

AIRBUS
GROUP

Q&A

A RIBERA

Session 7: Cyber and Supply Chain



Legal Framework

- ▶ How to understand better the cascade of legal aspects to be applied depending to the markets/countries where companies sell/buy/build goods&services?
- ▶ Depending to the countries where they are based, how to better control liability risks taken by companies through their sites/subsidiaries?
- ▶ How to ensure compliance to existing and evolving cybersecurity policies and standards (International, Regional, National) ?
 - For products and services delivered to customers
 - For data and processes exchanged with supply chain (data privacy, IP protection, etc)



Protecting ourselves and our supply chain

- ▶ What are the limits of proactive cyberdefense for private companies?
- ▶ Cybersecurity incidents sharing: How to share but protect confidentiality with our supply chain, in compliance with data privacy regulations ?
- ▶ Which cybersecurity level qualification framework usable depending to market/countries?



Answering to Cybersecurity regulation through cie policies and directives

- ▶ How to ensure we do no more no less what is legally expected (Countries dependency/ consistency)?
- ▶ Do we create market opportunities doing more?
 - eg Does French LPM compliance bring competitive advantage on external markets?



And the world is continuing to move ! Digitalisation impact

3D printing

- **CAD tools security is critical to ensure CAD model integrity from design to printer**
- ▶ How technically ensure security of 3D printing chain from CAD modelling to 3D printers?
- ▶ How to reinforce contractual obligation for CAD/CAM industry to deliver secured 3D printing chain?

BigData

- **Data Financial value is growing fast, Data analytics are demanding data like hell**
- ▶ How each supply chain actor can protect its own valuable data for its own competitive advantage when data exchanges between actors enable them to flood their own data lakes?
- ▶ How to ensure compliance with Personal Data Privacy rules?

