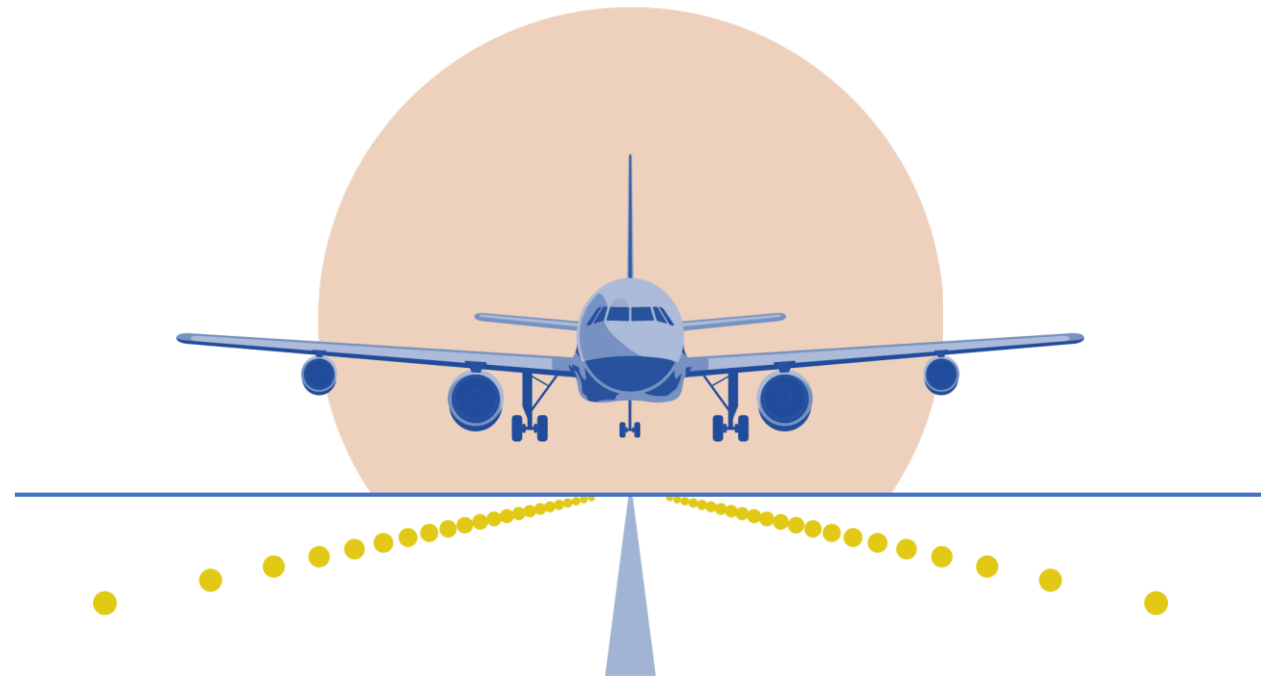




## E-ENABLING

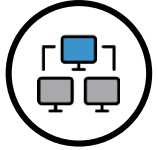
Air Operator Example  
Risk Assessment Process



**AIR OPERATOR EXAMPLE**

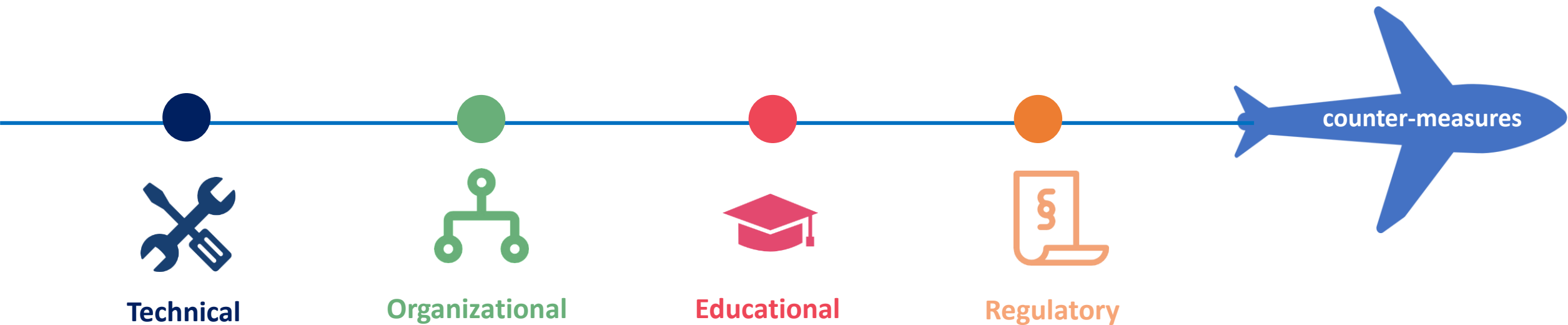


Most passengers, airlines, and the aircraft industry in general are used to very high safety standards and precautions surrounding aircraft systems.



As the computerization of aircraft steadily progresses, the question of security, i.e. the protection against intentional manipulations, becomes increasingly relevant.

**Increasing digitalization, connectivity and similar developments of modern „e-enabled“ aircraft are shown to cause an ever larger attack area.** This results in challenges to the aircraft industry and lead to a requirement for additional:



There is one operator having „e-enabled” aircraft in Poland: **LOT Polish Airlines (AOC holder, national air carrier)**

### E-enabling is implemented on:



**Boeing 737-8 MAX**  
(process of implementation the aircraft  
into the fleet - in progress)



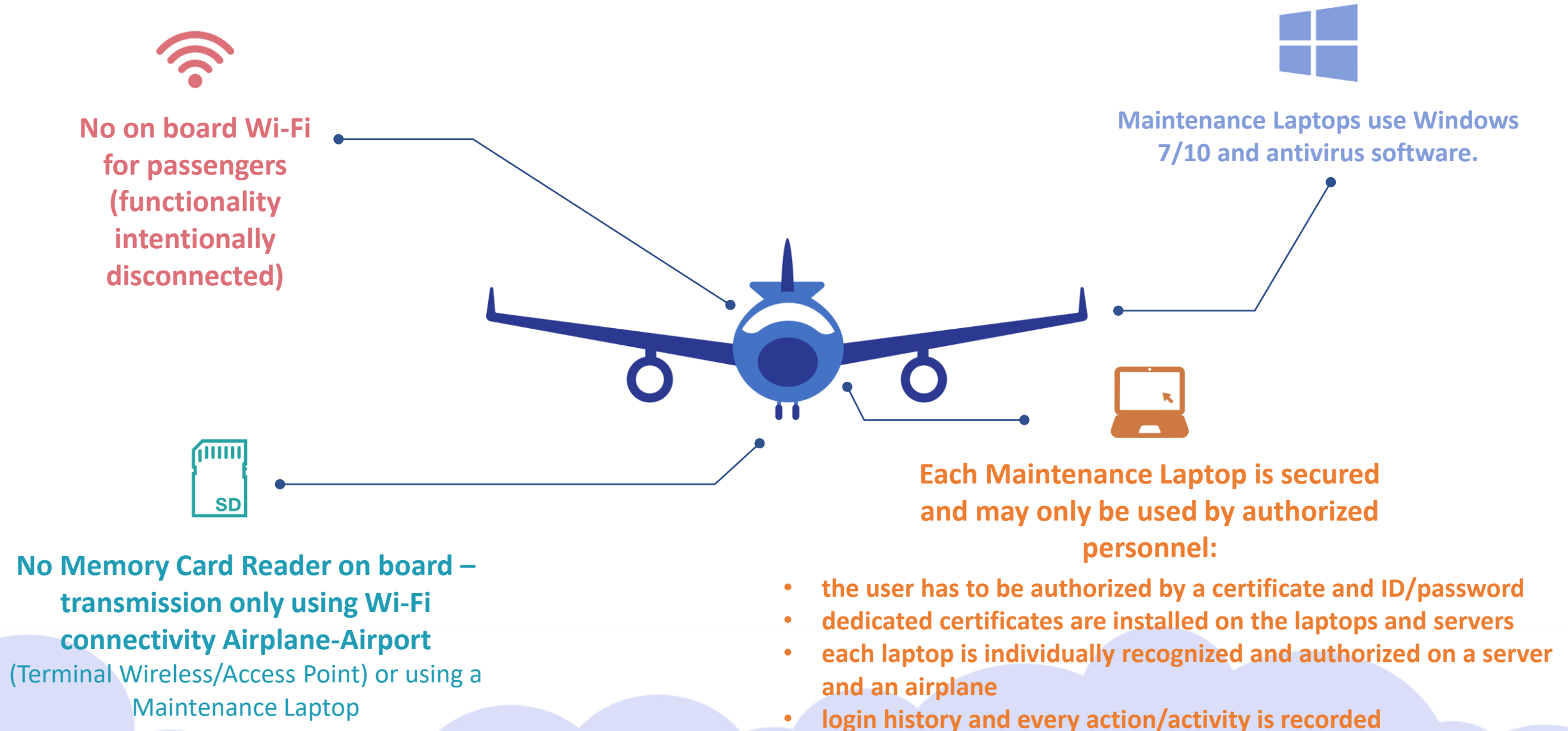
IT Administrators and  
Maintenance specialists  
at LOT Polish Airlines are  
responsible for  
E-enabling system  
efficiency and  
infrastructure security.



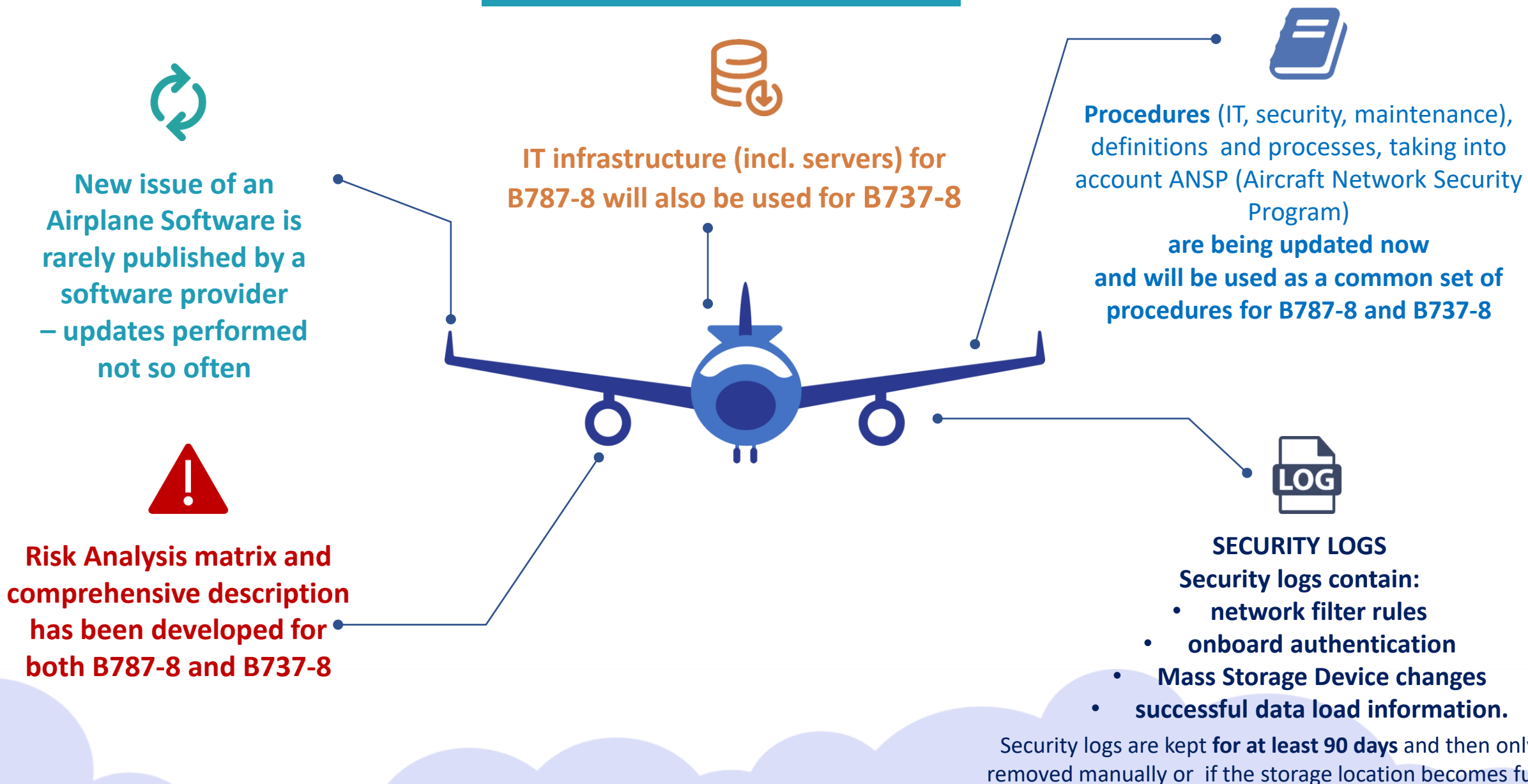
**Boeing B787-8 DREAMLINER**  
(8 a/c in the fleet)



## Essential data (part 1):



## Essential data (part 2):





**RISK ASSESMENT PROCESS**

## RISK ASSESMENT PROCESS

The purpose of the Risk Assessment Process is to identify any events that could pose a threat to a continuous operation.

Specific threats are constantly growing and adapting.

It is only when a given threat is paired with a specific vulnerability that security controls become effective at mitigating a particular risk.

Vulnerabilities are not just software bugs or unexpected behaviors in systems.

**Every system has vulnerabilities !**



## POTENTIAL HAZARDS



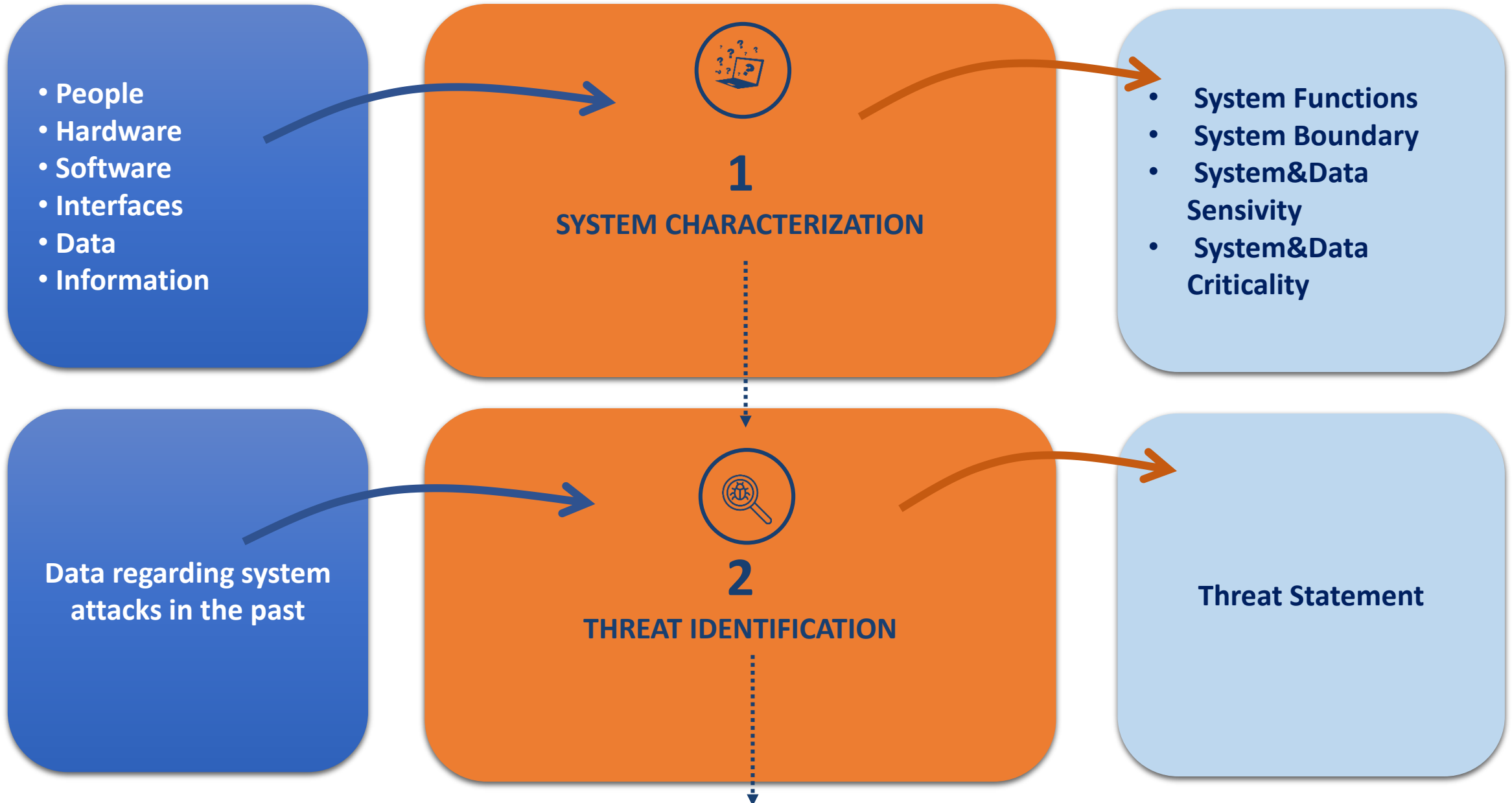
As with other advanced connectivity, a real threat exists, that may be intentional or unintentional, with a detrimental effect on system performance.



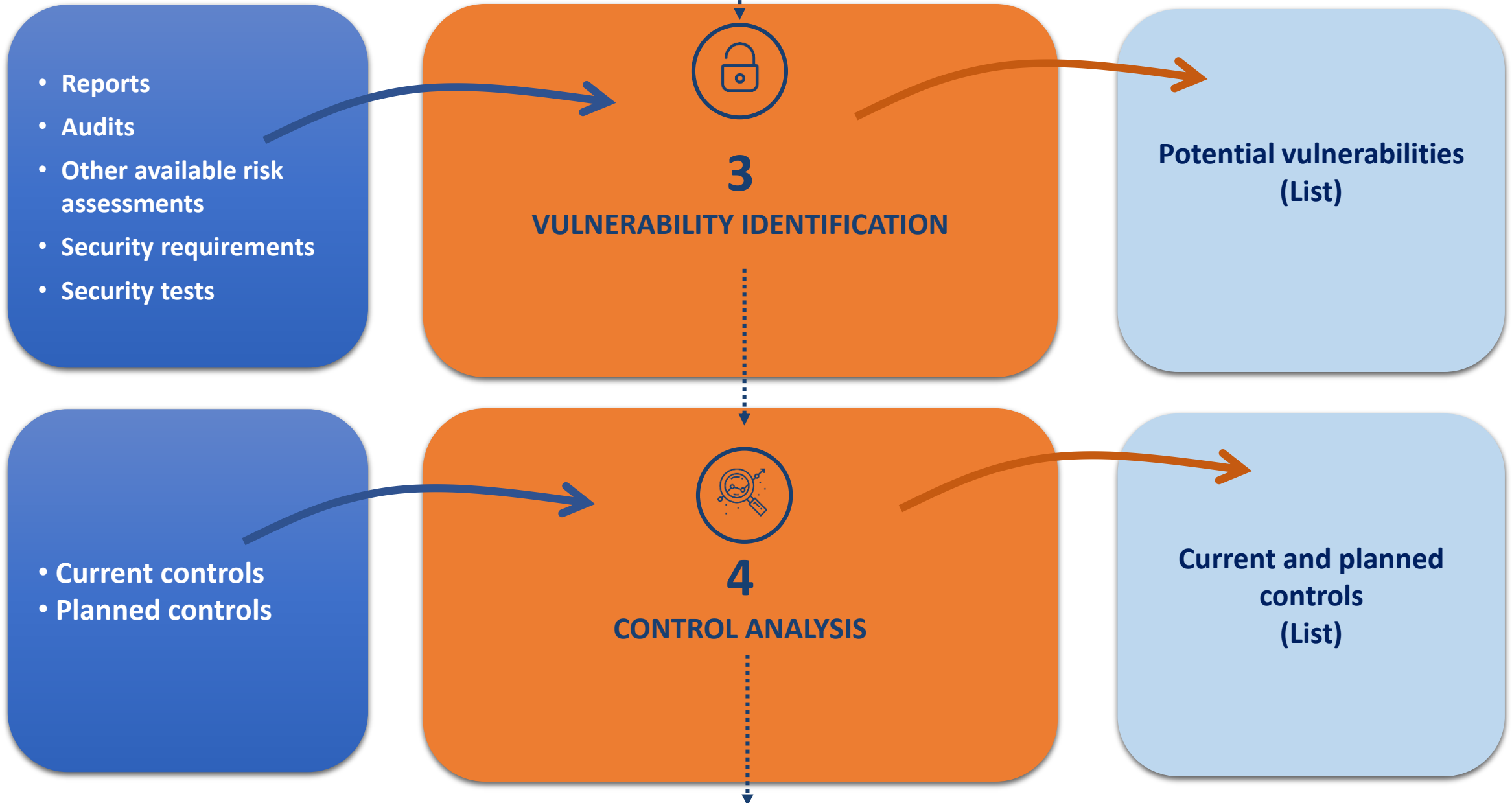
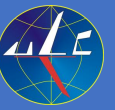
These effects may range from reduced performance, denial of service, or criminal activity.

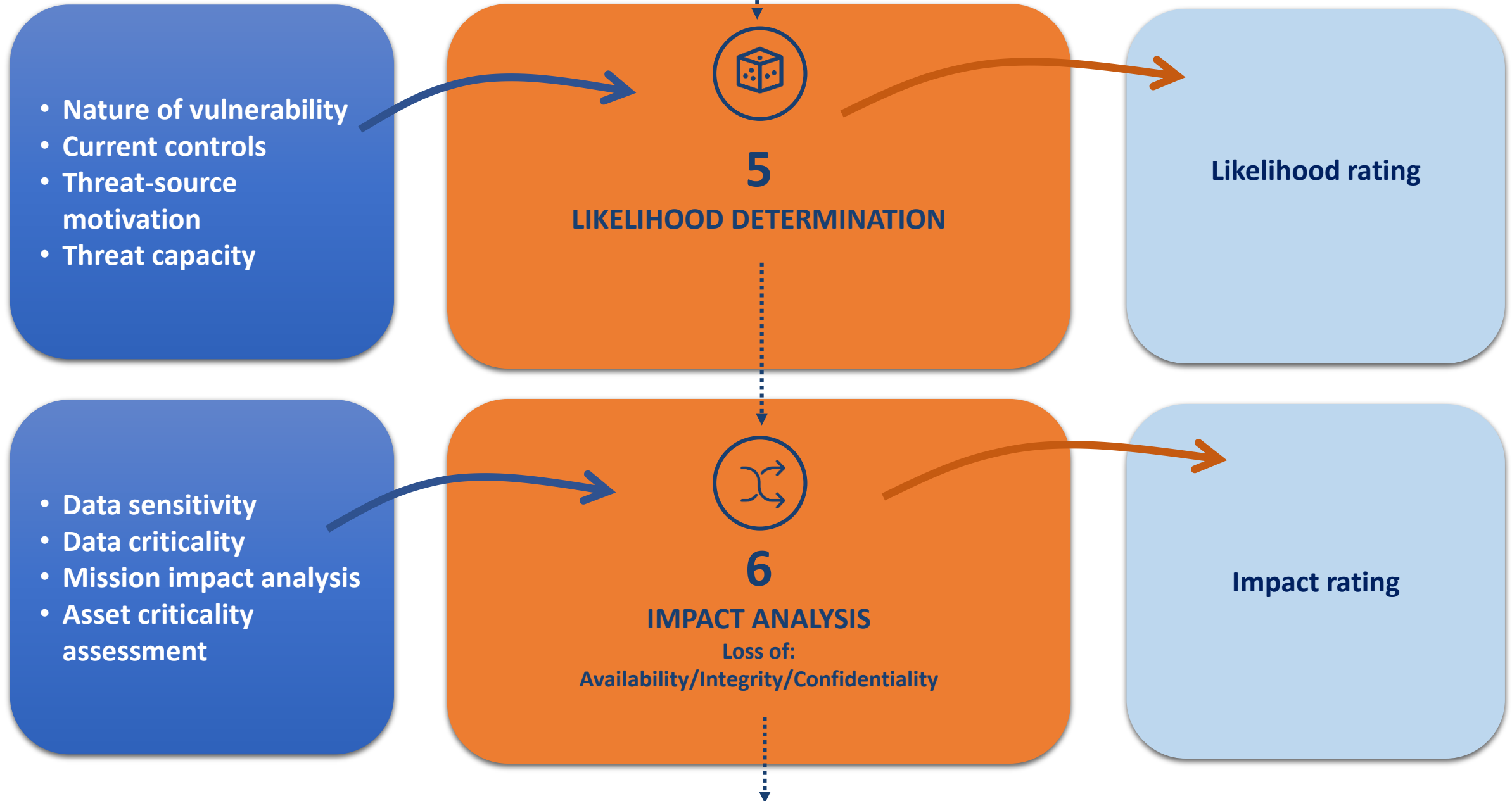


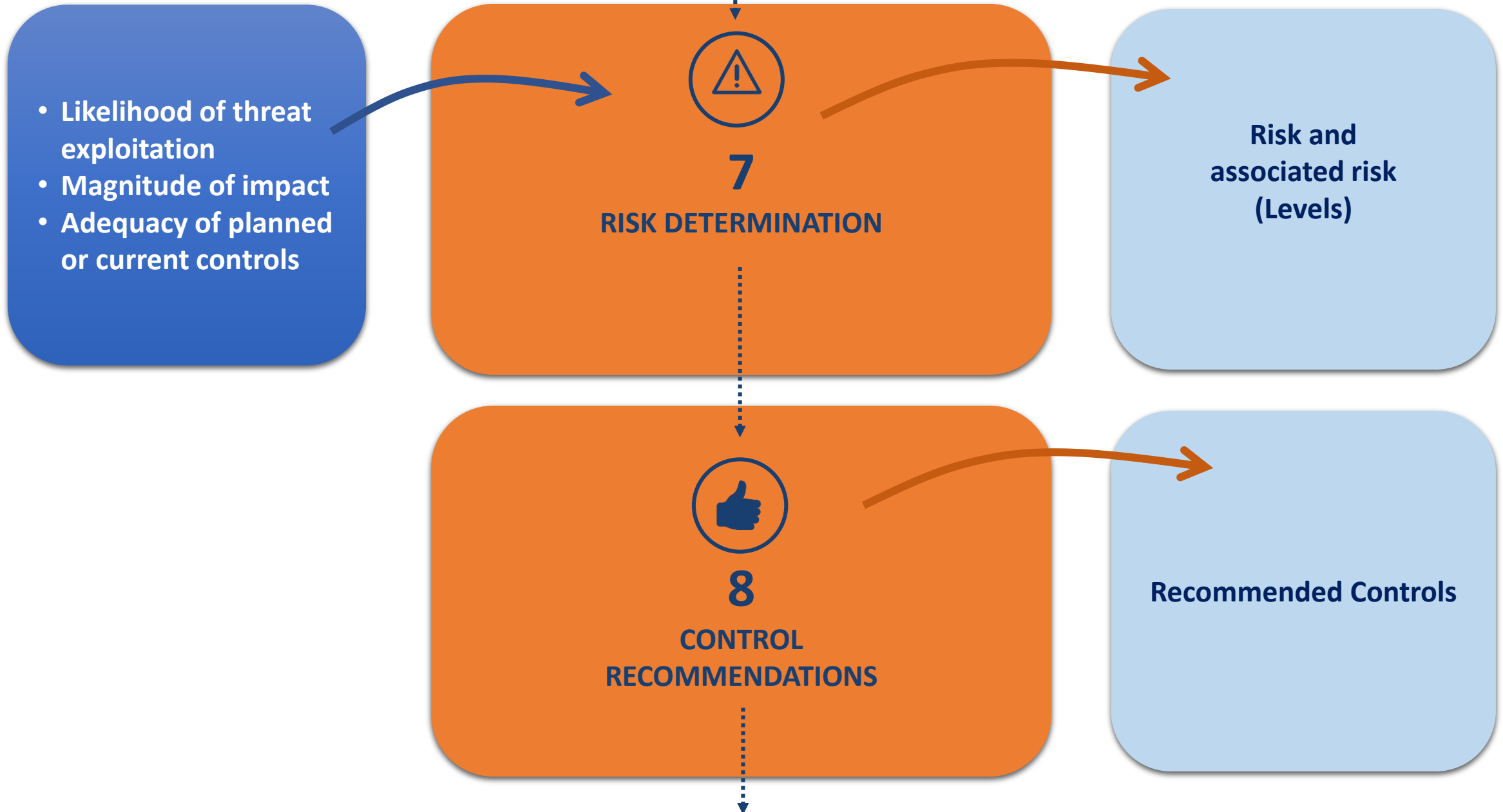
The operator shall develop an evaluation sheet and assess the risk for the implementation and use of the e-enabling system.



## RISK ASSESSMENT PROCESS (2)









LOT Polish Airlines has prepared a **threat list and conducted a risk assessment on the implementation of e-enabling solutions** in the implementation of new aircraft.



LOT Polish Airlines has developed **processes and procedures regarding e-enabling**, including security procedures.



The above information is **confidential** and available for authorized persons only.

Eliminates time-consuming and awkward physical software data loading via wireless data distribution and medialess software loading

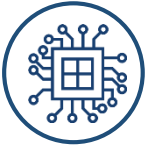
Enables near real-time data transactions both on- and off-board the airplane and provides the ability to access much of this data during flight to enable airlines to make timelier, informed maintenance and other operational decisions

Provides flight operations and maintenance personnel with data in digital formats to streamline the updating process, reduce errors, and eliminate the costs associated with shipping, handling, revising, and maintaining paper documents

Allows airlines to easily customize many aspects of their airplanes to fit their specific operations, eg. Aircraft selectable options or Aircraft modifiable interface setting files may be customized by an airline



## Summary:



**Modern aircraft become increasingly computerized**, standardized, and will continuously expand their digital on-board and off-board communications.



The move toward **e-enabled aircraft is inevitable**, and will **provide many benefits** for operators, manufacturers, and passengers.



These benefits will only be realized if the **additional services can be made secure**, without compromising the industry's impressive safety record.

**Systematic security engineering**

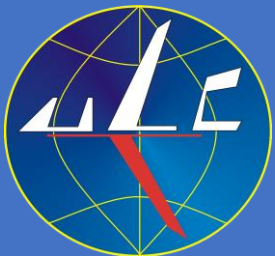
Mandatory inter-operable security standards and regulations

**Comprehensive security evaluations**

**Certifications for all aircraft IT systems involved**

are essential IT safety measures  
which shall be considered and  
implemented by civil aviation  
authorities.

# Thank You !



**Civil Aviation Authority of the Republic of Poland**

© 2017 Urząd Lotnictwa Cywilnego | ul. M. Flisa 2, 02-247 Warszawa,  
tel.: +48 22 520 72 00, fax.: +48 22 520 73 00  
email: [kancelaria@ulc.gov.pl](mailto:kancelaria@ulc.gov.pl)