

ICAO Trust Framework Activities



Challenges

Digital Aviation Ecosystem

- Digital transformation impacts all stakeholders in the aviation ecosystem
- Both systems and people are fundamentally affected
- Transformation in one area will be felt by everyone, intentionally or not



New Entrants, Diverse Needs, Global Challenges



Diverging Efforts

- Digital transformation is already happening
- Many taking action to secure their own part of the system
- Stakeholders recognize need for securing their information exchange





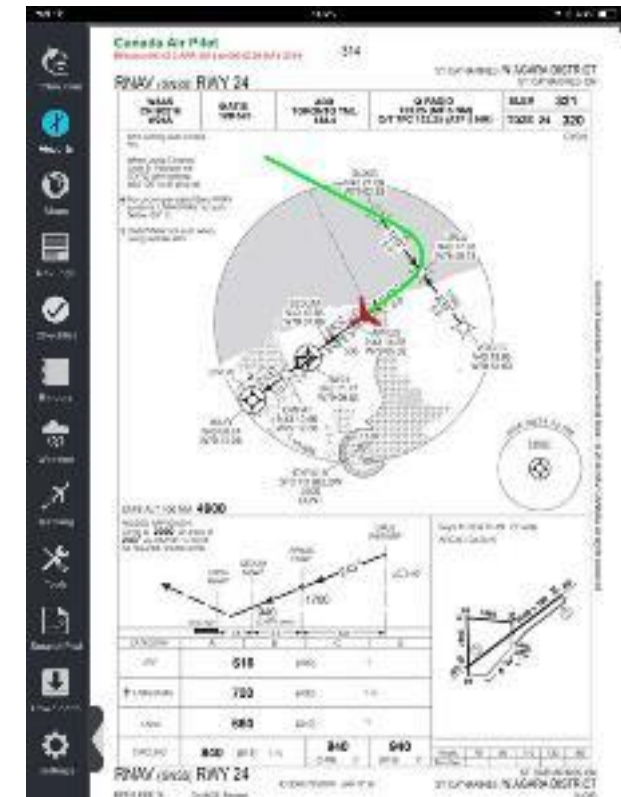
Converging Strategy

- Interoperability requires global coordination and cooperation
- Identify common needs that can unite all aviation ecosystem stakeholders
- Develop common solutions that build on existing foundations
- Agree on a common destination – where there is still one interoperable sky

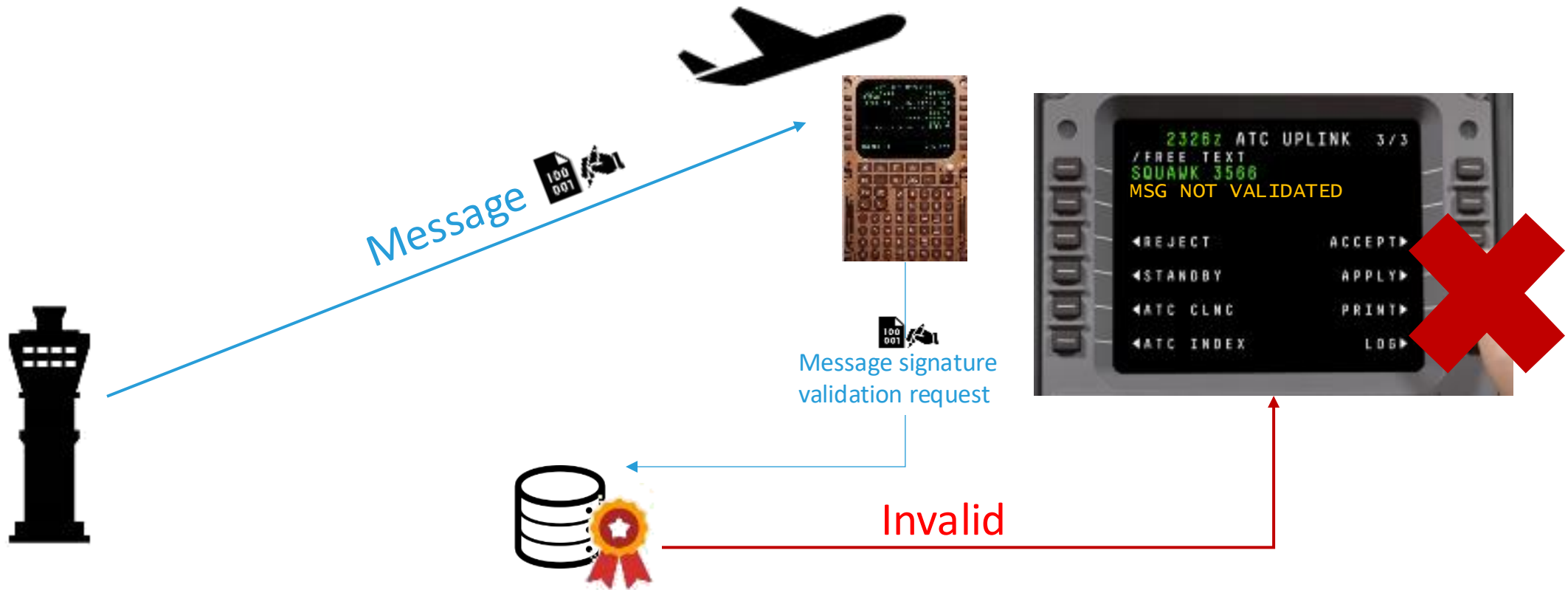


A Fundamental Question...

Can you trust these?



Hypothetical Example



A Real Example – SBAS Authentication

- GNSS spoofing is widely known
- SBAS spoofing is also a vulnerability with major safety implications
 - SBAS spoofing is not GNSS spoofing
- ICAO panels are jointly working on authentication of SBAS provisions

SBAS Authentication Certificate Profile

Digital Certificate fields

Version	3	
Serial number	Random	
Signature Algorithm	Ed25519	
Issuer	Issuer Distinguished Name	
Validity	From:	Date of creation
	To:	Date of creation + x months/weeks
Subject	Subject Distinguished Name	
Public Key Length/Type	256 bits for Ed25519	
Digital signature		
Extensions		
Subject Key Identifier (SKI)	(sha1 of the subject public key)	
Authority Key Identifier (AKI)	(sha1 of the issuer public key)	

Other areas (and who) can this apply to...

Use Case	Use Case Description	Targeted Users
Data Communications	Data communication between Air Traffic Controllers (ATCOs) and Pilots (air-ground communications) and between ATCOs from different states (ground-ground) communications.	ANSP; Airline Operations; OEM Products; Comms Service Provider
Manage Flight Plans	Steps taken by stakeholders to submit, review, approve (or reject), update and register flight plans within and between FIRs (Flight Information Regions). Digital Identity is used to assert and validate the authenticity of plans and providers.	ANSP; Airline Operations
Manage Electronic Pilot Licences	Here a pilot requests a Digital Pilot’s licence and the services available via the Trust Framework are augmented to validate the identity of the pilot (and the scope of the licence conditions) and a digital identity is created, registered and associated with the pilot’s licence.	Licencing / Registration; Personnel
USS Registration	A USS registered and certified for USS operations, by a Competent Authority, can register within the Trust Framework so that services they provide can be validated within the scope of their operations. This use case covers the steps and actors required to achieve this registration.	UAS / UTM; Licencing / Registration; OEM Products
Ramp Checks	Validation of personnel’s identity and aircraft documentation, via digital means, within and between states and regions can augment the digital identity services of a trust framework so that inspectors have the ability to confirm veracity.	Airport Operations; Personnel
UAS Operation Planning	Planning UAS operations, where interoperability with Air Traffic Controllers (ATCOs) is required to, for example approve transit of controlled airspace, requires validation of the operator and the plan submitted, which augments digital identity services.	UAS / UTM; ANSP
Electronic Flight Bags (EFBs)	The “papers” associated with flights (e.g., pax manifests, weather, flight plan routing) are being digitally transformed to be available on electronic devices (e.g., tablets) where acquisition and updates to information needs to be obtained over trusted connections from trusted sources, all vulnerable to interference.	Airline Operations / OEM Products / Comms Service Provider
Arrival M’gmt Sequences	Extended arrival management (E-AMAN) allows for the sequencing of arrival traffic much earlier than is currently the case, by extending the AMAN horizon from the airspace close to the airport to further upstream and so allowing smoother traffic management.	ANSP; Airline Operations; Airport Operations
MRO – Full Digital Interconnected Processes	Full lifecycle digital records management to track equipment from original manufacture to its installation, maintenance and replacement to include, but not limited to, its transfer between aircraft and aircraft operators.	OEM Products; Licencing / Registration; Aircraft Operators
Aerodrome Surface Traffic	Airports use Advanced Surface Movement Guidance and Control systems (A-SMGCS) to manage surface operations of vehicles and aircraft based on traffic density, complexity of aerodrome layout and operational weather conditions.	Airport Operations; Ground Handlers



Trust Framework

What is a Trust Framework?

- A trust framework can be described as a set of policies, procedures and technical requirements that enable organizations to share digital information and retain confidence that what is shared is authentic, unaltered, and sufficiently protected

Foundations of Digital Trust

- Common Baselines
 - Identity Management
 - Information Security
- Implementation
 - How-to Guidance
 - Assessment Criteria

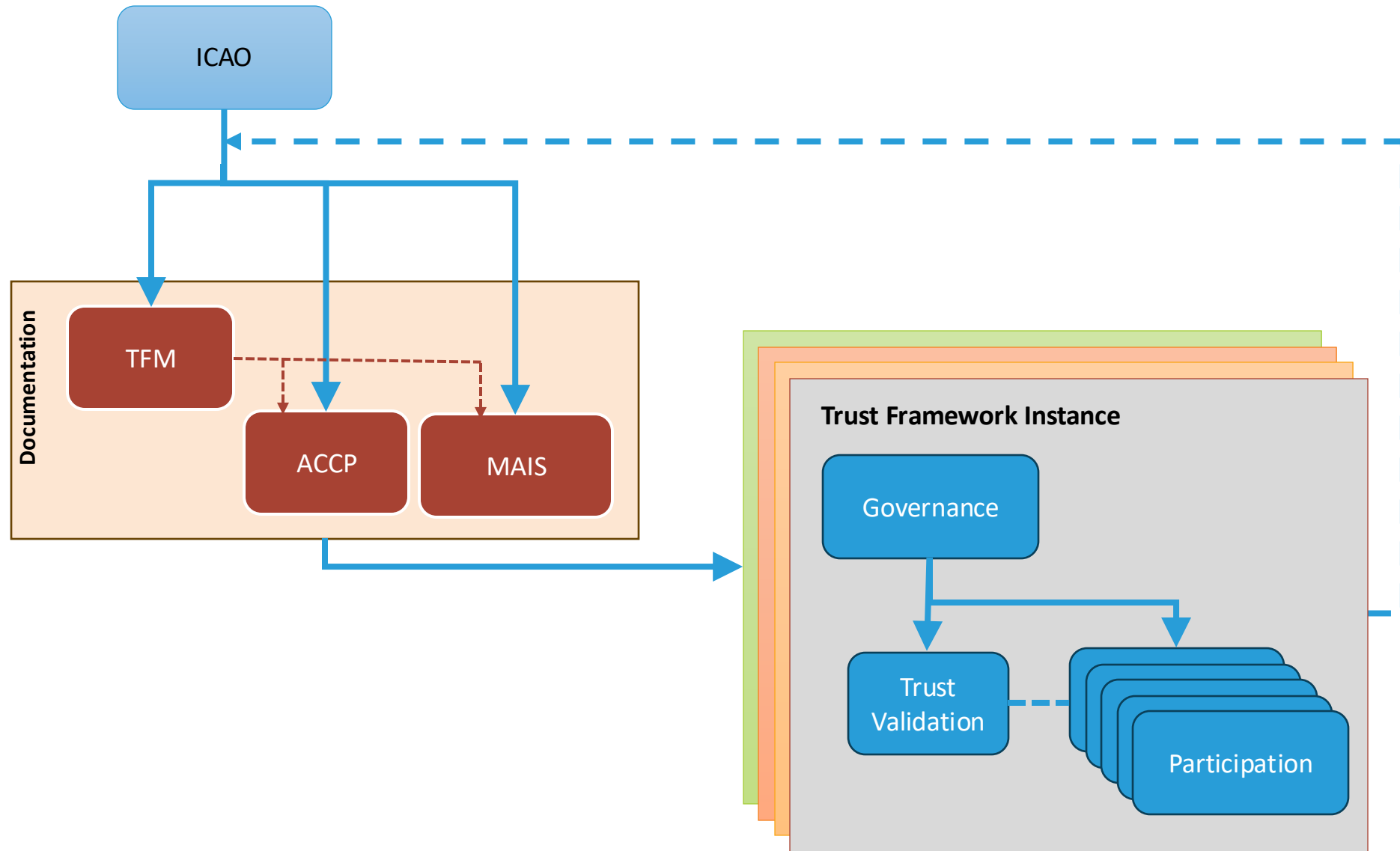
Trust Framework Instances

- A Trust Framework Instance (TFI) is a federated implementation model of a trust framework amongst organizations in an aviation domain with a common need to share information in a trusted way
- Implementations of TFIs will vary depending on many factors, but all would be based on common principles
- TFIs are self-organizing and self-governing
 - Participants agree to common baseline requirements for interoperability and assessment criteria (based on ICAO guidance)

TFI-level Functions

- Governance – how will the participants in a TFI agree to govern and assess themselves
- Validation – what is technically needed for participants to interoperate with each other
- Participation – Participant lifecycle management

At a glance...



Fundamental aspects of a TFI

- Identity assurance (IA) that provides a level of assurance that an individual, organization or device is who or what it claims to be
 - Accomplished through an identity management system
- Information security (IS) provides for information confidentiality, integrity and availability considerations that may have an impact on safety of operations
 - Realized by an information security framework

Identity Assurance

- Who (or what) are you?
- What proof do you have of this claim?
- Identity claims are based on a chain of trust
- Typically implemented as a public key infrastructure system for civil aviation (and related applications/systems)

Information Security

- Information security is the protection of information's confidentiality, integrity and availability
- An information security framework is the collection of best practices, guidelines, tools and assessment criteria that support information security

Key ICAO Deliverables

- Interoperability baseline
 - Aviation Common Certificate Policy (ACCP)
 - Manual on Aviation Information Security (MAIS)
- Implementation guidance
 - Trust Framework Manual (TFM)

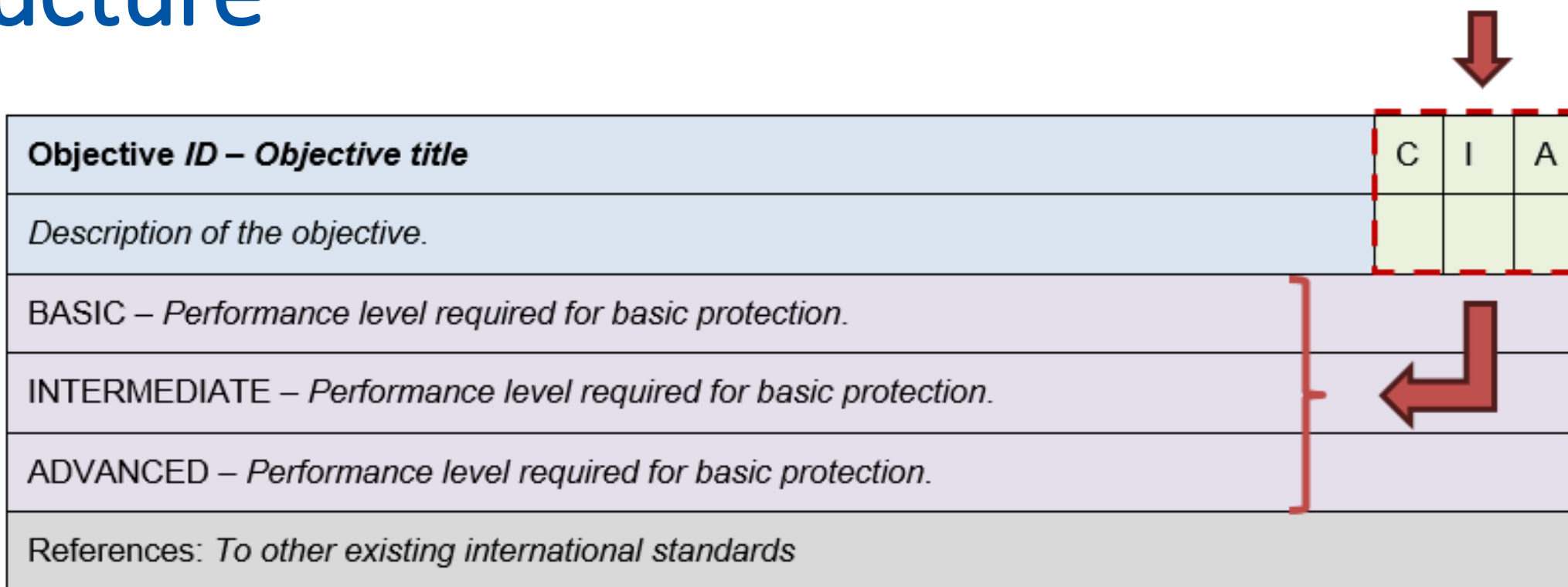
ACCP

- Provides a reference certificate policy that TFIs would instantiate for their trust validation anchors
- Provides a baseline for consistent, assessable processes and protocols for identity management
- Provides centralized catalogue of certificate profiles for aviation ecosystem users

Manual on Information Security

- Provides system owners with a common baseline for information security for external partner interoperability
- Leverages a 3-tiered (basic, intermediate, advanced) set set of performance objectives based on risk
- Is assessable (auditable) to provide trust assurance between parties

Information Security Objectives Structure



Objective ID – Objective title		C	I	A
Description of the objective.				
BASIC – Performance level required for basic protection.				
INTERMEDIATE – Performance level required for basic protection.				
ADVANCED – Performance level required for basic protection.				
References: To other existing international standards				

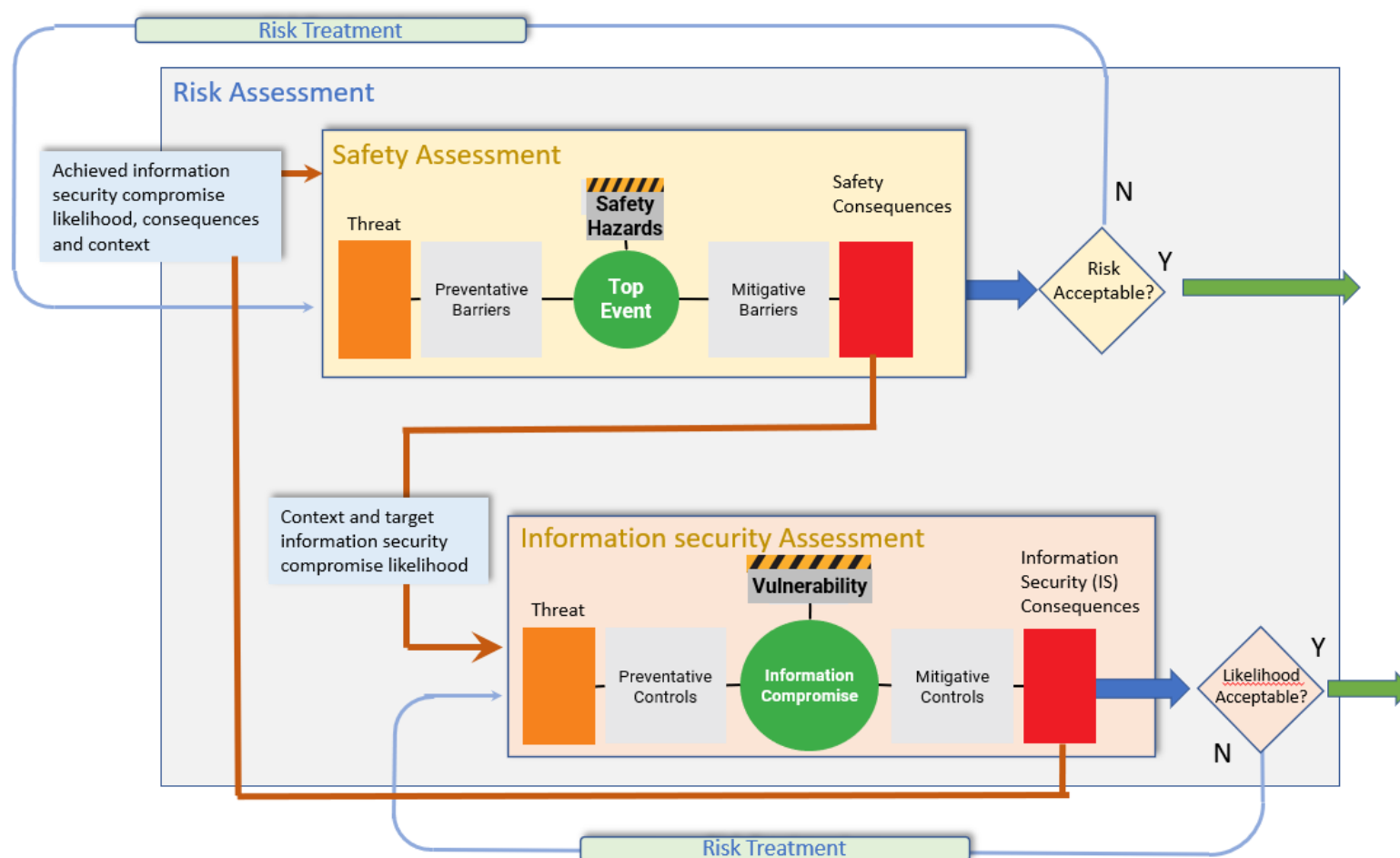
Security Objective Example

Objective CP.3 – Information system backups	C	I	A
Information system owners shall back up information systems data, system metadata and system documentation.	x	x	x
BASIC: The capability to restore data from backups should be tested on an annual basis.			
INTERMEDIATE: The capability to restore data from backups should be tested on a six month basis.			
ADVANCED: The capability to restore data from backups should be tested on a quarterly basis.			
References: NIST 800-53: CP-9, CP-9(1), CP-9(2), CP-9(3), CP-9(5).			

Associated Guidance for CP.3

- Information system owners should establish backup requirements as a part of their contingency planning process to enhance their ability to recover from an information system outage. Backup requirements may differ depending on the criticality or the function the information system. For example, an information system capturing flight data may require daily data backups with incremental backups every few hours. However, a separate information system used as a document store for non-critical reports may only need weekly backups, with incremental backups daily...

Inter-related Risk Assessment Process



MAIS Contents

- Chapter 1. Introduction
- Chapter 2. Risk Management
- Chapter 3. Information security assessment and authorization
- Chapter 4. Identity and Access Management
- Chapter 5. Information system configuration and management
- **Chapter 6. Incident response**
- Chapter 7. Continuity Planning
- Chapter 8. Information security Planning
- Chapter 9. Configuration Management
- **Chapter 10. Continuous Monitoring**
- Chapter 11. Information system maintenance
- **Chapter 12. Security in software development**
- Chapter 13. Supply chain risk management
- Chapter 14. Media Protection
- Chapter 15. Physical and environmental
- Chapter 16. Personnel security
- **Chapter 17. Information security awareness and training**

Trust Framework Manual (in development)

- Manual that will provide guidance on what a TFI is, and the circumstances that would warrant one
- Provides completely lifecycle management for TFIs
- Describes TFI pillars and functions, and relates their application to specific operational and regulatory use-cases
- Acts as the “how-to” guidance for the ACCP and the MAIS

Not Just Theoretical Work

- Technical trials underway to validate documentation produced to support TFIs
- Initial trials between FAA and EUROCONTROL concluded successfully
- Upcoming trials between FAA, EUROCONTROL and UK NATS exchanging digitally-signed flight plans

In Conclusion

- Challenges are many but solutions are emerging
- ICAO uniquely positioned to lead this effort
- Common destination, a globally interoperable sky



Thank You!