Global Forum
Shaping the future 2016

**DIGITALIZATION:** THE GLOBAL TRANSFORMATION

Monday 19th & Tuesday 20th
September 2016

**Evoluon Center,** Eindhoven, Netherlands


# Vendors assessments

## Cybersecurity goods & services support

Yannick FOURASTIER

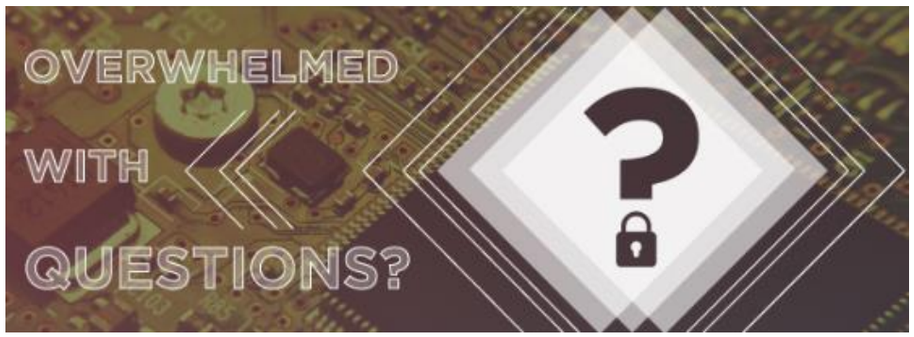
## Session 7 : Cyber and Supply chain

# Problem statement

- Liability → Cascading → Contractual chain

Requirements ⇆ Control

**A vendor as multiple customers :**




Answers quality decreases → **Risk increases**

Too many assessments kills the assessment

**Costs** → Supply chain competitiveness

# Securing the (security) assessment

- Questionnaire harmonization
  - Vertical standard, e.g. PCI (payment industry)
    - adapted to the need (within the vertical)
    - **not adapted to all the verticals**
  - Cross standard, e.g. NIST, SANS, etc.
    - **not adapted to the industrial need**
    - … but sexy approach and quite easy to implement

→ Need assessment interoperability, cross recognition

- What to assess :
  - Cybersecurity Management System (→ Vendor Security Alliance initiative)
  - Mitigation plan efficiency : security controls implementing

# Automation support for security control assessment

- Inspired from SP800-137… to early NISTIR 8011
  - Related to NIST 800-53 security controls
  - Assessing NIST 800-53 is kind a nightmare…

- What to assess : "Well implemented security controls"
  - The security controls results from services on goods (products/techno → security measures).
  - What security controls ? The ones required by the vertical standard
  - What products ? The catalogue of qualified ones (security efficiency)
  - What services ? The ones implemented / operated by qualified providers

- ☒ Job's done : tick the box !

ISCM
Information Security Continuous Monitoring

# What is at stake now ?

- Valid "ticked box" whatever Cross or Vertical :
  - "Cross" : Security controls harmonization whatever the vertical
  - "Vertical" : Vertical standards = selection of parameterized Sec.Controls
  - Qualification process of products and services : to harmonize

Harmonization
is not Uniformisation

Standardization is
**Interoperability**

Security Control implementation agility
+ cost effectiveness
+ simplified assessment

= **Trust**

# Thank you !

- Are you interested in working on :

## Security controls global definition

→ **yannick.fourastier@airbus.com**