How do airports cope with the impact of cybersecurity on aviation security

Eric Vautier (eric.vautier@adp.fr)

High Level Conference on
Cybersecurity in Civil Aviation, Krakow, Nov. 8th 2017

ICAO Risk Content Statement 2016

- Three areas of work on cyber:
  - > Aircraft and ATM interface systems
  - > “Other” aircraft systems
  - > Airport systems

- Airports systems: two broad categories:
  - > a potential facilitation activity e.g. by degrading IT-based aviation security measures such as access control and screening

  - > disruption of operations (departure control, baggage handling etc) – part of operational resilience and business continuity rather than conventional aviation security

Airport & aircraft safety

- ATC :
  - > Control tower
  - > Communications
  - > Radio navigation equipment
  - > Runway (lighting, RWSL)
  - > Surface Movement Guidance and Control System
- Flight handling
  - > Baggage, pax and freight screening
  - > Weight & balance
- Aircraft handling
  - > Gatelink
- Physical security
  - > Access control
  - > Border control

Cybersecurity & aircraft safety

- [Removed : screendumps on loss of integrity]

Cybersecurity & airport operations

- Airport Information System (AODB) :
  - > Flight schedules
  - > Resources allocation
  - > Flight Information Display System
- Airport optimization
  - > Collaborative Decision Making
  - > Runway capacity optimization
- Flight operations
  - > Check-in and boarding
  - > Baggage handling system
  - > Baggage reconciliation system
- Facility management
  - > Building management system
  - > Asset management

Cybersecurity & corporate operations

- Finance
  - > ERP
  - > CEO fraud
  - > Loyalty programs fraud
  - > Car parks
- Reputation
  - > Corporate Web Sites
- Legal
  - > GDPR
- Cyberthreats
  - > DDOS
  - > Spam/Phishing
  - > Malware

Cybersecurity and commodities

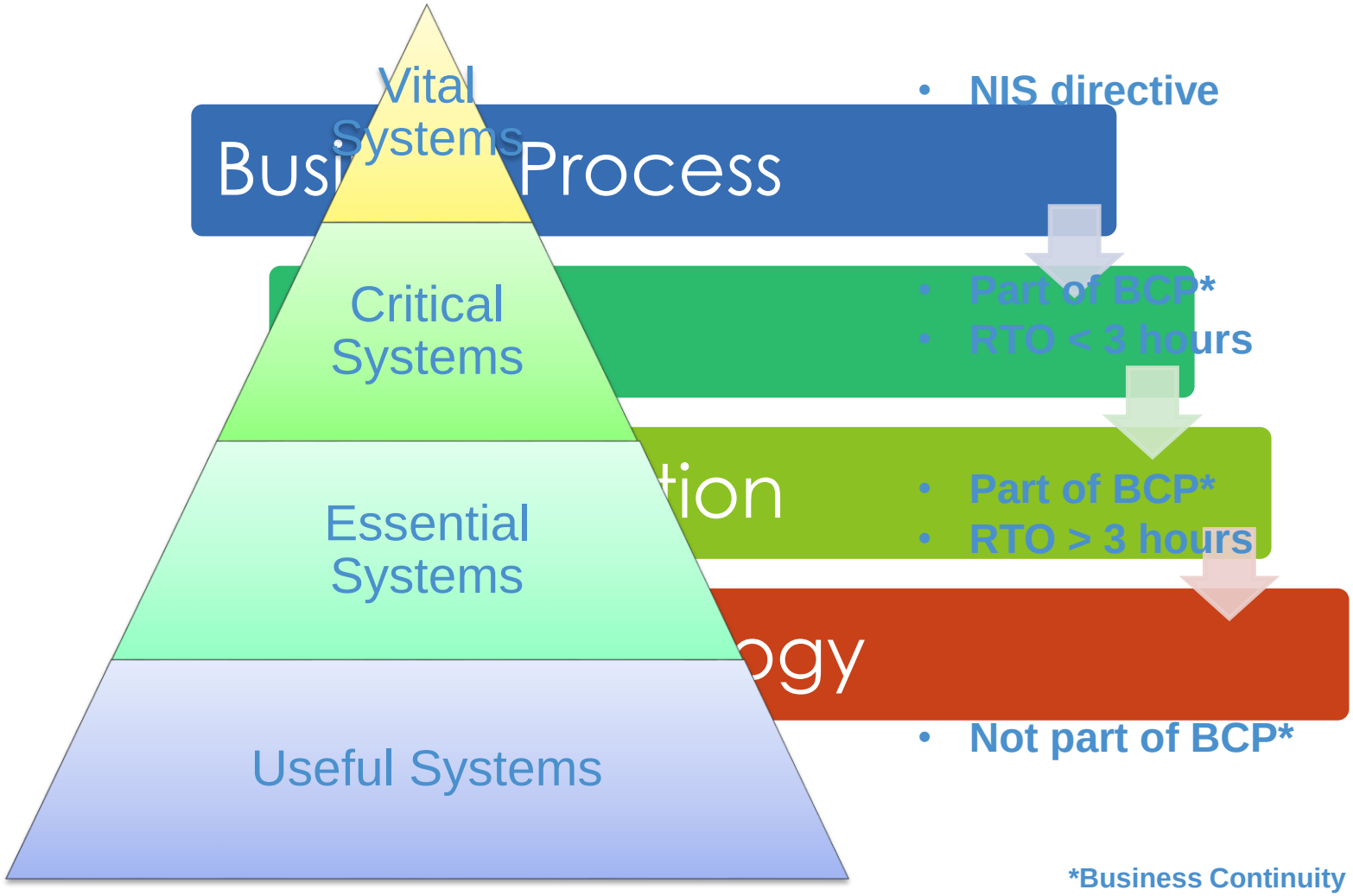
- Power supply
- Telecommunications (GSM)
- Internet access

NIS Directive

- Transposition into national legislation by May, 9th 2018

- "Already started" in Germany and France
  - > Changes in mindset of OES
    - Governance
    - Organisation
    - Operational teams
    - Cybersecurity teams
  - > Huge workload for operational teams
    - Inventory of vital systems
  - > Huge workload (to come) operational teams and IT teams
    - Risk assessments on vital systems
  - > Challenges for resources
    - Cybersecurity skills and experts
    - Expert costs
    - Remediation costs

NIS directive : where to start ?

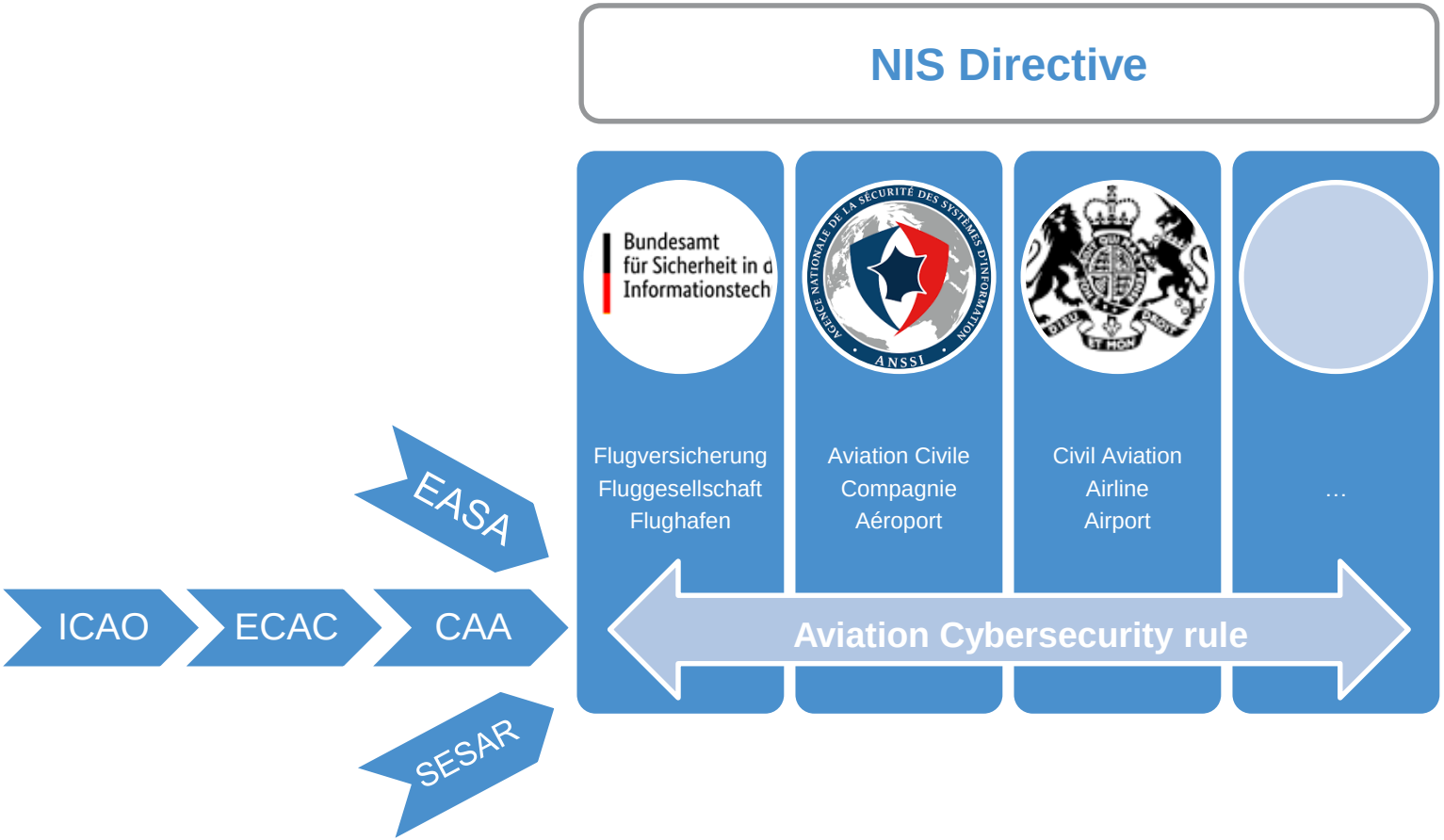


*Business Continuity Plan

NIS directive in aviation

- Pros :
  - > Operators are now accountable for cybersecurity, not only CISOs
  - > OES can work together
    - French airports
    - ACI Europe
    - Trusted partnerships
- Cons :
  - > Definition of « OES Airport » may vary
  - > OES will work (first ?) in silos
    - Little cooperation with non-OES airports
    - Little cooperation with airlines (OES/non OES), CAAs, aircraft manufacturers

NIS Directive & aviation regulations



NIS Directive & aviation regulations

- Consistency with NIS directive is essential:
  - > No duplication of efforts to implement cybersecurity
  - > No “interference” with the NIS Directive agenda
- Diversity should be allowed
  - > Civil aviations, airlines, airports
  - > Standardized approach per domain
- Cooperation is key
  - > Cooperation between EU NIS Directive group and EASA, ECAC, etc.
  - > Cooperation between EASA, IATA, CANSO, ACI Europe, etc.

THANK YOU

www.aci-europe.org

www.airportcarbonaccreditation.org

ACI EUROPE
AIRPORT GROUPING