EUROCONTROL

ATM Cybersecurity Maturity Model Level 1

Edition: 1.0
Edition date: October 2017
Status: Released
Intended for: General Public

SUPPORTING EUROPEAN AVIATION

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Head of SQS Unit	Dr. Frederic Lieutaud	
Head of Safety Unit, DNM, NOM	Mr. Antonio Licu	
Head of Network Operations Management Division	Mr. Kenneth Thomas	
Director NM	Mr. Joe Sultana	

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	30/06/2018		Creation of the Working Draft	All
0.2	23/08/2019		Draft version after 22 Aug 2018 Workshop with ANSPs and NM	All
0.3	22/09/2018		Incorporating the comments after initial trials and in prep for the WS on 5th of Nov with ANSPs and NM	All
0.4	22/10/2018		Version post Workshop on 5th of Nov	All
0.5	10/01/2019		Version in advance of 14 Feb 2019 WS with ANSPs and NM and incorporating all the feed-back from application with NM top 10 suppliers and ANSP trial of the model	All
0.6	15/02/2019		Proposed Issue after WS on 14th Feb	All
1.0	20/02/2019		Released issue	

CONTENTS

Introduction

What is a cybersecurity maturity model?	A cybersecurity maturity model describes a range of capabilities that you would expect to see in an organisation with an effective approach to cybersecurity. Each capability will have a description of the kinds of activities and processes you would expect to see, at different levels of maturity. An organisation assessing its overall cybersecurity maturity compares its own practices against those described in the levels of each capability, backing up the assessment with some evidence to justify the result. Maturity models are a highly simplified (but still useful) view of reality. They are not the same as a detailed audit, gap analysis and/or review, which still serve crucial purposes in cybersecurity.
Who is the model for?	The model is for Chief Information Security Officer (CISO) and/or cybersecurity managers (and similar roles) to use. Given the simplicity of the results, and focus on the most critical elements, the audience of the maturity is most likely to be top management.
How has the model been created?	EUROCONTROL's Network Manager (NM) commissioned a review by Helios, partnering with Prof Chris Johnson, to undertake a review of the cybersecurity of the NM and its critical suppliers. A maturity model approach was taken to be able to compare the suppliers. Publishing the maturity model for wider use is one of the review's goals. The initial model was developed after an August 2018 workshop with the NM and various Air Navigation Service Providers (ANSPs). The workshop identified critical areas and generated ideas that were then consolidated into a model to be road-tested with NM suppliers and revised as a result. Further updates are expected to refine the model over time (e.g. to automate reporting and to link the capabilities to a control type – i.e. People/Process/Technology - so that it can highlight where the organisation is strong and weak, and this can help drive additional investment).
Why create an ATM cybersecurity maturity model?	Being developed by the NM and ANSPs, and being used in the Air Traffic Management (ATM) industry, the model has most immediate applicability to ATM. Whilst not being designed for wider application, it may be useful. The potential usefulness of a model had been expressed by some ANSPs, and this model combines the elements that are most relevant to ATM today. In reality, this is a mixture and tailoring of various wider standards and guidelines. Note that the model does not identify new requirements for ATM stakeholders – instead it is capability and process-based, leaving detailed requirements to each organisation. Another advantage of using the model is that it gives a snapshot that brings together much information that may not otherwise be in a single document.

Is the model based on a standard?	Yes, the model is founded on NIST's Cyber Security Framework (CSF), together with some elements of ISO 27001. NIST CSF was chosen as a pragmatic and well-used standard. The 'Tiers' within the CSF were a helpful starting point, and linked (crucially) to a wider target-setting process that encompasses an organisation's business objectives, threat/risk environment, and requirements and controls. The CSF was extended to emphasise the leadership and governance, drawing on ISO 27001. The role of human factors in security has also been emphasised. The purpose of the model is to highlight the most critical elements in the ATM context. It is not a replacement for applying the whole standard. To maintain traceability with the NIST CSF, the highlighted text denotes new/modified text with respect to the NIST CSF
How can the model be used?	As a common reference in the ATM industry, four use cases are foreseen: 1. Comparing your organisation to how it looked in the past, to track improvements over time 2. Comparing your organisation to how it should look in the future after a roadmap of improvements is completed 3. Comparing your organisation's practices with others to develop and share good practice 4. Assessing suppliers and supply chain maturity
How many maturity levels are there?	There are five maturity levels defined, ranging from 'Non-existent' to 'Adaptive'. These are inspired by the 'Tier' terminology from the NIST CSF.
Does my organisation need to be at the highest level of cyber-maturity?	No. The model allows a broad assessment of strengths and weaknesses. Crucially it should facilitate discussions over improvement areas and the practices required to improve maturity. However, the overall goal is unlikely to be the highest level of maturity on all scores as each organisation's target is different, depending on threats, budget, etc.
How do I use the model?	The model has two levels of detail. Use of the high-level model is described here. It be undertaken independently of the more detailed model. The more detailed model is described later. The high-level model is a really simple maturity assessment with 13 capabilities and a classic maturity model answer set, indicating what Level 3 means, and what Level 4 means, etc. This enables assessment in under an hour by someone who has a suitably broad overview of that organisation. Given the broad and holistic nature of the maturity model, assessments from a range of perspectives, including from technical and operational personnel, will often be needed. Discussion and insight arising from any differences in perspective are a benefit of the assessment. The selected capabilities are the ones that are seen as most important and relevant. A form is provided to complete, including rationale and evidence. Your organisation must fulfil all elements of one level before you can say you are at next level; i.e. if you are any missing earlier elements then you must assess yourself at the lowest level that you fulfil all elements. Each capability also has a set of 'probing questions' that can be used to challenge the organisation through more open questioning. Application to a supplier can be done by the supplier itself, or by the customer or a third party. The model can, of course, be adapted as required for your organisation. In that sense, it simply offers a potential framework to use.

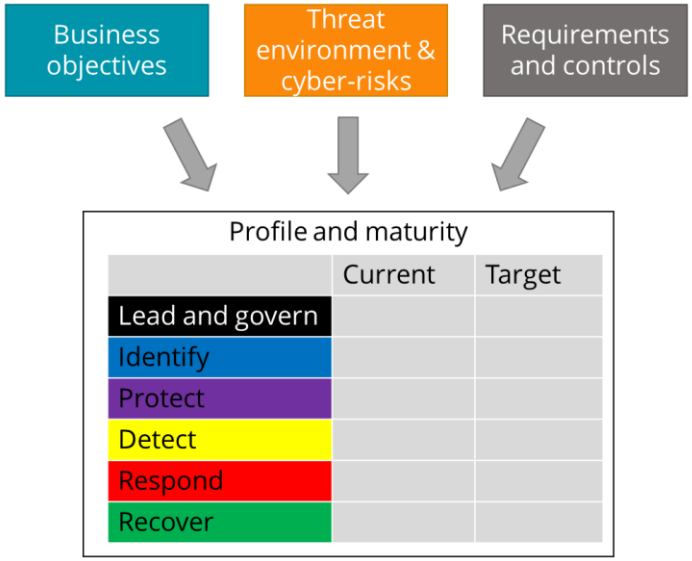
What is the output?

The following is an example of how the results can be presented to top management. Here there is an assessment of the ANSP and five of its suppliers. The suppliers have been ordered from most mature to least mature.

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
	Cyber Security Management System (CyberSecMS)	2	3	2	2	2	1
IDENTIFY	Asset Management	4	4	3	2	2	1
	Risk Assessment	1	3	3	1	2	1
	Information sharing	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
	Human-centred security	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

What should I do after using the model?

The model should give a broad assessment of strengths and weaknesses, and specifically where there are gaps between current and target maturity. Improvements can be identified and placed into a roadmap to increase maturity. NIST CSF guidance on establishing and improving a security programme can be used and adapted (as in the figure below) if required. Specific metrics may be needed to track improvements in particular capabilities.



Subcategory	Gaps	Priority	Budget	Year 1 improvements	Year 2 improvements
1	Small	Low	€		✓
2	Large	High	€€€	✓	✓
3	Medium	Moderate	€€	✓	
...					
N	None	Low	-		

What if I am already ISO27001 certified?	Congratulations. The maturity model is still intended to be helpful, even if your organisation's Information System Management System (ISMS) is fully compliant with ISO27001 requirements. If the operational environment (for an ANSP) or product development or service delivery function (for suppliers) is part of the Statement of Applicability, there should be a broad correlation between ISO27001 compliance and maturity. The maturity model is then an additional check on whether some key controls are appropriately strong and robust. Furthermore, note that whilst the term Cybersecurity Management System (CyberSecMS) is used here, it is effectively equivalent to an ISMS, and part of a broader Security Management System (SecMS).

High-level model

			Maturity levels				
Function	**Category**	**Description (from NIST)**	**Level 0 - Non-existent**	**Level 1 – Partial**	**Level 2 – Defined**	**Level 3 – Assured**	**Level 4 – Adaptive**
LEAD AND GOVERN	Leadership and governance	Top management demonstrate leadership and commitment to cybersecurity. The policies needed 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 established, together with parts of a strategy or plan; roles & responsibilities are established but no or weak link with top management	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
	Cybersecurity Management System (CyberSecMS)	The organisation has a set of interacting elements that establishes security policies and security objectives, and processes to achieve those objectives.	No documented CyberSecMS	Parts of a CyberSecMS documented, resourced and applied, but independently of other depts/systems	Fully operational CyberSecMS, that is externally audited CyberSecMS, and with links to other parts of the SecMS and the QMS and SMS	Certified CyberSecMS, with KPIs defined and tracked, and CyberSecMS/QMS/SMS processes are coordinated	Regular review against new good practices; KPIs show continual improvement; Certified Integrated Management System (IMS)
IDENTIFY	Asset Management	The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organisation's risk strategy.	No formal inventory of systems, their interdependencies and interfaces	Ad hoc, not formalised	All critical systems and interfaces are identified and described in a consistent way with clear owners	Interdependencies are well-understood and there is regular review and updates	Automated updates as the environment changes
	Risk Assessment	The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals,	No documented risk assessment processes or assessments	Ad hoc; no formalised assessment process	Management-approved processes that lead to cyber requirements being identified	Consistent, organisation-wide application with identified risk and requirement owners; external validation of risk levels by authorities; Security risk assessment is taken into account in	Continual review and linking of risks to latest vulnerabilities and threats; assurance that system-of-systems aspects are addressed

IDENTIFY		including system-of-system aspects resulting from dependencies.				safety risk assessment, and vice versa	
	Information sharing	The organisation obtains and shares threat intelligence, vulnerability and incident information activities, with internal and external parties	No, or very limited, cybersecurity information sharing	Using some threat intelligence and vulnerability information; Informal information sharing internally and externally where appropriate	Trends are identified; Internal and external sharing based on formal processes linked to risk assessment, vulnerability management, response and recovery processes; Relevant risk information is shared between safety and security functions	Threat intelligence and vulnerability information for all critical systems; Consistent, widespread and effective sharing	Information sharing is habitual and proactive; demonstrable leadership in improving industry-wide information sharing
	Supply Chain Risk Management	The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has in place the processes to identify, assess and manage supply chain risks. Appropriate levels of trust are established with data exchange partners.	No complete overview of all suppliers / partners	Some requirements placed on some suppliers and agreements with some partners; partial and informal understanding of supplier/partner cyber-maturity	Minimum set of requirements placed on all critical suppliers and agreements with partners, with mostly self-assessment for compliance	Requirements placed on suppliers with proportionate compliance checks and processes / penalties / measures for non-compliance	Independent reviews / audits / assessments supporting regular updates of requirements against new good practices
PROTECT	Identity Management and Access Control	Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access.	No access controls on critical systems or areas	Access controls on some critical systems and areas	Access controls on all systems and areas and linked to logs	Consistent controls within organisation-wide approach, including supply chain	Regular updates against new good practices
	Human-Centred Security	The organisation's personnel and partners are provided cybersecurity awareness education	No awareness/training programme	Ad hoc activities to inform and educate	Coherent programme in place that addresses whole organisation, including addressing human factors and	Sustained activities with follow-ups, differentiated for different roles, leading to increasing compliance and performance	State of the art syllabus, with systematic testing, leading to routine and proactive cyber-risk reporting from staff

PROTECT		and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Security is part of the organisation's culture.			organisational culture		
	Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Systems and processes are designed to be sensitive to the additional workload created by cybersecurity requirements.	Primary reliance on network boundary protection ('castle wall')	Some requirements for technical controls are defined upfront, supporting the 'security-by-design' principle; some non-essential services are disabled	Requirements for technical controls are defined and implemented; the principle of least functionality is also implemented (e.g. non-essential services are turned off) on all critical systems	Technical controls are demonstrated to be effective; Security architecture with virtual separation implemented and effective; Full control over technical infrastructure; Implementation designed with the human in mind, making it 'easy to do the right thing' and 'hard to do the wrong thing'	Security architecture can adapt dynamically to changing threat and risk landscape
DETECT	Anomalies and Events	Anomalous activity is detected in a timely manner and the potential impact of events is understood.	No documented procedures or controls	Ad hoc and typically manually	Suitably resourced controls are in place to detect anomalies and events; some detection is automatic; penetration testing flags missed positives	Procedures to reduce false positives; resourcing includes safeguards and/or emergency cover	State of the art detection capabilities are combined with additional mitigations when new threats are known not to be detectable
RESPOND	Response Planning	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	No plans exist to respond to security anomalies	Plans exist with high-level responsibilities	Well-defined responsibilities at all levels, 24/7/365 reaction times based on logic and agreements with suppliers / partners; violations of plans are addressed	Exercises and audits drive improvements in plans; resourcing includes safeguards and/or emergency cover; information sharing includes voluntary sharing with other parties	Response planning is widely coordinated, frequently exercised and updated, drawing on new good practices and knowledge
RESPOND	Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	Incidents cannot be contained or mitigated; there is no graceful degradation of services	Some incidents can be contained or mitigated without full loss of services; in some cases full loss of services cannot be avoided	Incidents can be contained and/or mitigated with minimal service loss; Sites have appropriate manual disaster recovery services	Sites have automated disaster recovery services with limited (or no) human intervention; data breaches and loss of data integrity have well-	Mitigations are monitored, regularly tested and adapted to ensure alignment with the operational environment; Automation

						rehearsed mitigations	exists to address incidents before they are apparent to humans; Self-healing exists
RECOVER	Recovery Planning	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	No recovery procedures established for cyber incidents	Procedures exist for some systems	Procedures exist for all critical systems, together with backups for systems and data to recover from outages	Regular testing of procedures, including communication with internal and external stakeholders	Lessons identified from exercises and incidents (both internal and external) drive updates in policy and procedures

Scoring form

Function	Category	Level score? (0-4)	Justification? Justify the score	Evidence? Provide evidence for the score	Additional probing questions aimed at ANSPs	Additional probing questions aimed at ATM suppliers
LEAD AND GOVERN	Leadership and governance				• Do you have an approved policy, strategy, plan and budget? • How is the whole organisation aligned with them? • Who is responsible for what? • How do you ensure that security is integrated into all operational processes?	• Do you have an approved policy, strategy, plan and budget for securing the product/service? • How is the whole organisation aligned with them? • Who is responsible for what? • How do you ensure that security is integrated into all processes that deliver the product/service?
	Cybersecurity Management System (CyberSecMS)				• What standards(s) do you use? • How is the CyberSecMS coordinated/integrated with the QMS/SMS? • How do you measure the effectiveness of the CyberSecMS?	• What standards(s) do you use? • If there is a supporting CyberSecMS, how is it coordinated/integrated with the QMS/SMS? • How do you measure the effectiveness of the CyberSecMS?
IDENTIFY	Asset Management				• How many critical systems / assets do you have? • How do you label physical and data assets? • What are their dependencies? • What is your patching policy? • How do you identify and trace vulnerabilities?	• How many critical systems / assets do you have for delivering the product/service? • How do you label physical and data assets? • What are their dependencies? • What is your patching policy? • How do you identify and trace vulnerabilities?
	Risk Assessment				• How do you identify and assess threats? • Is there a process that identifies, assigns and tracks cyber requirements? • How do you ensure that the process works? • What is your organisation's risk tolerance?	• How do you identify and assess threats? • Is there a process that identifies, assigns and tracks cyber requirements? • How do you ensure that the process works? • What is your risk tolerance your own organisation and your customers?
	Information sharing				• Who do you share risk information with?	• Who do you share risk information with?
	Supply Chain Risk Management				• How do you determine the level of trust you have with different suppliers / partners? • How do you ensure the right requirements are placed on suppliers? • How do you ensure the right supplier/partner behaviours?	• How do you determine the level of trust you have with different sub-contractors / partners in delivering the product/service? • How do you ensure the right requirements are placed on sub-contractors? • How do you ensure the right sub-contractors/partner behaviours?
PROTECT	Identity Management and Access Control				• How do you assign access rights?	• How do you assign access rights?

	Human-Centred Security				• How do you ensure that awareness leads to the right behaviours? • What indicators do you use to predict who will later be detected violating security policy?	• How do you ensure that awareness leads to the right behaviours? • What indicators do you use to predict who will later be detected violating security policy?
	Protective Technology				• Do you have a defined security architecture (for now or future)? • How does it support security by design? • How does it support data exchange and protection, and resilience? • How have you addressed the human factors in ensuring security controls are effective?	• Do you have a defined security architecture (for now or future)? • How does it support data exchange and protection, and resilience?
DETECT	Anomalies and Events				• How do you ensure that all cyber events / incidents can be detected?	• How do you ensure that all cyber events / incidents can be detected?
RESPOND	Response Planning				• How do you determine the required reaction times for services? • Do you consider cyber-attacks with subtle and believable data manipulation? • Do you have a Service Level Agreement (SLA), or similar requirements, between Ops and supporting departments (inc IT)? • How you ensure that enough resourcing is in place to respond to events/incidents?	• How do you determine the required reaction times for services? • Do you consider cyber-attacks with subtle and believable data manipulation? • Do you have a Service Level Agreement (SLA), or similar requirements, between the departments that deliver the product/service? • How you ensure that enough resourcing is in place to respond to events/incidents?
	Mitigation				• How do you respond to security events? • Who do you communicate with during an incident (internally and externally)? • How often are the lines of communication tested? • Are contacts named or are they roles and numbers that automatically change as people move roles in an organisation? • Are the means of contact (phones, email, etc) themselves resilient to an attack?	• How do you respond to security events? • Who do you communicate with during an incident (internally and externally)? • How often are the lines of communication tested? • Are contacts named or are they roles and numbers that automatically change as people move roles in an organisation? • Are the means of contact (phones, email, etc) themselves resilient to an attack?
RECOVER	Recovery Planning				• Do your operational contingency procedures include cyber incidents? • How do you return to normal operation?	• For services, do your contingency procedures include cyber incidents? • For services, how do you return to normal operation?

Detailed model

There will also be a more detailed maturity assessment, breaking down each of the high-level capabilities into more detailed areas. The extra detail would come from the NIST CSF, along with its references for further guidance. Such a detailed model is also best applied recursively – i.e. by department, function or system level before combining (by averaging maturity levels) for an overall result. This approach will require much more extensive liaison with stakeholders (e.g. relevant ANSP departments include Ops, IT, equipment, procurement, safety, quality, etc).

The excel version of the detailed questionnaire for Level 1 Maturity Model - has been appended to this report.

Function	Category	Level (0-4)	Level		Comments	Justification?	Evidence?	Description (mostly from NIST)	Level 0 - Non-existent	Level 1 – Partial	Level 2 – Defined	Level 3 – Assured	Level 4 – Adaptive
						Justify the score	Provide evidence for the score						
Lead and Govern	Leadership and governance	4	Adaptive	Updated regularly to reflect progress, threats and risks				Top management demonstrate leadership and commitment to cybersecurity. The policies needed 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 established, together with parts of a strategy or plan; roles & responsibilities are established but no or weak link with top management	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
	Cybersecurity Management System (CyberSecMS)	3	Assured	Certified CyberSecMS, with KPIs defined and tracked, and CyberSecMS/QMS/SMS processes are coordinated				The organisation has a set of interacting elements that establishes security policies and security objectives, and processes to achieve those objectives.	No documented CyberSecMS	Parts of a CyberSecMS documented, resourced and applied, but independently of other depts/systems	Fully operational CyberSecMS, that is externally audited CyberSecMS, and with links to other parts of the SecMS and the QMS and SMS	Certified CyberSecMS, with KPIs defined and tracked, and CyberSecMS/QMS/SMS processes are coordinated	Regular review against new good practices; KPIs show continual improvement; Certified Integrated Management System (IMS)
Identify	Asset Management	2	Defined	All critical systems and interfaces are identified and described in a consistent way with clear owners				The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organisation's risk strategy.	No formal inventory of systems, their interdependencies and interfaces	Ad hoc, not formalised	All critical systems and interfaces are identified and described in a consistent way with clear owners	Interdependencies are well-understood and there is regular review and updates	Automated updates as the environment changes
	Risk Assessment	1	Partial	Ad hoc, no formalised assessment process				The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals, including system-of-system aspects resulting from dependencies.	No documented risk assessment processes or assessments	Ad hoc, no formalised assessment process	Management-approved processes that lead to cyber requirements being identified	Consistent, organisation-wide application with identified risk and requirement owners; external validation of risk levels by authorities; Security risk assessment is taken into account in safety risk assessment, and vice versa	Continual review and linking of risks to latest vulnerabilities and threats; assurance that system-of-systems aspects are addressed
	Information sharing	0	Non-existent	No, or very limited, cybersecurity information sharing				The organisation obtains and shares threat intelligence, vulnerability and incident information activities, with internal and external parties	No, or very limited, cybersecurity information sharing	Using some threat intelligence and vulnerability information; Informal information sharing internally and externally where appropriate	Trends are identified; Internal and external sharing based on formal processes linked to risk assessment, vulnerability management, response and recovery processes; Relevant risk information is shared between safety and security functions	Threat intelligence and vulnerability information for all critical systems; Consistent, widespread and effective sharing	Information sharing is habitual and proactive; demonstrable leadership in improving industry-wide information sharing
	Supply Chain Risk Management	4	Adaptive	Independent reviews / audits / assessments supporting regular updates of requirements against new good practices				The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has in place the processes to identify, assess and manage supply chain risks. Appropriate levels of trust are established with data exchange partners.	No complete overview of all suppliers / partners	Some requirements placed on some suppliers and agreements with some partners; partial and informal understanding of supplier/partner cyber-maturity	Minimum set of requirements placed on all critical suppliers and agreements with partners, with mostly self-assessment for compliance	Requirements placed on suppliers with proportionate compliance checks and processes / penalties / measures for non-compliance	Independent reviews / audits / assessments supporting regular updates of requirements against new good practices
Protect	Identity Management and Access Control	3	Assured	Consistent controls within organisation-wide approach, including supply chain				Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access.	No access controls on critical systems or areas	Access controls on some critical systems and areas	Access controls on all systems and areas and linked to logs	Consistent controls within organisation-wide approach, including supply chain	Regular updates against new good practices
	Human-Centred Security	2	Defined	Coherent programme in place that addresses whole organisation, including addressing human factors and organisational culture				The organisation's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Security is part of the organisation's culture.	No awareness/training programme	Ad hoc activities to inform and educate	Coherent programme in place that addresses whole organisation, including addressing human factors and organisational culture	Sustained activities with follow-ups, differentiated for different roles, leading to increasing compliance and performance	State of the art syllabus, with systematic testing, leading to routine and proactive cyber-risk reporting from staff
	Protective Technology	1	Partial	Some requirements for technical controls are defined upfront, supporting the 'security-by-design' principle; some non-essential services are disabled				Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Systems and processes are designed to be sensitive to the additional workload created by cybersecurity requirements.	Primary reliance on network boundary protection ('castle wall')	Some requirements for technical controls are defined upfront, supporting the 'security-by-design' principle; some non-essential services are disabled	Requirements for technical controls are defined and implemented; the principle of least functionality is also implemented (e.g. non-essential services are turned off) on all critical systems	Technical controls are demonstrated to be effective; Security architecture with virtual separation implemented and effective; Full control over technical infrastructure; Implementation designed with the human in mind, making it 'easy to do the right thing' and 'hard to do the wrong thing'	Security architecture can adapt dynamically to changing threat and risk landscape

Detect	Anomalies and Events	0	Non-existent	No documented procedures or controls				Anomalous activity is detected in a timely manner and the potential impact of events is understood.	No documented procedures or controls	Ad hoc and typically manually	Suitably resourced controls are in place to detect anomalies and events; some detection is automatic; penetration testing flags missed positives	Procedures to reduce false positives; resourcing includes safeguards and/or emergency cover	State of the art detection capabilities are combined with additional mitigations when new threats are known not to be detectable
Respond	Response Planning	4	Adaptive	Response planning is widely coordinated, frequently exercised and updated, drawing on new good practices and knowledge				Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	No plans exist to respond to security anomalies	Plans exist with high-level responsibilities	Well-defined responsibilities at all levels, 24/7/365 reaction times based on logic and agreements with suppliers / partners; violations of plans are addressed	Exercises and audits drive improvements in plans; resourcing includes safeguards and/or emergency cover; information sharing includes voluntary sharing with other parties	Response planning is widely coordinated, frequently exercised and updated, drawing on new good practices and knowledge
	Mitigation	3	Assured	Sites have automated disaster recovery services with limited (or no) human intervention; data breaches and loss of data integrity have well-rehearsed mitigations				Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	Incidents cannot be contained or mitigated; there is no graceful degradation of services	Some incidents can be contained or mitigated without full loss of services; in some cases full loss of services cannot be avoided	Incidents can be contained and/or mitigated with minimal service loss; Sites have appropriate manual disaster recovery services	Sites have automated disaster recovery services with limited (or no) human intervention; data breaches and loss of data integrity have well-rehearsed mitigations	Mitigations are monitored, regularly tested and adapted to ensure alignment with the operational environment; Automation exists to address incidents before they are apparent to humans; Self-healing exists
Recovery	Recovery Planning	2	Defined	Procedures exist for all critical systems, together with backups for systems and data to recover from outages				Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	No recovery procedures established for cyber incidents	Procedures exist for some systems	Procedures exist for all critical systems, together with backups for systems and data to recover from outages	Regular testing of procedures, including communication with internal and external stakeholders	Lessons identified from exercises and incidents (both internal and external) drive updates in policy and procedures

0
1
2
3
4

Abbreviations

CSF	[NIST] Cyber Security Framework
CyberSecMS	Cybersecurity Management System
ISMS	Information System Management System
NM	Network Manager
QMS	Quality Management System
SecMS	Security Management System
SMS	Safety Management System

Acknowledgements

The following experts have participated and contributed in the development of ATM Cybersecurity Model – Level 1 - v 1.0

Prof Chris Johnson	Glasgow University
Matt Shreeve	Helios
Rolf Theisinger	DFS
Stephane Deharvengt	DSNA
Laurent Macquet	DSNA
Gerardo Sarmiento	ENAIRE
Francesco di Maio	ENAV
Maurizio Mancini	ENAV
Stephen Williams	NATS
Gregers Katsuhiro Inoue	NAVIAIR
Steen Halvorsen	NAVIAIR
Miriam Le Fevre	NAVIAIR/COOPANS
Antony Verheijen	LVNL
Wim Holthuis	LVNL
Francois Santy	THALES

Joris Lambrechts	EUROCONTROL NM
Sebastien Barbereau	EUROCONTROL NM
Bilgehan Turan	EUROCONTROL DECMA
Patrick Mana	EUROCONTROL DECMA
Frederic Lieutaud	EUROCONTROL NM
Tony Licu	EUROCONTROL NM

www.eurocontrol.int