ATM CYBERSECURITY MATURITY MODEL

27 SEPTEMBER 2018

HELIOS

an egis company

APOLOGIES FROM LAKE COMO… WISH I COULD BE WITH YOU IN GLASGOW!

RECAP: WHY DO CYBERSECURITY?

- Support **safety** as insecure systems may not be safe
- Avoid (lengthy) **outages**
- Enable **innovation** and **partnership** by information sharing
- Enable technical **modernisation** (virtualisation, cloud, etc)
- **Save money** by reducing complexity
- Protect **reputation** and **trust**
- Manage **corporate risk**
- Comply with **regulations**

WHAT IS A MATURITY MODEL?

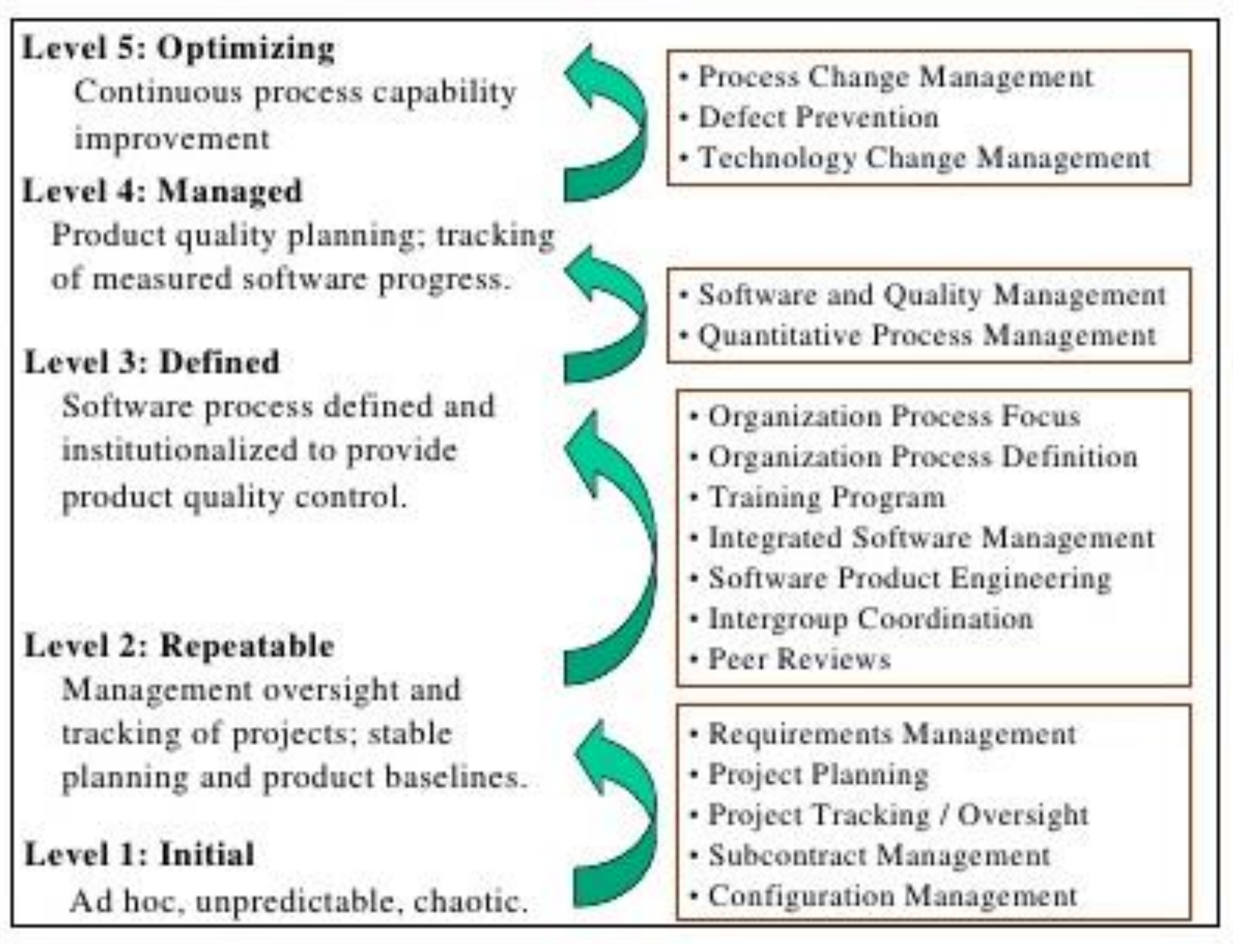
Compare own practices to model

Use evidence to back up assessment

Contains a range of capabilities

Describes a range of levels

E.g. Early model for software dev



Level 5: Optimizing
Continuous process capability improvement

- Process Change Management
- Defect Prevention
- Technology Change Management

Level 4: Managed
Product quality planning; tracking of measured software progress.

- Software and Quality Management
- Quantitative Process Management

Level 3: Defined
Software process defined and institutionalized to provide product quality control.

- Organization Process Focus
- Organization Process Definition
- Training Program
- Integrated Software Management
- Software Product Engineering
- Intergroup Coordination
- Peer Reviews

Level 2: Repeatable
Management oversight and tracking of projects; stable planning and product baselines.

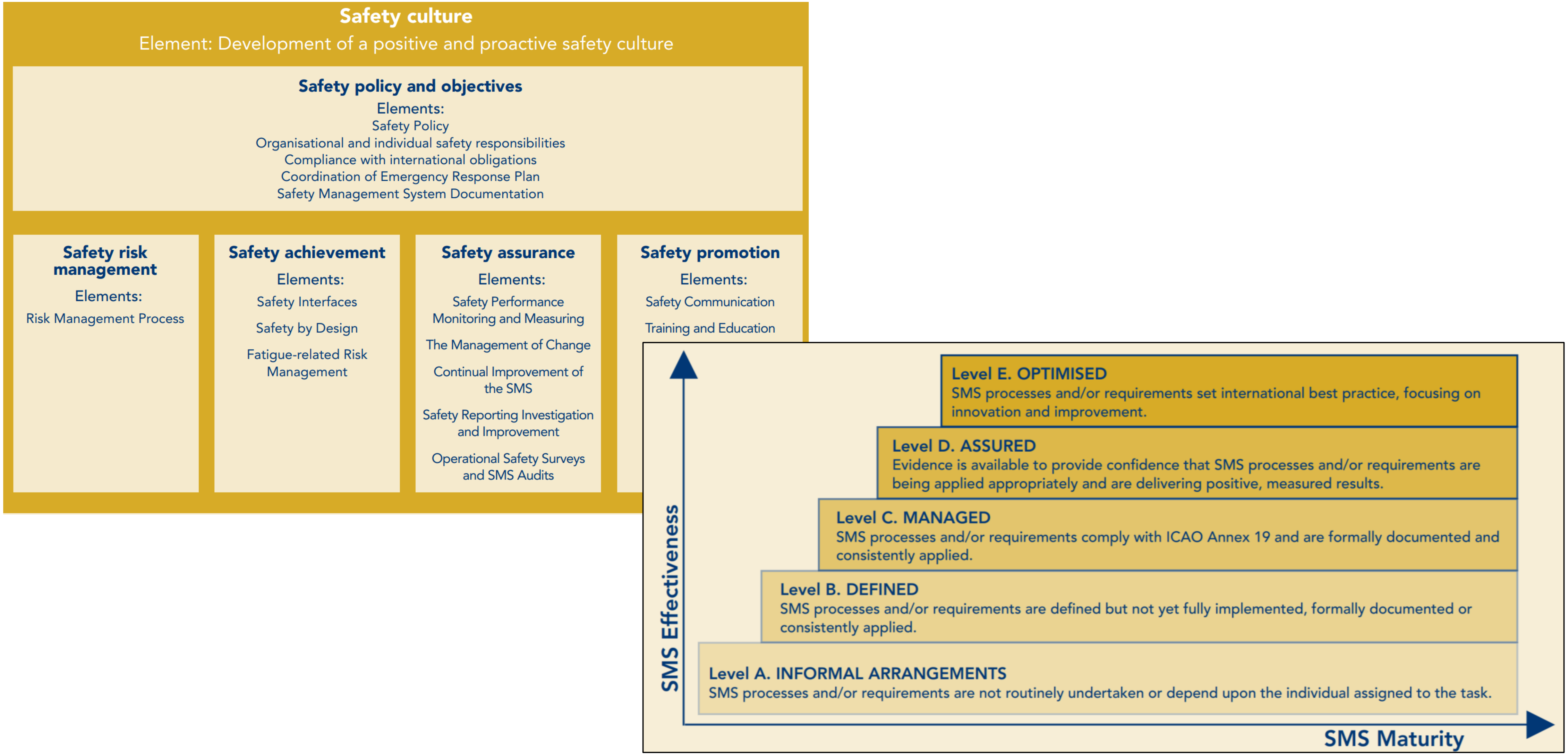
- Requirements Management
- Project Planning
- Project Tracking / Oversight
- Subcontract Management
- Configuration Management

Level 1: Initial
Ad hoc, unpredictable, chaotic.

PURPOSE OF AN ATM CYBERSECURITY MATURITY MODEL

- Common model across ANSPs/NM to:
  - Compare your ANSP to how it looked at some point in the past, to track improvements over time.
  - Compare your ANSP with others, to drive and share good practice
- Common model across suppliers to assess supply chain maturity

CYBER EQUIVALENT OF CANSO STANDARD OF EXCELLENCE IN SAFETY MGT SYSTEMS?



Safety culture

Element: Development of a positive and proactive safety culture

Safety policy and objectives

Elements:
Safety Policy
Organisational and individual safety responsibilities
Compliance with international obligations
Coordination of Emergency Response Plan
Safety Management System Documentation

Safety risk management

Elements:
Risk Management Process

Safety achievement

Elements:
Safety Interfaces
Safety by Design
Fatigue-related Risk Management

Safety assurance

Elements:
Safety Performance Monitoring and Measuring
The Management of Change
Continual Improvement of the SMS
Safety Reporting Investigation and Improvement
Operational Safety Surveys and SMS Audits

Safety promotion

Elements:
Safety Communication
Training and Education

Level E. OPTIMISED
SMS processes and/or requirements set international best practice, focusing on innovation and improvement.

Level D. ASSURED
Evidence is available to provide confidence that SMS processes and/or requirements are being applied appropriately and are delivering positive, measured results.

Level C. MANAGED
SMS processes and/or requirements comply with ICAO Annex 19 and are formally documented and consistently applied.

Level B. DEFINED
SMS processes and/or requirements are defined but not yet fully implemented, formally documented or consistently applied.

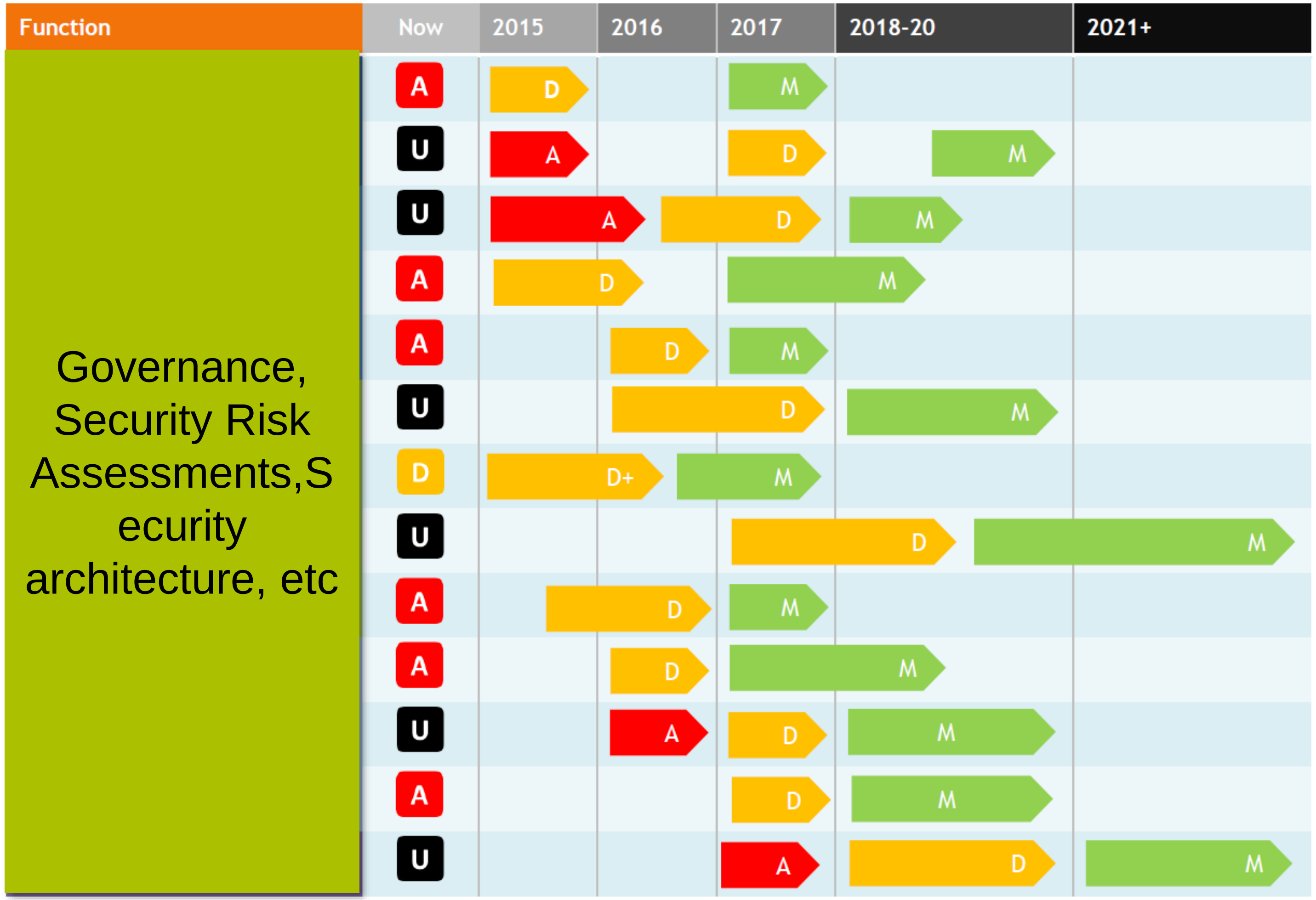
Level A. INFORMAL ARRANGEMENTS
SMS processes and/or requirements are not routinely undertaken or depend upon the individual assigned to the task.

STARTING POINT

1. Cyber regulations are high-level and risk-based… leaving us asking “What is good enough?”
2. Maturity models are a gross simplification, but are useful especially in simple reporting to management
3. ANSPs/NM and ATM suppliers are similar enough to compare
4. Only comparing is insufficient; then sharing practices is vital
5. A ‘one size fits all’ approach is tricky but possible
6. ATM has *some* unique characteristics that warrant inclusion
7. Developing an *aviation* maturity model is a step too far

CYBER MATURITY MODELS: PREVIOUS WORK ON SESAR AND FROM ELSEWHERE

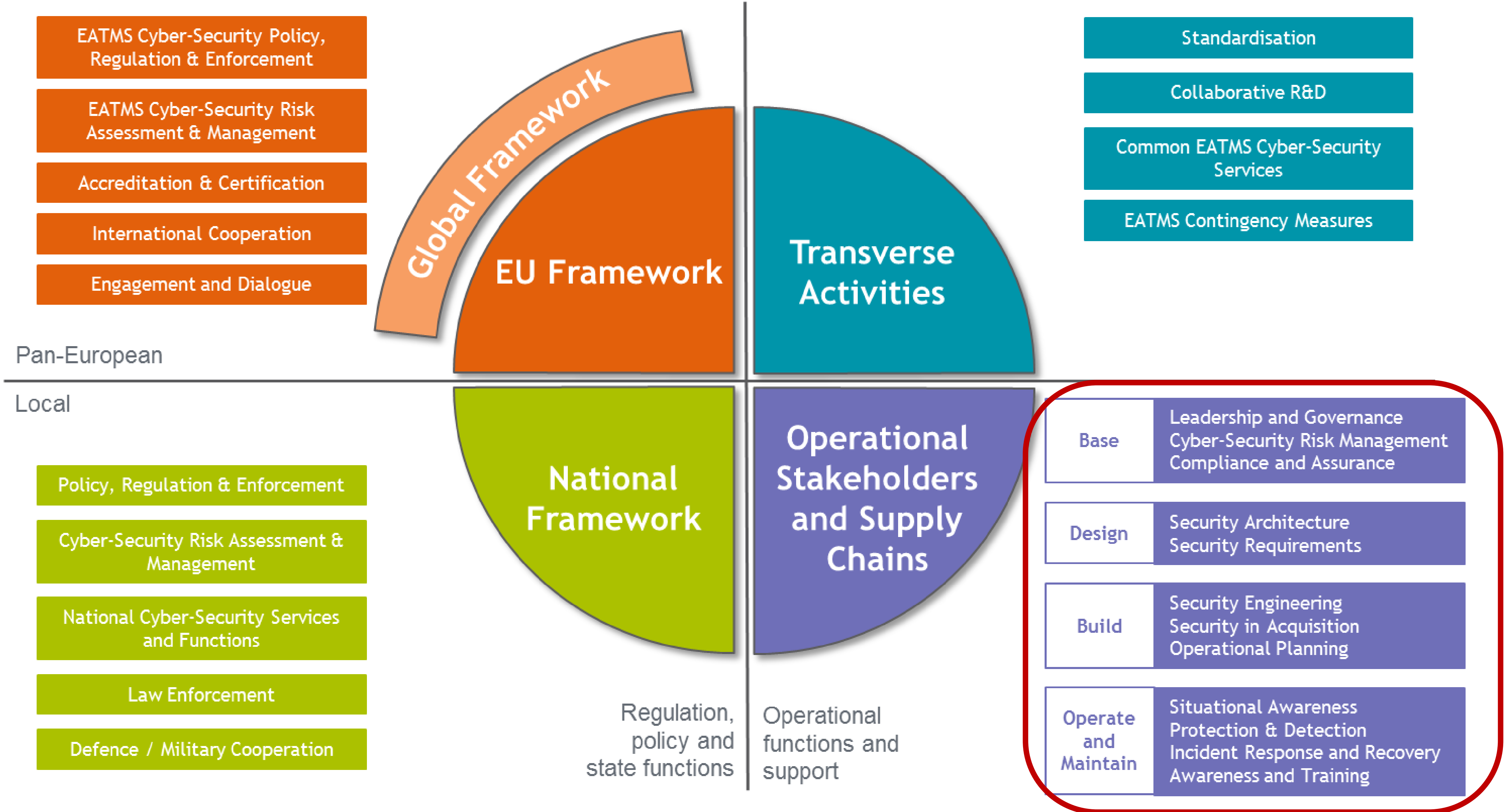
PREVIOUS WORK: SESAR WORK PROGRAMME



Function	Now	2015	2016	2017	2018-20	2021+
Governance, Security Risk Assessments,Security architecture, etc	A	D		M		
	U	A		D	M	
	U	A	D		M	
	A	D		M		
	A		D	M		
	U		D		M	
	D	D+	M			
	U			D	M	
	A	D		M		
	A		D	M		
	U		A	D	M	
	A			D	M	
	U			A	D	M

Unadressed Ad-hoc Defined Managed Optimised

PREVIOUS WORK: EUROPEAN ATM SYSTEM



- EATMS Cyber-Security Policy, Regulation & Enforcement
- EATMS Cyber-Security Risk Assessment & Management
- Accreditation & Certification
- International Cooperation
- Engagement and Dialogue

Global Framework

EU Framework

Transverse Activities

- Standardisation
- Collaborative R&D
- Common EATMS Cyber-Security Services
- EATMS Contingency Measures

Pan-European

Local

National Framework

Operational Stakeholders and Supply Chains

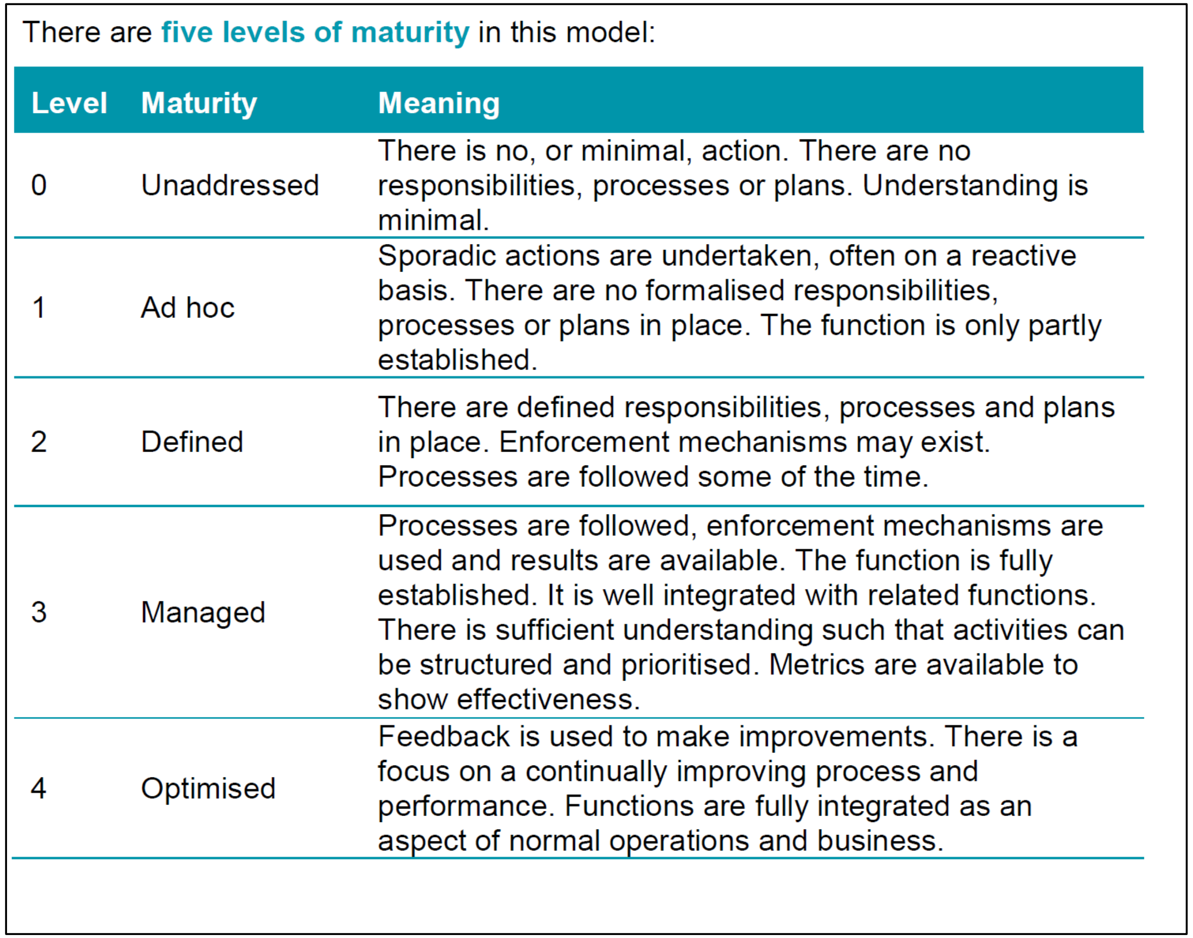
- Policy, Regulation & Enforcement
- Cyber-Security Risk Assessment & Management
- National Cyber-Security Services and Functions
- Law Enforcement
- Defence / Military Cooperation

Base	Leadership and Governance Cyber-Security Risk Management Compliance and Assurance
Design	Security Architecture Security Requirements
Build	Security Engineering Security in Acquisition Operational Planning
Operate and Maintain	Situational Awareness Protection & Detection Incident Response and Recovery Awareness and Training

Regulation, policy and state functions

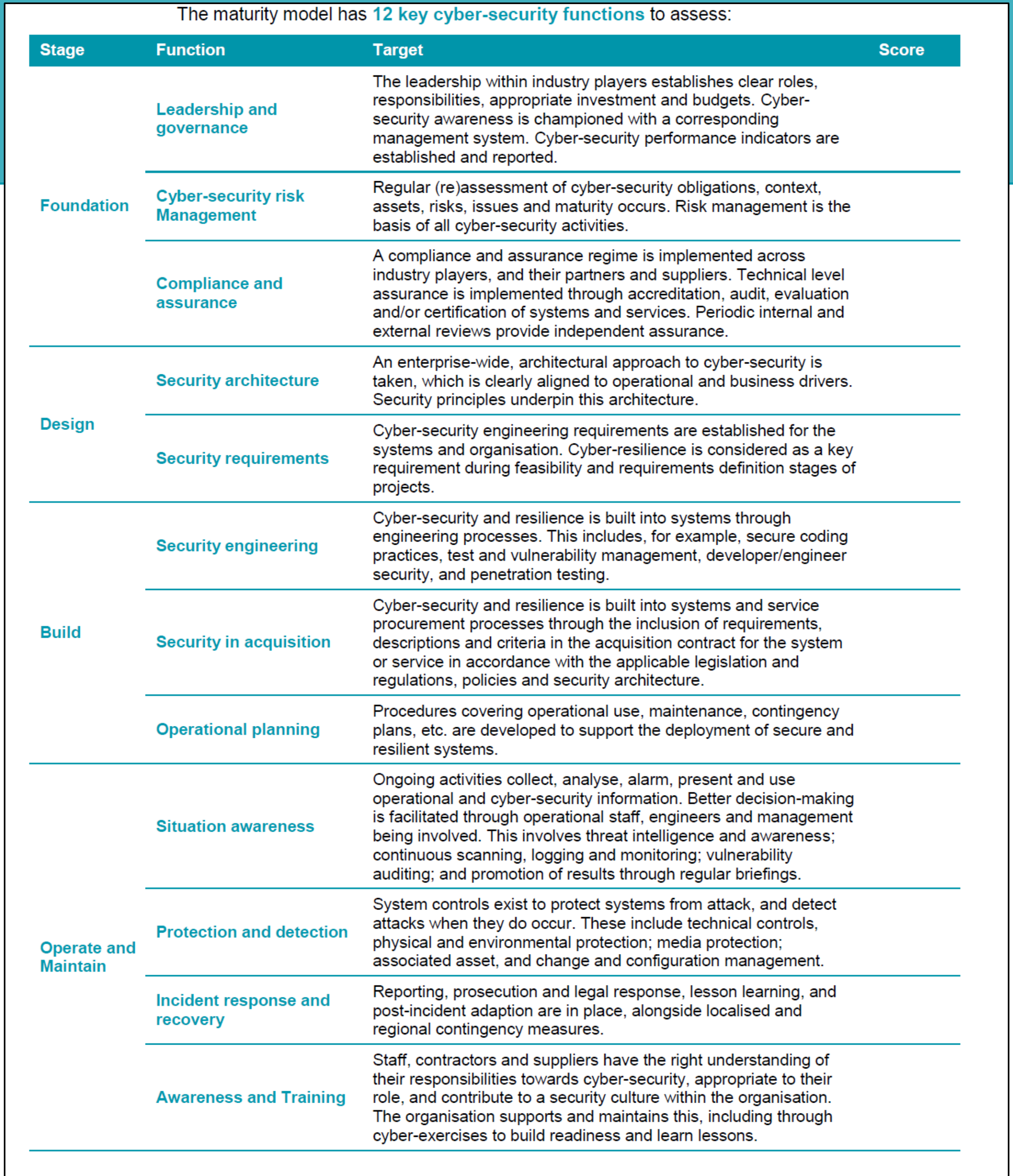
Operational functions and support

PREVIOUS WORK: APOC (ECTRL/SESAR)



There are **five levels of maturity** in this model:

Level	Maturity	Meaning
0	Unaddressed	There is no, or minimal, action. There are no responsibilities, processes or plans. Understanding is minimal.
1	Ad hoc	Sporadic actions are undertaken, often on a reactive basis. There are no formalised responsibilities, processes or plans in place. The function is only partly established.
2	Defined	There are defined responsibilities, processes and plans in place. Enforcement mechanisms may exist. Processes are followed some of the time.
3	Managed	Processes are followed, enforcement mechanisms are used and results are available. The function is fully established. It is well integrated with related functions. There is sufficient understanding such that activities can be structured and prioritised. Metrics are available to show effectiveness.
4	Optimised	Feedback is used to make improvements. There is a focus on a continually improving process and performance. Functions are fully integrated as an aspect of normal operations and business.



The maturity model has **12 key cyber-security functions** to assess:

Stage	Function	Target	Score
Foundation	Leadership and governance	The leadership within industry players establishes clear roles, responsibilities, appropriate investment and budgets. Cyber-security awareness is championed with a corresponding management system. Cyber-security performance indicators are established and reported.	
	Cyber-security risk Management	Regular (re)assessment of cyber-security obligations, context, assets, risks, issues and maturity occurs. Risk management is the basis of all cyber-security activities.	
	Compliance and assurance	A compliance and assurance regime is implemented across industry players, and their partners and suppliers. Technical level assurance is implemented through accreditation, audit, evaluation and/or certification of systems and services. Periodic internal and external reviews provide independent assurance.	
Design	Security architecture	An enterprise-wide, architectural approach to cyber-security is taken, which is clearly aligned to operational and business drivers. Security principles underpin this architecture.	
	Security requirements	Cyber-security engineering requirements are established for the systems and organisation. Cyber-resilience is considered as a key requirement during feasibility and requirements definition stages of projects.	
Build	Security engineering	Cyber-security and resilience is built into systems through engineering processes. This includes, for example, secure coding practices, test and vulnerability management, developer/engineer security, and penetration testing.	
	Security in acquisition	Cyber-security and resilience is built into systems and service procurement processes through the inclusion of requirements, descriptions and criteria in the acquisition contract for the system or service in accordance with the applicable legislation and regulations, policies and security architecture.	
	Operational planning	Procedures covering operational use, maintenance, contingency plans, etc. are developed to support the deployment of secure and resilient systems.	
Operate and Maintain	Situation awareness	Ongoing activities collect, analyse, alarm, present and use operational and cyber-security information. Better decision-making is facilitated through operational staff, engineers and management being involved. This involves threat intelligence and awareness; continuous scanning, logging and monitoring; vulnerability auditing; and promotion of results through regular briefings.	
	Protection and detection	System controls exist to protect systems from attack, and detect attacks when they do occur. These include technical controls, physical and environmental protection; media protection; associated asset, and change and configuration management.	
	Incident response and recovery	Reporting, prosecution and legal response, lesson learning, and post-incident adaption are in place, alongside localised and regional contingency measures.	
	Awareness and Training	Staff, contractors and suppliers have the right understanding of their responsibilities towards cyber-security, appropriate to their role, and contribute to a security culture within the organisation. The organisation supports and maintains this, including through cyber-exercises to build readiness and learn lessons.	

PREVIOUS WORK: UK GOV CYBER INCIDENT RESPONSE MATURITY

Level	Name	Description
0	Minimal	Essentially nothing in place
1	Defined	Written policies, procedures, etc are in place, but little evidence to demonstrate that they have been implemented and meet good practice
2	Partial	Evidence that some elements (eg for some critical systems/infrastructure) have been implemented and meet good practice, or that there is limited assurance
3	Established	Good evidence of widespread implementation (ie all critical systems/infrastructure and outsourced services), with appropriate assurance in place (eg test and exercise programmes)
4	Optimised	Evidence that lessons are being learnt, that there is a focus on improvement, that UK Government support to counter 'high threat' (where necessary) is being effective and that international mechanisms have been used
N/A	Not applicable	Capability not applicable to the organisation
N/K	Not known	Insufficient evidence was available to judge the maturity

CSIR for aviation operators - Current									
Organisation	A	B	C	D	E	F	G	H	I
Phase 1 – Prepare									
Criticality assessment	3	3	2	3	3	3	3	2	1
Safety-security planning	3	2	2	2	0	0	0	0	0
Incident response governance and planning	4	3	3	0	3	2	2	2	2
Phase 2 – Detect									
Security monitoring of external threats	3	3	2	2	2	3	3	3	2
Security monitoring of internal threats	2	2	2	0	2	2	3	0	1
Notification from 3rd parties / wider supply chain	3	2	2	1	2	2	0	0	2
Internal event reporting	4	3	3	2	2	3	3	3	1
Phase 3 – Respond									
First response, triage and assessment	4	2	2	2	3	2	2	3	2
Containment and eradication	3	3	2	3	3	2	2	2	2
Service and operational continuity	3	3	2	2	3	3	3	2	2
Recovery	3	3	2	3	2	2	2	2	1
Coordination with state	3	4	3	1	2	1	2	0	1
Collection of evidence	2	3	1	2	2	1	0	1	1
Phase 4 - Follow up									
Detailed investigation	2	3	3	2	3	2	0	2	1
Information sharing	3	2	2	2	2	2	2	0	2
Post incident review and lessons identified	4	2	2	0	3	2	2	1	1

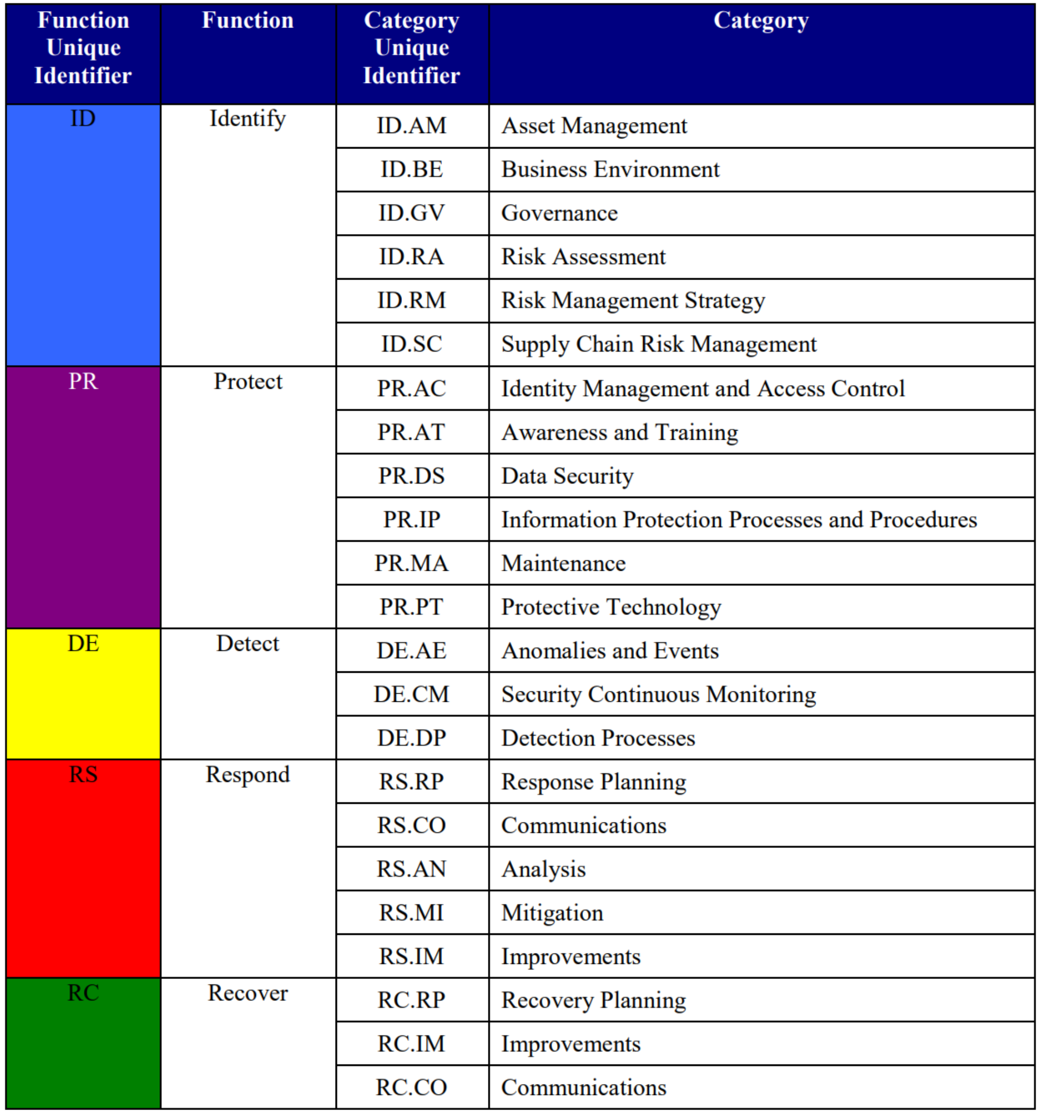
August Workshop

NATS, DFS, ENAIRE, ENAV, NAVIAIR, Network Manager

KEY DECISIONS FOR US

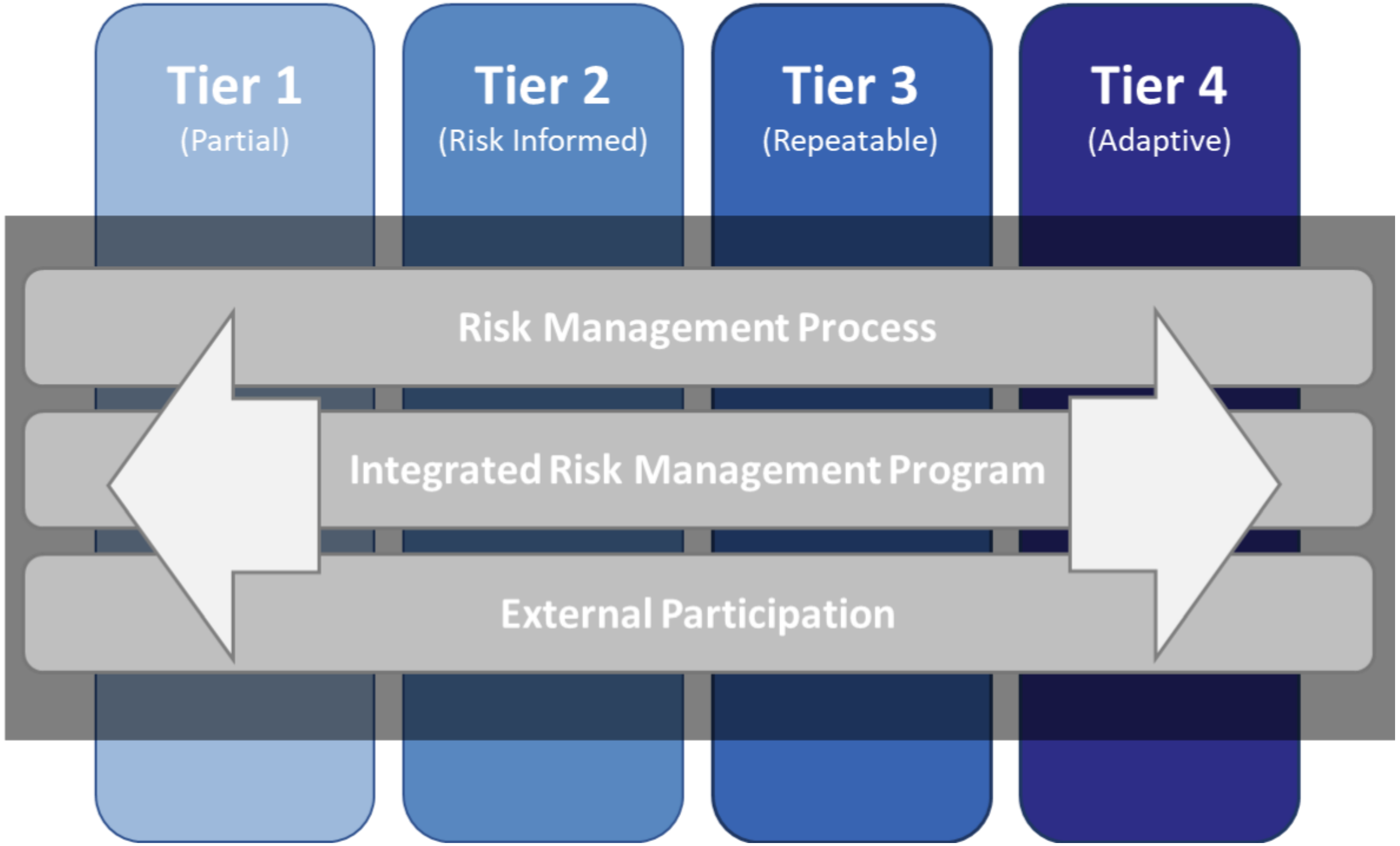
1. What is the scope? (Org vs SecMS/ISMS vs System-level)
2. Adopt, adapt or create? What are the capabilities and levels?
3. Which standard(s) to link to?
    - NIST cyber standards from US
    - ISO 27k Information Security
    - ED-205 ATM systems security specification
    - EN 16495 Information security for ATM
4. How tailored to ATM? What additional capabilities?
5. What objective criteria / evidence is expected?

RECOMMENDATION FROM NATS CISO: ADAPT NIST CSF

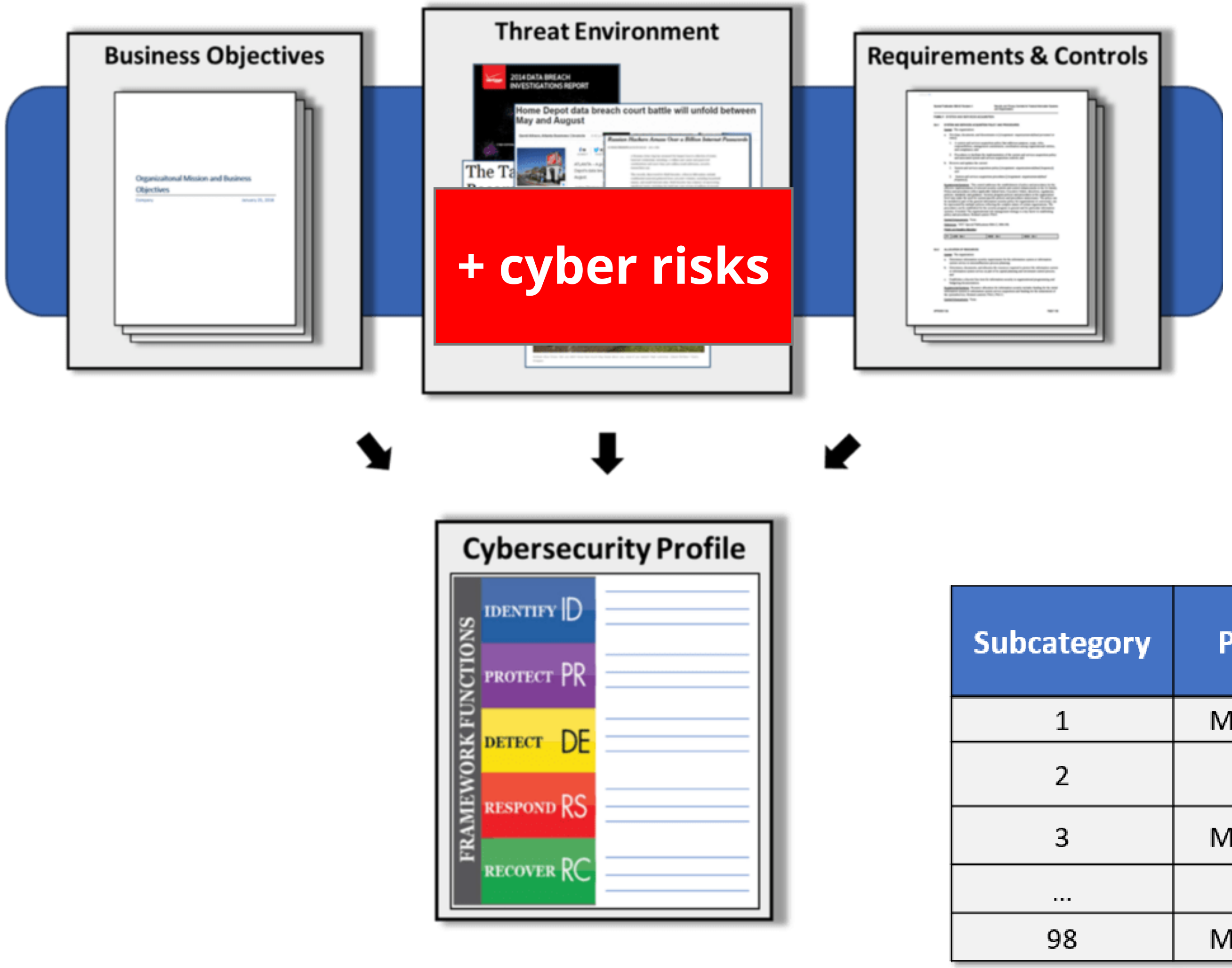


Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- From recent discussion with UK, Australia, NZ, Germany and Canada ANSPs



NIST CYBER SECURITY FRAMEWORK



Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

Target Profile

SUGGESTION #2: TWO STAGE MATURITY MODEL

- **Stage one** – a high level maturity assessment (eg NIST CSF categories) with around 12-15 questions with a CMMI-like answer set showing examples of what a 3 means, and what a 4 means etc.
- **Stage two** – a lower level maturity assessment, breaking down each of the stage one questions into a category – so say 2-5 sub questions for each of the 12-15 categories'
- For each of the questions, link them to a lifecycle position (e.g. Protect/Detect/Respond etc) and a control type (e.g. People/Process/Technology) so that the automated reporting you include can highlights where the ANSP is strong and weak, and this can help drive additional investment

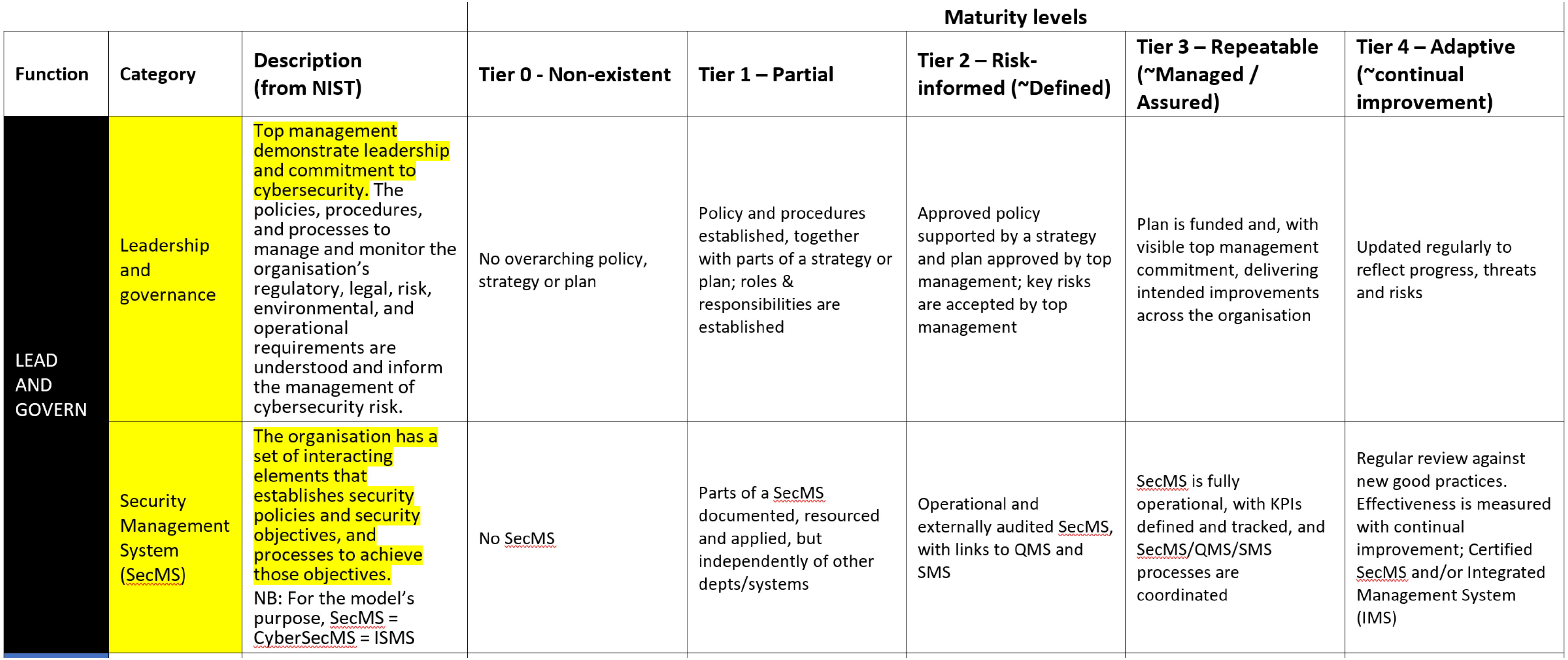
WORKSHOP DISCUSSION

- Keep it simple (“something that Grandma could understand”)
    - “Perfect is the enemy of good”
    - “As simple as possible, but no simpler”
    - “Not a comprehensive audit”
    - “Visual is good for senior management”
- Should help drive goal-setting and investment decisions
- Use NIST CSF as pragmatic, but add SecMS parts from ISO27k
    - Leadership, governance and management are crucial!
- Should be at organisation- and process-level, not system-level
    - Should not introduce new requirements
- Threat awareness vital for risk awareness
    - Maturity likely to degrade over time due to new threats

ASSESS YOUR MATURITY AND THAT OF YOUR SUPPLIERS

Function	Category	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
LEAD AND GOVERN	Leadership and governance	3	3	3	2	1	1
	Security Management System (SecMS)	2	3	2	2	2	1
IDENTIFY	Asset Management	4	4	3	2	2	1
	Risk Assessment	1	3	3	1	2	1
	Risk Management Strategy	2	3	2	1	1	0
	Supply Chain Risk Management	2	3	3	2	1	0
PROTECT	Identity Management and Access Control	3	4	2	2	3	2
	Awareness and Training	1	3	3	2	2	0
	Protective Technology	3	4	2	3	1	1
DETECT	Anomalies and Events	3	2	2	2	2	0
RESPOND	Response Planning	2	3	3	3	0	0
	Mitigation	3	3	2	2	0	1
RECOVER	Recovery Planning	3	3	3	1	2	1

DRAFT MODEL – SEE WORD FILE FOR REST



			Maturity levels				
Function	**Category**	**Description (from NIST)**	**Tier 0 - Non-existent**	**Tier 1 – Partial**	**Tier 2 – Risk-informed (~Defined)**	**Tier 3 – Repeatable (~Managed / Assured)**	**Tier 4 – Adaptive (~continual improvement)**
LEAD AND GOVERN	Leadership and governance	Top management demonstrate leadership and commitment to cybersecurity. The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	No overarching policy, strategy or plan	Policy and procedures established, together with parts of a strategy or plan; roles & responsibilities are established	Approved policy supported by a strategy and plan approved by top management; key risks are accepted by top management	Plan is funded and, with visible top management commitment, delivering intended improvements across the organisation	Updated regularly to reflect progress, threats and risks
	Security Management System (SecMS)	The organisation has a set of interacting elements that establishes security policies and security objectives, and processes to achieve those objectives. NB: For the model's purpose, SecMS = CyberSecMS = ISMS	No SecMS	Parts of a SecMS documented, resourced and applied, but independently of other depts/systems	Operational and externally audited SecMS, with links to QMS and SMS	SecMS is fully operational, with KPIs defined and tracked, and SecMS/QMS/SMS processes are coordinated	Regular review against new good practices. Effectiveness is measured with continual improvement; Certified SecMS and/or Integrated Management System (IMS)

NEXT STEPS

- Out for review with ANSPs
- Being used by Network Manager security review study
- Being informally trialled elsewhere
- Next workshop on 5 November to refine

- Please use, feed back your experience and come to the workshop

SAFETY AND SECURITY

THOUGHTS FOR DISCUSSION

GM FOR COMMON REQUIREMENTS 2017/373

GM1 ATM/ANS.OR.B.005 Management system:

- “Traditionally, separate management systems were developed to address issues such as safety, quality, environment, health and safety, finance, human resources, information technology and data protection. However, it is foreseen that more and more the services providers will establish integrated management systems following the harmonised set of requirements in this Regulation.
- The Regulation does not require that the different management systems are integrated but it facilitates their integration”

EXAMPLE: EASA GM ON THE IMPLEMENTATION OF THE REMOTE TOWER CONCEPT FOR SINGLE MODE OF OPERATION

- "Consequently, the introduction of the remote tower concept may affect the security risk assessment and these security vulnerabilities may have an impact on safety. For this reason, these security vulnerabilities may add new causes to the existing safety hazards (e.g. possible corruption of navigation aids information, loss of visual presentation data) or may add new hazards (e.g. complete loss of the provision of ATS). Based on these considerations, the ATS provider should conduct a dedicated security risk analysis and take the necessary measures to protect its systems and constituents against information and cyber security threats."

NSA DISCUSSION ON CYBERSECURITY AND SAFETY (2017)

“Insecure systems cannot be assumed to be safe”

- “But not all cyber-impacts are on safety of life”
- “Cybersecurity is not just safety”
- "Security is a pre-requisite for safety”

“Safety cases have limited value unless security has been addressed”

“Safety assurance requires effective and demonstrable cyber-security”

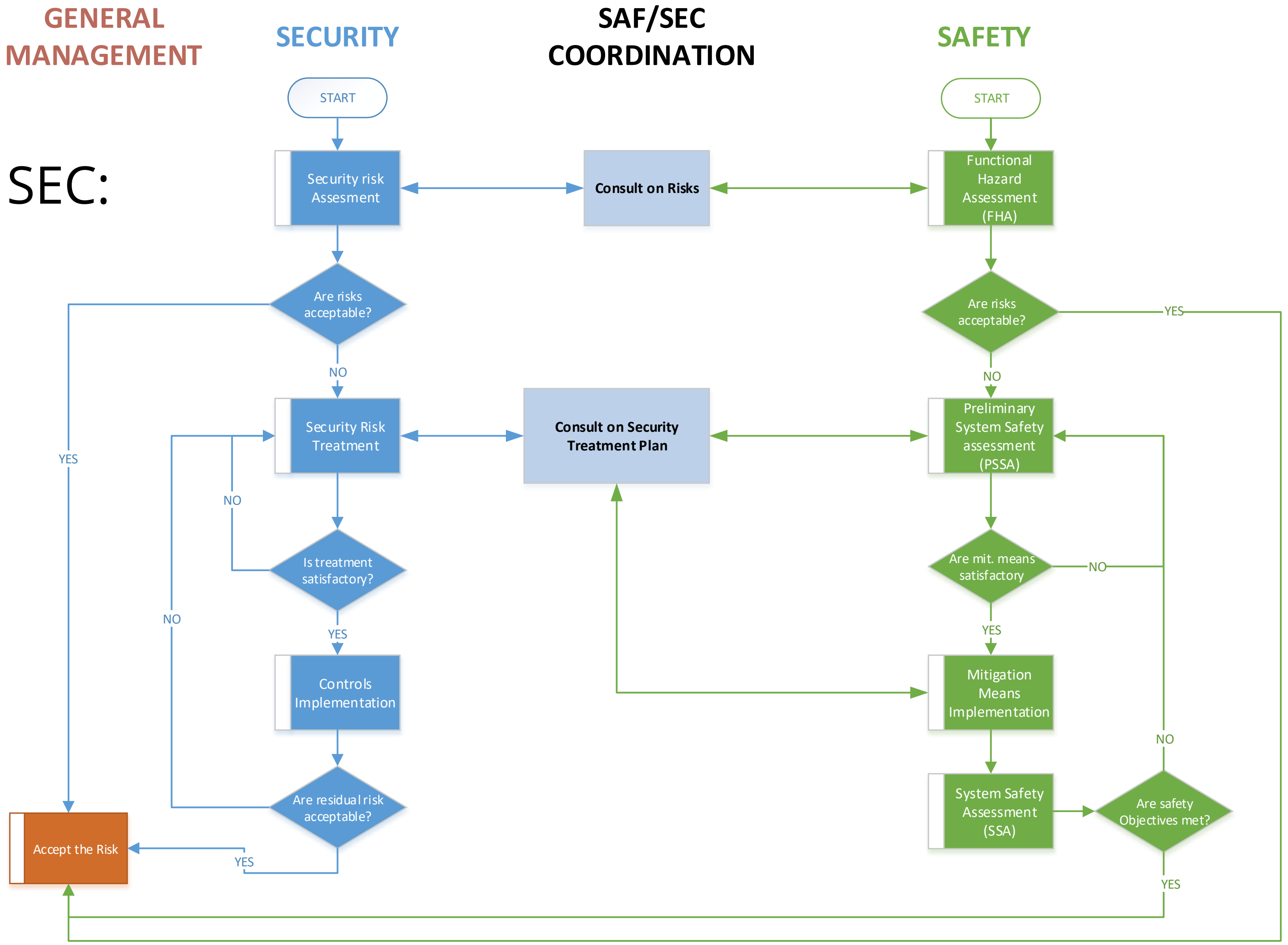
“Cyber-informed safety oversight of changes and certification of ANSPs are the fundamental roles, and the key areas to address”

“Some NSAs are starting to develop procedures for oversight of changes that combine these considerations”

“Cyber-incidents can either directly or indirectly cause safety hazards”

NEW STANDARD ED-205: PROCESS STANDARD FOR SECURITY CERTIFICATION / DECLARATION OF ATM/ANS GROUND SYSTEMS

Touchpoints between SAF and SEC:

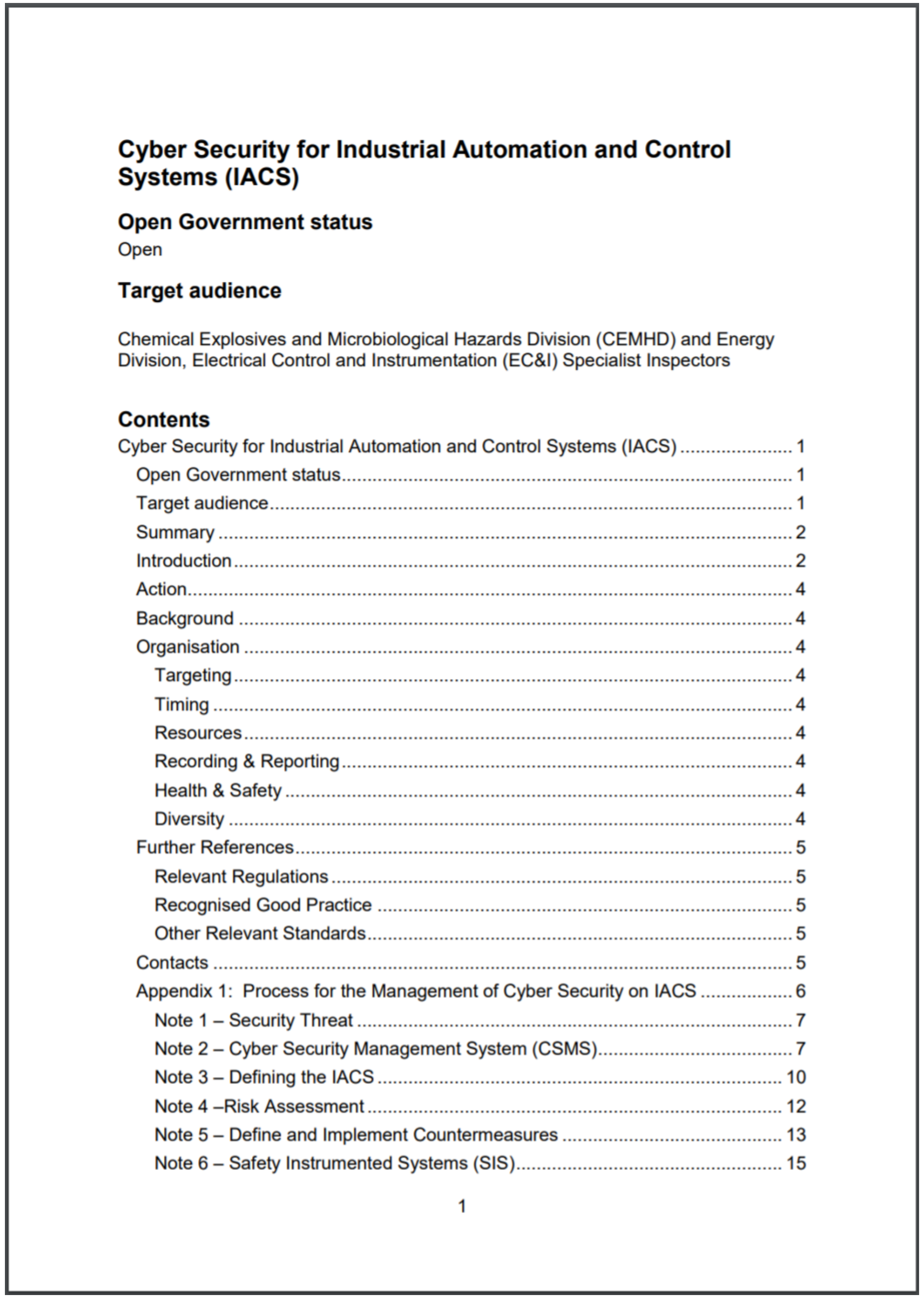

GENERAL MANAGEMENT
SECURITY
SAF/SEC COORDINATION
SAFETY
START
Security risk Assesment
Consult on Risks
START
Functional Hazard Assessment (FHA)
Are risks acceptable?
Are risks acceptable?
YES
NO
NO
YES
Security Risk Treatment
Consult on Security Treatment Plan
Preliminary System Safety assessment (PSSA)
NO
Is treatment satisfactory?
Are mit. means satisfactory
NO
NO
YES
YES
Controls Implementation
Mitigation Means Implementation
NO
Are residual risk acceptable?
System Safety Assessment (SSA)
Are safety Objectives met?
Accept the Risk
YES
YES

NEW STANDARD EN 16495 ATM – INFOSEC FOR ORGS SUPPORTING CIVIL AVIATION OPERATIONS

A.2.3 Alignment of safety and security risk management

- "Both safety and security form elements of an overall risk management in many organisations in ATM. This should be reflected in aviation in a consistent approach to safety and security in terms of:
- A consistent representation of the processes and assets, that are subject to individual safety and security-cases.
- An "all hazards" approach considering both "unintentional events" in terms of technical failure, acts of god, human error, organisational weaknesses as well as the intentional acts i.e. crime and terror
- An "all impacts" approach considering all relevant aviation key performance areas. While Safety as the aim to "protect life and limb" stands out, other areas – notably Capacity and Cost Effectiveness – need to be considered as well.
- Alignment of safety and security should also include the identification and resolution of conflicts between risk mitigation measures."

- http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf



Cyber Security for Industrial Automation and Control Systems (IACS)

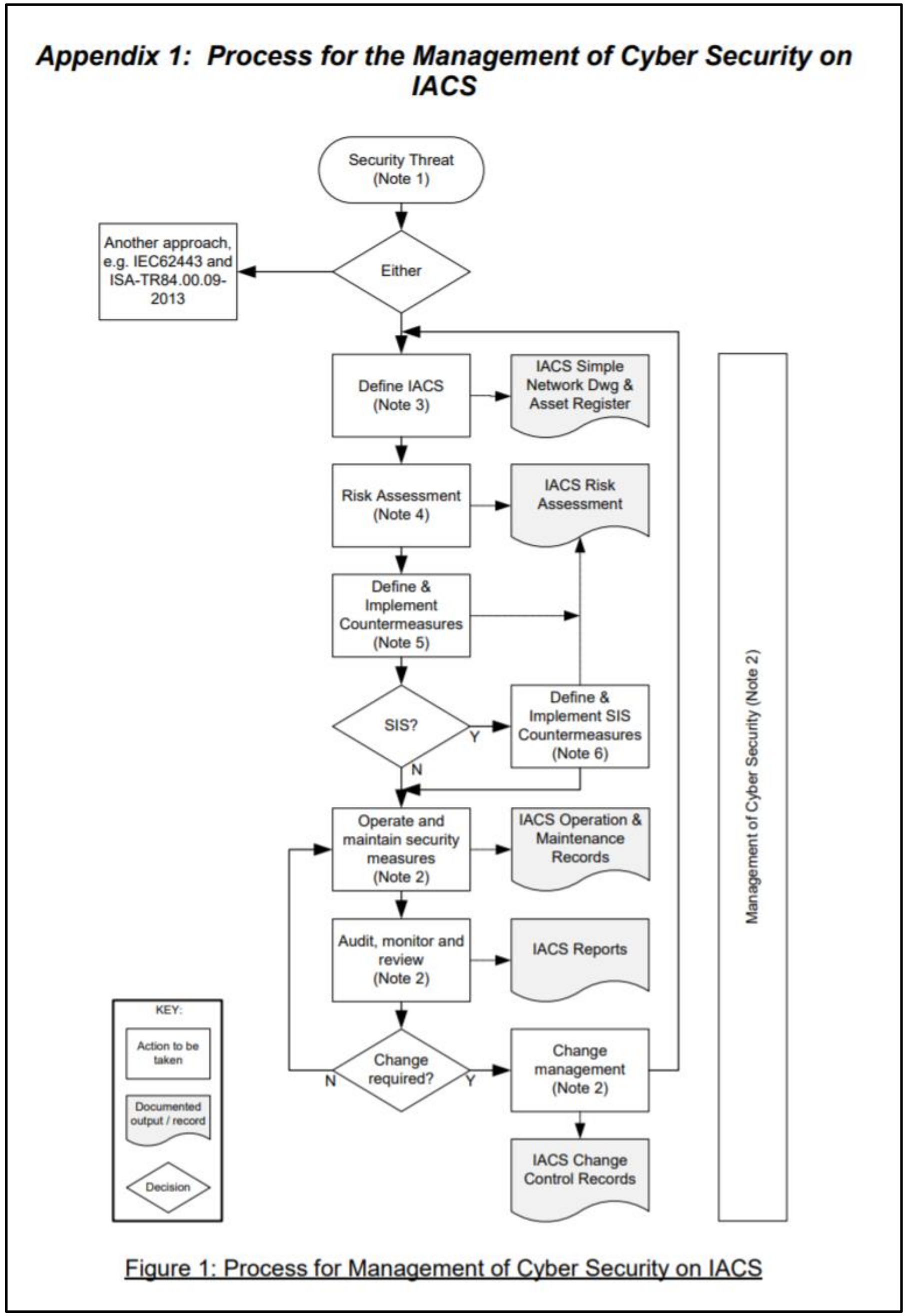
Open Government status

Open

Target audience

Chemical Explosives and Microbiological Hazards Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors

Contents



Appendix 1: Process for the Management of Cyber Security on IACS

Security Threat (Note 1)
Either
Another approach, e.g. IEC62443 and ISA-TR84.00.09-2013
Define IACS (Note 3)
IACS Simple Network Dwg & Asset Register
Risk Assessment (Note 4)
IACS Risk Assessment
Define & Implement Countermeasures (Note 5)
SIS?
Y
N
Define & Implement SIS Countermeasures (Note 6)
Operate and maintain security measures (Note 2)
IACS Operation & Maintenance Records
Audit, monitor and review (Note 2)
IACS Reports
Change required?
N
Y
Change management (Note 2)
IACS Change Control Records
Management of Cyber Security (Note 2)
KEY:
Action to be taken
Documented output / record
Decision

Figure 1: Process for Management of Cyber Security on IACS

OPEN QUESTIONS FOR DISCUSSION

- How is SEC already addressed within SAF activities?
- How best to achieve effective and efficient coordination between SAF and SEC?
- What are the links to other related risk management disciplines (eg BCM, Quality)?
- What are the pros, cons and challenges of further integration?

29 Hercules Way
Aerospace Boulevard
AeroPark
Farnborough I Hampshire
GU14 6UU I UK
Tel: +44 1252 451 651
www.askhelios.com

HELIOS
an egis company