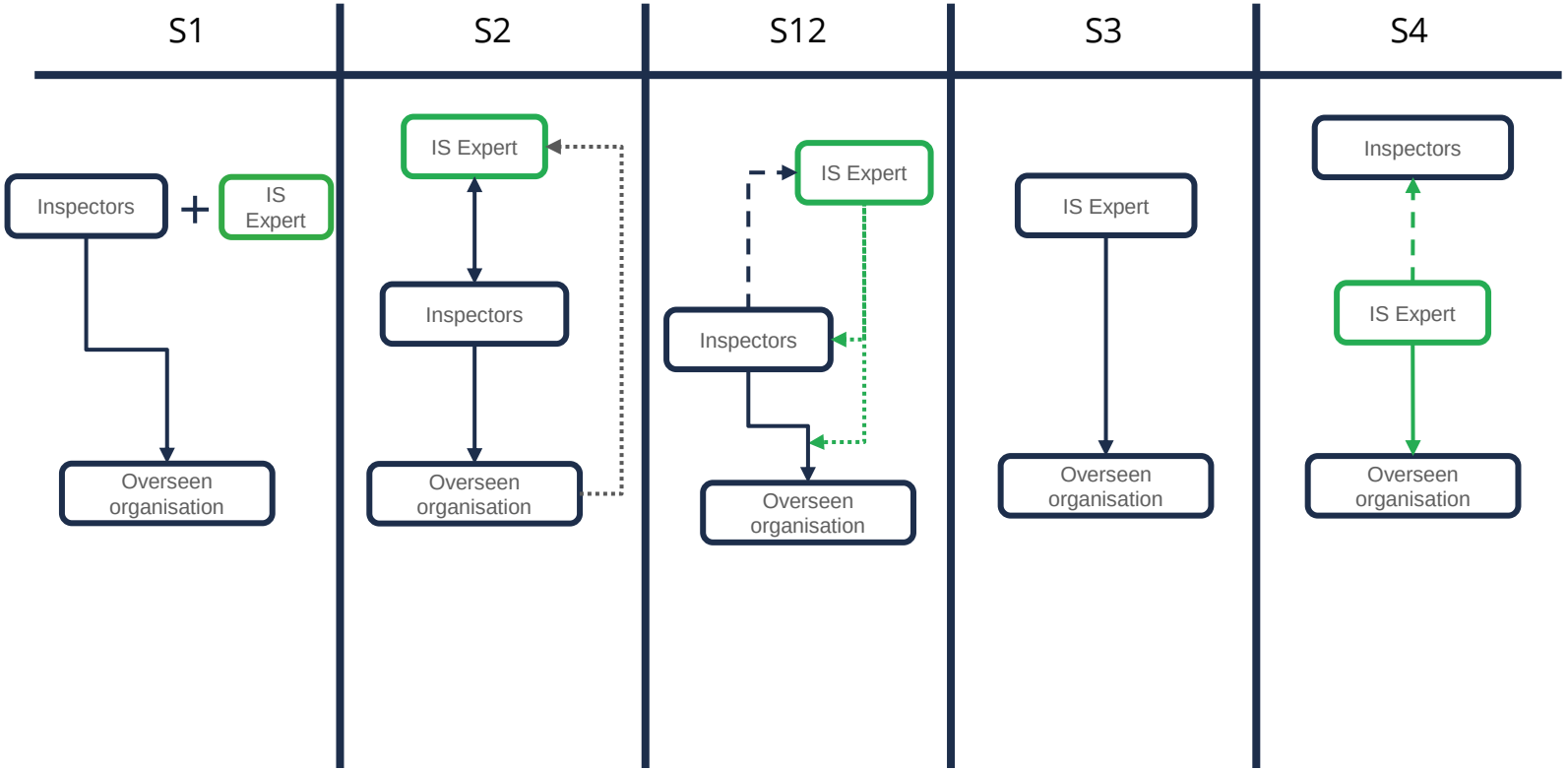
Information Security Expert support

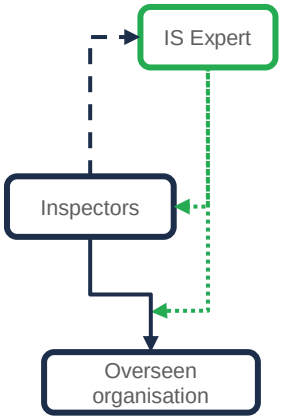


- Dual competencies
- Relevance of oversight

- Change management (new topics and new working methods)
- Bringing the two different cultures together

Deployment of oversight


S1
S2
S12
S3
S4
Inspectors
IS Expert
Overseen organisation
IS Expert
Inspectors
Overseen organisation
IS Expert
Inspectors
Overseen organisation
IS Expert
Overseen organisation
Inspectors
IS Expert
Overseen organisation



S12

Expert involvement "à la carte": involvement of the information security expert depending on the complexity of the organisations and the inspector's level of competence in the Part IS

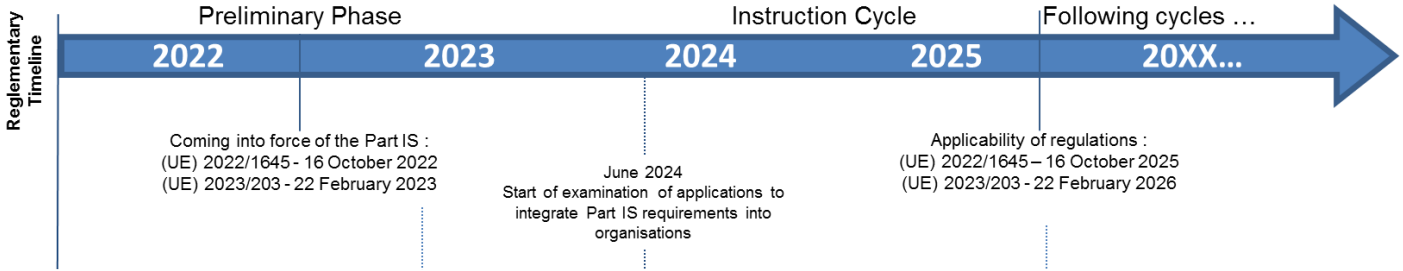
Advantages	Disadvantages

• **Gradual increase in competency on the subject**
• **Credibility on the subject**
• **Flexibility in oversight.**
  • Reliability of oversight
  • Optimisation of resources
	• **Difficulty in managing exploitation of the expert company's resources**
	• Difficulty in coordinating the two entities (planning, culture, etc.)
	• Potential reluctance to implemention of the Part IS (new skills to be acquired: resistance to change)

Impact on OSAC's system

- Part IS training for inspectors
- Part IS certification on inspector licences
- "Airworthiness regulatory training" for IS experts
- Instructions must be drawn up to standardise the level of involvement of the IS expert

Deployment of oversight



- Operational and methods departments worked together to develop this scenarios

- No transition period between the coming into force and the application of the regulations
- Integration of a completely new subject: time is needed to gather experience and knowledge

User support

- Updating the impacted public documentation
- Creation of internal tool and processes
- Creation of a FAQ tab on OSAC website

- Working groups with inspectors and organisations
- Symposiums

- Participation at aeronautic events
- Videos

Conclusion

- Information security issues are **clearly a challenge for aviation in the coming years**. They are generally well managed by large organisations, but less so by small and medium-sized organisations.

  PART-IS is an opportunity to bring small and medium-sized aeronautical organisations up to speed in terms of information security.

  But this broadens the scope of oversight for the authorities, who must take proper account of this new responsibility.

- IS is generally well managed by military entities.

  However, an IS regulation such as PART-IS could provide an opportunity for an overall review of the military aeronautics sector, in particular by ensuring that these issues are correctly addressed by the other players (subcontractors, suppliers, etc.).

Thank you for your attention

APAVE/OSAC ready to support you