Cyber Resilience Tabletop Exercise

Presented by UAE

Amman, Jordan, 16 November 2022

Agenda

- Overview of UAE Regulations

- Cyber Security & resilience activities in UAE

- Recommendations/Proposals

Overview on UAE regulations

UAE Regulatory Updates:

- Plan to transform UAE regulations for ANSPs and to adopt necessary regulations specifically adapted for the UAE environment.

- Multiple roadshow meetings were conducted by GCAA with all UAE ANSPs and the new regulations are being finalized after incorporating the respective ANSPs amendments.

- Part of these new regulations is the guidance on clear and concise Cyber Security requirements in the form of the ICAO Mid endorsed Minimum Security Baseline(MSB) documents.
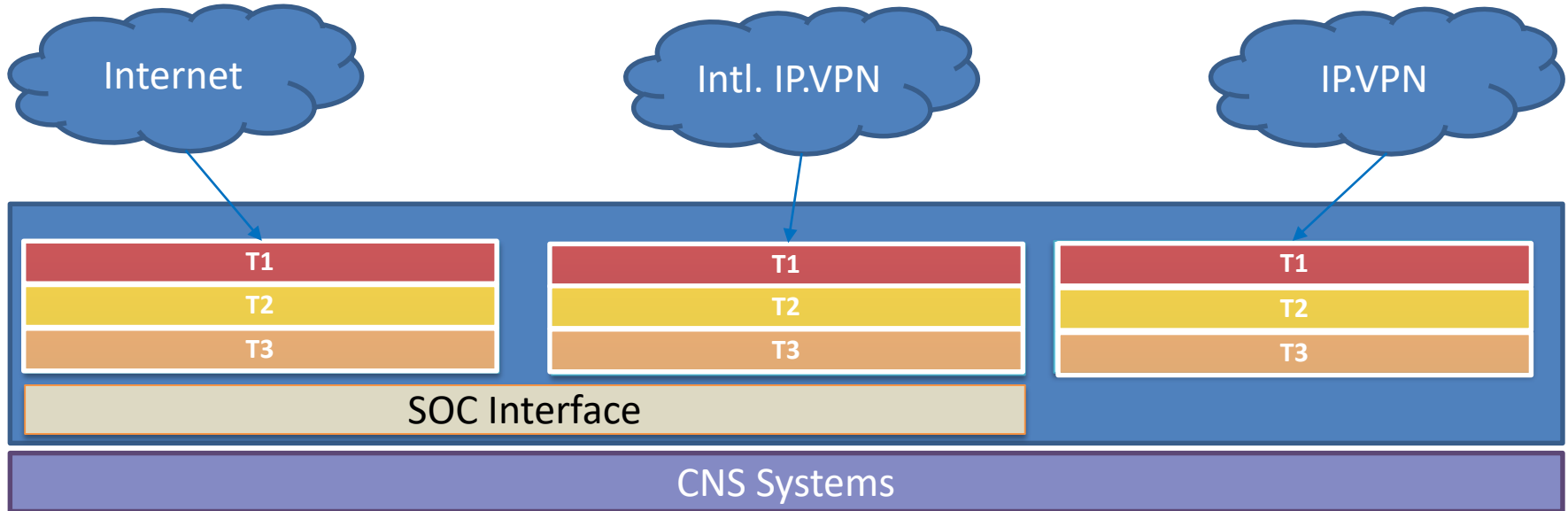
Cyber Security & resilience activities in UAE

UAE ANSPs Cyber Security Overview

- Introduction of UAE ANS Cyber Security Strategy & relevant action plans which includes:

    - Implementation of SOC (Security Operation Center) at multiple ANSPs

    - MSB Compliance Enforcement for all Systems/Vendors

    - Continuous enhancements to the regional ATM Data Cyber Security Portal (adcsportal.ae)

    - Implementation of MSB Governance Center (MSBGC) at GCAA ANS

    - Design and Development of In-house PKI (Public Key Infrastructure) House at GCAA ANS

    - Periodic multi-level Cyber Security training, workshop, and awareness sessions for all technical and non-technical staff.

    - Basic Cyber Security skills as part of CNS ATSEP certification

    - Periodic State level Cyber Security audit on operational systems

Cyber Security & resilience activities in UAE

GCAA ANS SOC Implementation:

Cyber Security & resilience activities in UAE

MSB Governance Center (MSBGC):

Vision

Ensure systematic, transparent and consistent implementation of MSB (Minimum Security Baseline) across all Systems/Vendors, thereby making the skies safer and secure
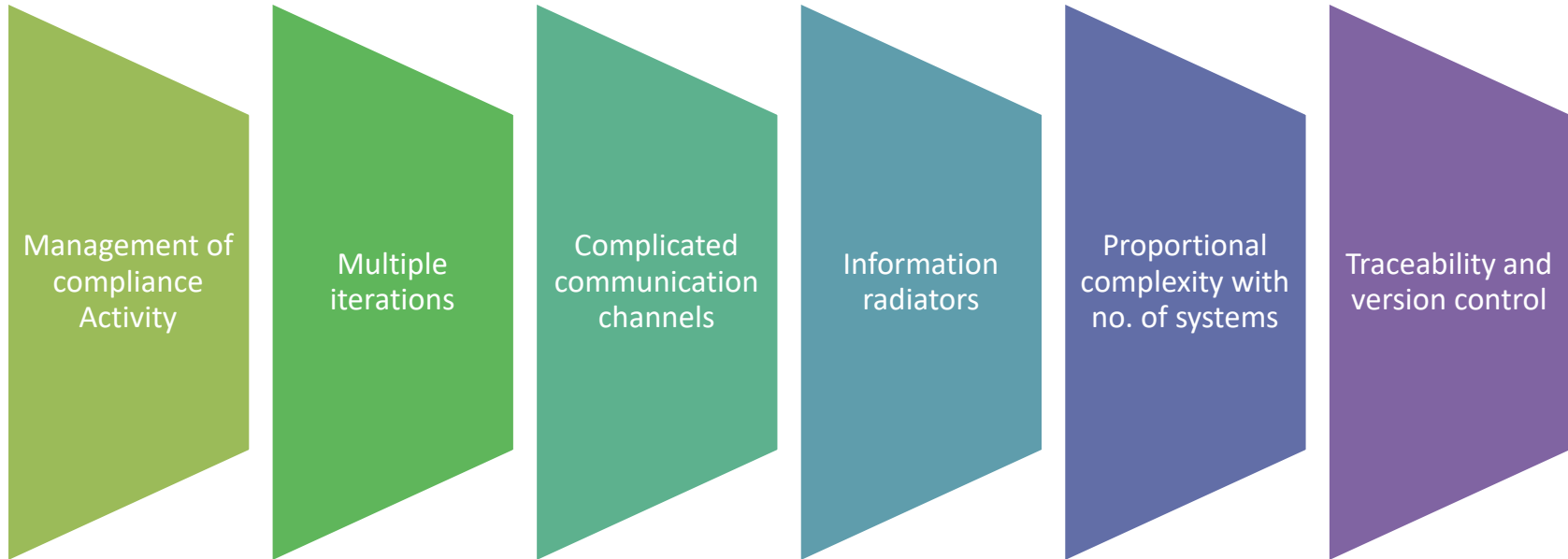
Problem Statement

As the number of products, systems and vendors increases, various challenges and risks also escalates, thus making it difficult to ensure smooth and full implementation of MSB compliance across the platforms

Cyber Security & resilience activities in UAE

MSBGC – Key Challenges

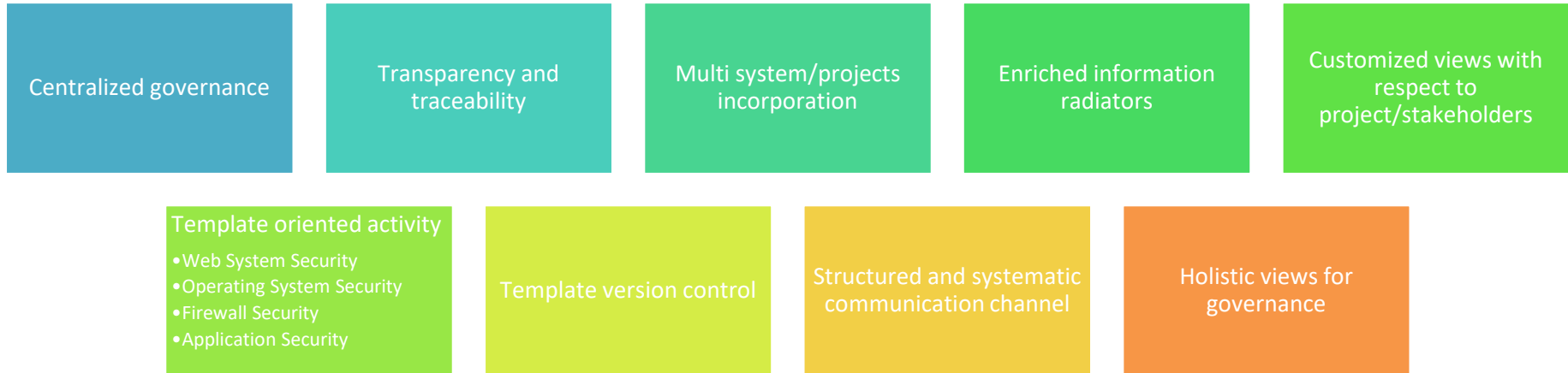| Management of compliance Activity	Multiple iterations	Complicated communication channels	Information radiators	Proportional complexity with no. of systems	Traceability and version control

Cyber Security & resilience activities in UAE

MSBGC – The Solution

To overcome challenges, GCAA-ANS came up with the solution to have a MSBGC (MSB Governance Center) system that defines/refines the process using latest tools and technologies resulting in a systematic approach to achieve the security standards within ATM systems.

Centralized governance	Transparency and traceability	Multi system/projects incorporation	Enriched information radiators	Customized views with respect to project/stakeholders

Template oriented activity
- Web System Security
- Operating System Security
- Firewall Security
- Application Security

Template version control

Structured and systematic communication channel

Holistic views for governance

Cyber Security & resilience activities in UAE

MSBGC – Value Achieved

Safe and secure skies

Systematic and structured approach, enhances effectiveness and efficiency

Holistic view provides improved governance

Information radiators increases transparency and trust between stakeholders

Effective reporting generates value for stakeholders on focused proceedings

Continuous improvements in accordance to industry or security measures.

Maximum business value to liaise with fast paced technology revolutions

Recommendations/Proposals

- It is worth noting that more than 90% of successful cyber attacks are on people and not on the equipment.

- By simply installing state of the art Cyber Security equipment will not provide an ANSP any level of protection unless there is a sound cyber strategy in place that is continuously evolving to meet the ANSP ever-changing threat landscape.

- States are, therefore, urged to align their Cyber Security strategy/policy with the ICAO requirements and industry best practices.

- States are urged to ensure the adequate training/awareness of their staff on the current cyber threats within ASNP domain as well as the traditional IT domain.

- States are urged to share information amongst each other and have continuous engagement and collaboration on cyber related activities.

- States are invited to discuss and agree on MSBGC Concepts and potential implementation benefits

Thank You.