Appendix I — Draft example of a maturity matrix for the ATM/ANS domain

Function	Category	Level (0-4)	Level		Comments	Justification of score	Evidence of score	Description (mostly from NIST)	Level 0 - Non-existent	Level 1 – Partial	Level 2 – Defined	Level 3 – Assured	Level 4 – Adaptive
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