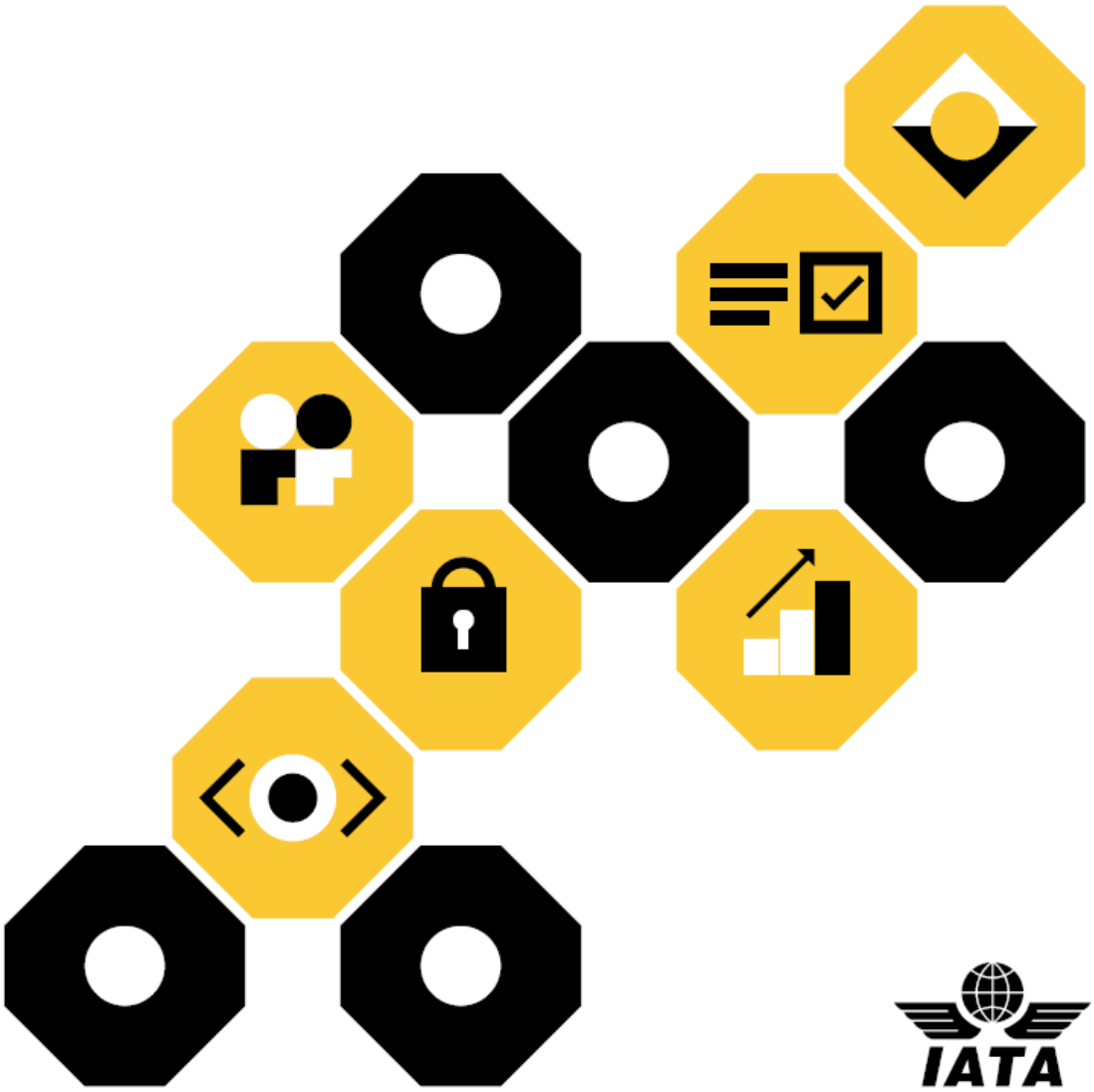
SECURITY MANAGEMENT SYSTEM TOOLKIT FOR EXTERNAL SERVICE PROVIDERS



IATA

This document allows organizations to monitor their progress towards IATA's SeMS (Security Management System) approach for External Service Providers (ESPs[1]). The toolkit may be utilized as part of a quality control activity intended to provide organizations a formal level of assurance as to their security arrangements. It is designed to be used for an appraisal across a range of areas of an organization and to help build on strengths as well as address opportunities to improve in line with the "SeMS for ESPs" framework.

The main objective of this tool is to help develop an understanding of the organization's progress in terms of IATA SeMS in a consistent, structured, and harmonized way rather than to deliver a specific 'score'.

Utilizing the attributes from the attachment, check if the organization can achieve a rating of at least level 1. If not, assign level 0 (Under development). If capable of reaching level 1, move to the level 2 and continue with the assessment. The grading system 0 – 4 or (*Under development*, *Present, Suitable, Operating, or Effective"* (UPSOE) shall be used as a development model, with the assessment confirming strengths and helping to identify improvement opportunities. The tool has been designed to capture key SeMS requirements and can be used to assess any type of aviation organization. It has been customized based on the EASA document "Management System Assessment Tool" Edition 2.0 (2023) for aligning Safety and Security methodologies (SMS and SeMS).

The below content guides the assessor through the list of attributes. Some items may not be relevant depending on the type or nature of the organisation. It is important that the assessor using the tool records evidence of the assessment. Evidence includes documentation, reports, records of interviews and discussions. For example, for an item to be "Present" the evidence is likely to be documented only, whereas for assessing whether it is "Operating" it may involve assessing records as well as face to face discussions.

The document uses four (4) maturity levels:

Present (1)	The organization has documented the relevant item within its Management System Documentation. However, it has not shown how well the documentation aligns with the organization's size, nature, complexity, and operations.
Suitable (2)	The relevant item is appropriately aligned with the organization's size, nature, complexity, and operations, as well as the inherent risks. However, the organization has not demonstrated how this item is utilized to generate specific outputs.
Operating (3)	Evidence indicates that the relevant item is actively utilized, resulting in the production of outputs. However, the organization has not shown how these outputs are effectively utilized for proactive security management actions.
Effective (4)	There is clear evidence that the relevant item is successfully achieving its intended outcome significantly contributing to overall security through proactive actions.

Maturity levels for each question should be entered as a corresponding numeric value into a Google Form facilitating the collection of data, and the creation and sharing of non-sensitive assessments among stakeholders. For more information, please contact aviationsecurity@iata.org and request access to SeMS Aviation Community. Potential assessors (internal or external) should use the SeMS Quiz for testing their SeMS competency and aim at more than 90% successful answers.

The reliability of any assessment or evaluation based on this tool's content is a matter for the independent judgement of users. The tool should not be used as a compliance checklist to verify that all the individual elements of a SeMS are in place. **"Being compliant" does not necessarily mean "being secure". Focussing on** each element of this tool and notably verifying each process 'step by step' or 'word by word' is too linear. This may mislead the assessor back to "compliance"; push the structure of the organisation to an inappropriate set-up or overly complicate SeMS. Finally, it may miss the ultimate objective which is to: evaluate how secure the operations are and ensure no major risk has been overlooked.

[1] *"ESP" (External Service Provider) would be when an Operator employs a third party (company or individual) outside the organization to perform security measures on a fee-for-service or to pay a third party to fulfill any part of your ISARP obligations under contract.*

CORE ASSESSMENT

Start the evaluation on level 1, moving to the level 2 once satisfied with the assessment of level 1 (same applies to subsequent levels).
If no sufficient evidence exists to establish at least level 1, mark level 0.

CORPORATE COMMITMENT AND GOVERNANCE (C1)

1. SECURITY COMMITMENT AND POLICY ALIGNMENT WITH SeMS PRINCIPLES

Overall objective: Evaluate SeMS governance in relation to Senior Management commitment reflected in the security policy and elements related to its implementation.

1.1 Security prioritization	There is an intent to define security as a priority, but no documentation exists to confirm is has been established.	Security established as a strategic and operational priority.	Security priority reflects the size, complexity, and nature of security operations of the organization.	The Security priority and its associated objectives are promoted at all organizational levels.	Employees across the organisation are familiar with the security priority.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
1.2 Security Policy	There is an intent to introduce security policy, but no documentation exists to confirm is has been established.	Security Policy set up and endorsed by Senior Management.	Security Policy includes commitment to compliance with security regulations and reflects the size, complexity, and nature of security operations of the organization.	The policy is reviewed periodically to ensure it remains relevant to the organization.	The organisation is proactively reviewing and taking action to address any identified and predicted shortfalls in security policy.
	Evaluation level				
	0 - Under development ☐	**1 - Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (1.1 and 1.2). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (1.1 and 1.2) and what could be done to make the organization adept for that level.*				

2. SECURITY ACCOUNTABILITIES AND RESPONSIBILITIES

Overall objective: Evaluate SeMS structure in relation to security accountabilities and responsibilities.

2.1 Accountability	There is an intent to assign security accountability, but no structure exists that would ensure it is implemented.	A Manager is appointed with the responsibility and overall accountability for security and SeMS.	The Manager with the responsibility and overall accountability for security and SeMS has control of resources and authority to take critical security decisions.	The Manager with the responsibility and overall accountability for security and SeMS ensures that the SeMS is properly resourced, implemented and maintained.	The Manager with the responsibility and overall accountability for security and SeMS ensures that the performance of the SeMS is monitored, reviewed, and improved.
	Evaluation level				
	0 - Under development ☐	**1 - Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
2.2 Responsibilities	There is an intent to assign security responsibilities, but no structure exists that would ensure it is implemented.	The security responsibilities are defined and documented for managerial and non-managerial roles within the organisation.	Security responsibilities of operational/business managers are reflected in job/job family descriptions, or organisational charts. Security responsibilities reflect the operational scope and complexity of the organization. Description of responsibilities also reflects areas of shared responsibilities or areas cross-cutting throughout the organization.	Processes and procedures exist where operational/business managers react to security issues and participate in security initiatives and activities. Reacting to security issues is based at least on outcomes of oversight based on 8.1 and Appendix 1.	Managers provide feedback and input on security processes and procedures, promote security principles, security awareness and security culture with their subordinated personnel.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (2.1 and 2.2). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (2.1 and 2.2) and what could be done to make the organization adept for that level.*				

3. SECURITY OBJECTIVES AND PERFORMANCE INDICATORS (SePI)

Overall objective: Evaluate SeMS in relation to security objectives and performance indicators.

3.1 Objectives	There is an intent to identify security objectives, but no documentation exists to evidence this.	Security objectives are defined and documented, with responsibilities for establishing them assigned.	Security objectives are relevant to the organisation and its activities. They are understandable and communicated.	Objectives are monitored by the right level of (senior) managers to determine what action need to be taken to ensure they are being met.	Security objectives reviewed to determine if they are relevant and aligned with other operational objectives. They are actively used in internal discussions about security processes and procedures by all managers with security responsibilities.
	Evaluation level				
	0 - Under development ☐	**1 - Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
3.2 Performance indicators	There is an intent to identify security performance indicators, but no documentation exists to evidence this.	The indicators to monitor and track performance are defined and documented with responsibilities for establishing them assigned. See Appendix 3	Security performance indicators reflect the size, complexity, and nature of security operations of the organization and enable actual collection of data and measurements.	Performance data are regularly published/ communicated/reviewed against criteria. Reactive and proactive analysis conducted to identify need to change measurements or target values.	Data exchange loop in place between Security Performance Indicators (SePI) monitoring data, quality control, security risk and other risk management processes (e.g., safety, operational).
	Evaluation level				
	0 - Under development ☐	**1 - Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (3.1 and 3.2). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (3.1 and 3.2) and what could be done to make the organization adept for that level.*				

4. SECURITY AWARENESS AND CULTURE

Overall objective: Evaluate overall security awareness and culture in relation to commitment to security by demonstrating responsibility for security outcomes and culture that encourages robust reporting without anxiety.

4.1 Security culture	There is an intent to establish security culture and bolster security awareness.	Security culture, alertness and awareness endorsed and established as organizational norms.	Security awareness is reflected in procedures relevant for the areas of operations. The security culture principles are understandable to all staff. Security culture is reinforced by the commitment of those with security responsibilities.	The Security Manager and senior management are promoting their commitment to security culture through active and visible participation in the SeMS. Evidence of security culture and its principles being applied and promoted to staff.	The security culture principles are reviewed on a regular basis and applied consistently. Evidence that acceptable/encouraged and unacceptable behaviours are determined and recognized. The organisational commitment to security addresses interactions with key stakeholders.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
4.2 Security reporting	There is an intent to implement security occurrences reporting.	Security reporting system established, and its principles are described in the organization's documentation. Responsibilities for rectifications are defined and assigned.	Security reporting system is accessible and designed in a way that is adequate for size, complexity, and operational profile of the organization. It is understandable for all personnel and used.	Relevant management levels engage in the rectification and prevention of re-occurrence of security issues identified through reporting. There are methods in place to record, categorize and analyse (root cause, trends) reports with rectifications.	Security reporting feeds information into risk assessment and quality control. Outputs of security reporting system used to showcase positive and negative security behaviours and outcomes.
	Evaluation level				
	0 - Under development ☐	**1 - Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (4.1 and 4.2). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (4.1 and 4.2) and what could be done to make the organization adept for that level.*				

RESOURCE MANAGEMENT (C2)

5. SECURITY TRAINING AND COMPETENCIES ASSESSMENT

Overall objective: Evaluate processes related to aviation security trainings and assessment of competencies/performance.

5.1 Security training	There is an intent to implement security training.	Initial and recurrent training (awareness and job-related, including SeMS training) provided to identified groups by competent (certified) instructors.	Training scope and materials comply with regulations and are adapted to audience. Responsibilities assigned to ensure personnel is trained as required.	Process to monitor compliance and relevance of training processes (training curriculum, frequency, updates, target groups) including vendors/subcontractors.	Communication loop with quality control and risk management to adjust training and target groups with needs anticipated and predicted (change management).
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
5.2 Competency assessments	There is an intent to implement security competency assessments	Competency assessment framework defined and documented. Defined personnel authorized and responsible for conducting assessments.	Processes in place for periodical assessment of competencies and covering groups adequate given size, complexity, and operational profile of the organization. Adequate resources are provided.	The competency assessment programme and processes are routinely reviewed and improved.	The competency assessment results are used to formulate remedial actions when necessary and feed into the training programme improvements.
	Evaluation level				
	0 - Under development ☐	**1 - Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (5.1 and 5.2). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (5.1 and 5.2) and what could be done to make the organization adept for that level.*				

THREAT ASSESSMENT AND RISK MANAGEMENT (C3)

6. SECURITY RISK ASSESSMENT

Overall objective: Evaluate processes of security risks identification, assessment, documentation and management (risk handling strategies).

6.1 Threats and vulnerabilities	There is an intent to implement processes to identify vulnerabilities and threats.	There is a process that defines how threats and vulnerabilities are identified through reactive and proactive methods, using multiples sources. The methodology to define the criteria for security investigations is documented.	Multiple sources of threats and vulnerabilities (internal and external) are considered and reviewed, as appropriate in the domain. The interfaces are properly addressed. Threats and vulnerabilities are documented in an easy-to-understand format. The security threats and vulnerabilities at organisation's level are consistent with the ones identified at authority's level, where relevant. The process includes the management of organisational change when it impacts security.	The threats and vulnerabilities are identified and documented. Technical, human, and organisational factors related are being considered. The criteria for security investigations are identified and applied. The level of sign-off for security investigations is defined and adequate to the level of risk. Security investigations are carried out and recorded.	The organisation has processes and means that capture threats and vulnerabilities which are maintained and reviewed to ensure they remain up to date. As appropriate, the organisation is continuously and proactively identifying threats and vulnerabilities related to its activities and operational environment and involves all key personnel and relevant stakeholders. Threats and vulnerabilities are assessed in a systematic and timely manner by qualified personnel. Threats and vulnerabilities cross-cutting throughout the organization are considered.
Evaluation level					
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**

6.2 Risk assessment	There is an intent to implement risk assessment processes.	There is a process that defines risk assessment methodology, which ensures realized risks are identified and treated.	Usable criteria are defined and fit the service provider's actual environment, including consideration to the expert judgement when data is not available. The used definitions are sufficiently explicit or detailed. For the acceptance of the risk's level, the right level of organisation's authority within the organisation (responsibilities) in cooperation with the stakeholders is clearly defined.	Evidence can be produced that the risk assessment is conducted. It includes maintaining the risk register, risk analysis, deciding on treatment, monitoring of residual risk. Risk assessments are carried out in a consistent manner based on the defined process. Appropriate measures are being applied to reduce the risk to an acceptable level including timelines and allocation of responsibilities.	The methodology Is subject to regular review. Risk assessments are reviewed to identify improvements in the processes. Risk assessments are regularly reviewed to ensure they remain current and consider emerging threats. Risk tolerance criteria are used routinely, consistently applied in management decision making processes, and are regularly reviewed. Treatments are practical and sustainable, applied in a timely manner and do not create additional risks. The effectiveness of the treatments is monitored using occurrence reporting and quality management.
Evaluation level					
	0 - Under development ☐	**1 - Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**

6.3 Risk management	There is an intent to implement processes of risk management.	Risk handling and treatment strategies are defined and processes to decide and apply treatments are in place. Process is evidenced by the risk register.	Process is understandable and includes all relevant internal stakeholders as adequate given the size, complexity, and profile of the organization. Responsibilities are assigned at every step of the process and include defining timelines for implementation of treatments. Responsibilities are assigned for monitoring the implementation. Resources provided to maintain the register and conduct data analysis.	Appropriate treatments are being applied to reduce security risks to an acceptable level, including timelines and allocation of responsibilities agreed with the stakeholders. Operational, technical, human, and organisational factors are considered as part of the development of treatments. Senior management is actively involved in risk monitoring.	The organisation is reviewing the process and taking action to address any changes in structure and assignment of responsibilities to mitigate gaps or overlaps in the ownership. Needs are anticipated and predicted (change management). Where the data indicates concerning trends or negative impact on risks in other areas, appropriate action is taken.
Evaluation level					
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (6.1, 6.2 and 6.3). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (6.1, 6.2 and 6.3) and what could be done to make the organization adept for that level.*				

QUALITY CONTROL AND ASSURANCE (C5)

7. SECURITY QUALITY CONTROL AND ASSURANCE

Overall objective: Evaluate processes related to quality control and quality assurance.

7.1 Quality control and assurance processes	There is an intent to implement quality control processes.	Quality Control and Assurance procedures defined, agreed, and conducted.	The quality control and assurance cover all applicable regulations and standards. It adequately covers areas of operations and regulatory requirements.	Schedule of quality control is based on risk assessment. Harmonized quality control methodology implemented across all quality control activities and includes the variety of quality control methods (inspections, audits, tests, self-assessments). Training/instructions/mentoring is provided to maintain consistency of methodology.	The organization regularly reviews quality control and assurance program to identify need for change and to ensure it remains effective. The organization regularly reviews documentation and recording processes and procedures to identify need for change and to ensure it remains effective.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
7.2 Competencies and documentation	There is an intent to define quality control competencies and documentation requirements.	The organization's documentation establishes procedures including scheduling and recording of activities. Documentation describes competencies required for persons conducting activities.	Documentation processes are easy to use and understandable. Provided resources to conduct quality assurance and quality control activities are adequate given size, complexity, and scope of operations.	Processes and procedures are consistently executed and followed. Training/instructions/mentoring is provided to maintain consistency of competencies, documentation, and record-keeping practices.	The organization regularly reviews competencies, documentation and recording processes and procedures to identify need for change and to ensure it remains effective.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (7.1 and 7.2). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (7.1 and 7.2) and what could be done to make the organization adept for that level.*				

8. IDENTIFICATION AND CORRECTION OF DEFICIENCIES

Overall objective: Evaluate processes related to identification of deficiencies and rectification.

8.1 Identification and correction of deficiencies	There is an intent to implement identification and correction of deficiencies.	The organization has documented process for classification of identified deficiencies and correction thereof (corrective action plan) This includes assigning responsibilities for corrective action.	The process of classification is understandable and consistently applied and based on Appendix 1. Timelines for determining, accepting, and implementation of corrective actions are suitable for the type of operations.	The identification of deficiencies and correction is carried out in accordance with the procedures including causal analysis to address root causes. Evidence exist, deficiencies are corrected in line with processes and procedures (including established timelines).	The organisation regularly reviews the status of corrective actions, as well as its effectiveness. Resolution of deficiencies constitutes part of performance measurements.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
8.2 Continuous improvement process	There is an intent to establish continuous improvement processes.	There is a process for how audit results are communicated to the accountable managers and senior management. The organization has documented process of tracking improvements and following up on unresolved deficiencies.	Quality control (QC) and assurance is producing data that are regularly reviewed and communicated. Triggers for follow-up and escalation are defined and understandable. Responsibilities at managerial level are clear and understood.	Actions are taken by business/operations. Decision making is based on data provided by the QC results. Managers are engaged and play an active role in corrective actions of security issues in operational areas they are responsible for. Organization engages management and leadership in discussions regarding deficiencies that re-occur or where corrective actions have not been successful.	The interface between compliance monitoring and the security risk management processes is described. Significant findings are used in internal security training and security promotion sessions. The audit results and root causes, causal and contributing factors are analysed and considered when reviewing internal policies and procedures.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (8.1 and 8.2). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (8.1 and 8.2) and what could be done to make the organization adept for that level.*				

EXTENDED ASSESSMENT

Start the evaluation on level 1, moving to the level 2 once satisfied with the assessment of level 1 (same applies to subsequent levels).
If no sufficient evidence exist to establish at least level 1, mark level 0.

RESOURCE MANAGEMENT (C2)

9. SECURITY PROFESSIONAL CRITERIA

Overall objective: Evaluate processes related to implementation of aviation security criteria at the recruitment stage and during the period of employment for key security positions.

9.1 Personnel security criteria	There is an intent to establish professional security criteria for key security positions.	The organization has documented process for Identification of key security positions relevant for operations and management.	Processes in place to use security criteria for prospective candidates to ensure they are qualified and experienced, commensurate to description and requirements for key security positions. These criteria relevant for key security positions included in job descriptions.	Process to ensure security criteria are retained/maintained by personnel holding key security positions. People holding these positions are assessed against specific security criteria.	The organisation regularly reviews its processes to assess applicability and need for change to criteria conducted. Feedback from business/operational managers about security criteria is considered.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for the attribute (9.1). *Briefly describe where the organization couldn't demonstrate evaluation level for the attribute (9.1) and what could be done to make the organization adept for that level.*				

QUALITY CONTROL AND ASSURANCE (C5)

10. SECURITY CRITERIA FOR OUTSOURCED SERVICES AND PRODUCTS

Overall objective: Evaluate incorporating of security criteria in subcontracting services or purchase of products used in the implementation of security measures.

10.1 Security criteria for services and products	There is an intent to establish security criteria for outsourced services and products.	The organization has documented process for subcontracting security services and acquiring products which includes identification of security criteria.	Criteria are understandable. These criteria are clearly communicated.	Process in place to use security criteria in procurement processes for services and products.	There is a review process for these criteria based on performance monitoring, quality control. New products or changes to services are proactively approached (change management). Feedback on products' suitability is analysed and new solutions considered.
Evaluation level					
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**

10.2 Monitoring of external service providers and products	There is an intent to introduce monitoring for performance of subcontractors and verify security products.	The organization has documented processes for monitoring subcontracted security services and verification of acquired products against established criteria.	Criteria for monitoring and tracking performance are understandable and based on Appendix 1. Responsibilities for monitoring and verification are assigned and adequate for the organization's size, complexity, and nature of operations. Quality control and assurance is included in monitoring and verification process.	Monitoring and verification activities are actually conducted. Data is collected and analysed.	Collected data is used for performance analysis of subcontractors. Communication channels with vendors are created and feedback is provided. Risk assessment receives feeds about providers' performance and usability of products. The qualitative and quantitative means are reviewed; regularly updated to ensure they remain relevant, then reviewed with the relevant SeMS governance body and allow the maturation of the organisation's SeMS.
Evaluation level					
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for each of attributes (10.1 and 10.2). *Briefly describe where the organization couldn't demonstrate evaluation level for each of attributes (10.1 and 10.2) and what could be done to make the organization adept for that level.*				

SECURITY DOCUMENTATION (C6 - AVIATION SECURITY PROGRAM)

11. CONSISTENCY OF SECURITY DOCUMENTATION

Overall objective: Evaluate security documentation and how it reflects security regulations and standards.

11.1 Security documentation	There is an intent to establish and maintain security documentation.	Organization has process in place to develop and distribute security documentation based on identified applicable security regulations and standards Responsibility is assigned for tracking and communicating updates internally and externally.	Process of maintaining documentation based on identification of applicable regulations is adequate to organization's scope of operations and considers applicability of multiple National Civil Aviation Security Programs and a range of standards expected by various customers.	Documents guide the operation to meet the intent of the regulation. Frontline and/or corporate feedback regarding documentation of guidance is reviewed by the organisation. Documentation is readily available to all relevant personnel. Personnel follow the documentation relevant to their activities.	The organisation is reviewing and adhering to regulatory requirements, making changes as necessary based on changes to the regulation or feedback from within the organisation.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for the attribute (11.1). *Briefly describe where the organization couldn't demonstrate evaluation level for the attribute (11.1) and what could be done to make the organization adept for that level.*				

THREAT ASSESSMENT AND RISK MANAGEMENT (C3)

12. SECURITY INFORMATION ANALYSIS

Objective: Evaluate processes related to collection of aviation security information, including threat information and operational security reporting.

12.1 Aviation security information	There is an intent to establish collection and analysis of security information.	The process of security information collection, communication and protection is documented.	Process is understandable and responsibilities for collection, and analysis of security information is assigned. The process determines what, when, and how security information needs to be collected, communicated, and protected. The means of communication are adapted to: - the size and complexity of the organisation - the audience and - the significance of what is being communicated.	Security critical information is being identified and communicated throughout the organisation, including contracted organisations where appropriate. "The need to know" principles are implemented. Training and instructions are provided and adapted to the audience. Collection, communication, and protection measures are subject to quality control.	Methods of collection, communication and protection of security information are reviewed regularly seeking for continuous improvement. Security communication is assessed to determine how it is being used and understood, and to improve it where appropriate. Decision making, actions, and communication reflect a positive security culture and security leadership demonstrating commitment to the security policy. Training and instructions are updated accordingly.
Evaluation level					
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for the attribute (12.1). *Briefly describe where the organization couldn't demonstrate evaluation level for the attribute (12.1) and what could be done to make the organization adept for that level.*				

MANAGEMENT OF EMERGENCIES AND INCIDENTS (C4)

13. SECURITY EMERGENCY MANAGEMENT

Objective: Evaluate processes of security emergency and incidents management.

13.1 Emergency management	There is an intent to establish security emergency management.	An Emergency Response Plan (ERP) is developed and distributed. It defines procedures, roles, responsibilities and actions of the various organisations and key personnel. Incident reporting system is defined and established.	Key personnel have easy access to the relevant parts of the ERP at all times. ERP involves all relevant personnel and actors. The coordination with other organisations (including non-aviation organisations) is defined with appropriate means. Communication and reporting tools are available to all personnel.	The ERP can be quickly activated. It is reviewed and tested regularly to make sure it remains up to date. Different scenarios with variations test the robustness of the ERP. Actions are taken to improve the ERP effectiveness. Training programme and tools is defined to respond to various types of security incidents, including new threats.	Process is in place to analyse and review lessons learned from the emergency response drills and exercises with feedback/input of participants considered.
	Evaluation level				
	0 - Under development ☐	**1 – Present ☐**	**2 - Suitable ☐**	**3 - Operating ☐**	**4 - Effective ☐**
	Evidence / rational for rating				
	Briefly describe where the organization demonstrated evaluation level for the attribute (13.1). *Briefly describe where the organization couldn't demonstrate evaluation level for the attribute (13.1) and what could be done to make the organization adept for that level.*				

Appendix 1 – OPERATIONAL SECURITY IMPLEMENTATION VERIFICATION CHECKLIST

Operational Security Process	ISM *) reference	Conformity with SOPs **) applicable at the station level				Comments and Description of Findings
		Yes	No	NA ***)	NC ****)	
1. Check in and boarding	*GRH 2.2.4*					
2. Access control to airside and security restricted areas	*SEC 3.1.3*					
3. Access control within the security restricted area	*SEC 3.1.2*					
4. Personnel and crew access control and screening	*SEC 3.1.3*					
5. Carriage of weapons (firearms)	*GRH 3.7.5, SEC 3.3.1, SEC 3.3.3*					
6. Passenger and Cabin Baggage	*SEC 3.4.1, SEC 3.4.7*					
7. Transfer passengers' screening	*SEC 3.4.3*					
8. Additional passengers' screening	*SEC 3.4.4*					
9. Protection of passengers	*SEC 3.4.5*					
10. Behaviour detection	*SEC 3.4.6*					
11. Special Category Passengers	*GRH 3.7.6, SEC 3.5.1*					
12. Hold Baggage Authorization	*GRH 3.7.8, SEC 3.6.6*					
13. Hold Baggage Screening	*GRH 3.7.10, GRH 3.7.11, SEC 3.6.1, SEC 3.6.2*					
14. Hold Baggage Protection	*GRH 3.7.7, GRH 3.7.9, SEC 3.6.1, SEC 3.6.2*					
15. Aircraft Protection	*GRH 3.7.1*					
16. Aircraft Search	*GRH 3.7.2*					
17. Transit stop aircraft procedures	*GRH 3.7.3*					
18. Mishandled baggage protection	*GRH 3.7.9*					
19. Cargo security procedures	*GRH 3.7.4, CGO 3.7.4 SEC 3.7.1*					
20. Security of cargo facilities	*CGO 3.7.1*					
21. Security controls of persons and vehicles (cargo)	*CGO 3.7.2*					
22. Cargo protection	*CGO 3.7.6*					
23. Transfer cargo	*CGO 3.7.7*					
24. In-flight, catering, co-mail, co-mat, and other supplies	*SEC 3.8.1*					
25. Other supplies' protections	*SEC 3.9.1*					
26. Cybersecurity	*ORG 3.6.1, SEC 4.1.1*					

*) ISM Edition 18 (January 2026)
**) Standardized Operating Procedures – part of Aircraft Operator Security Program (AOSP), Supplementary Station Procedures (SSPs) and Standard Ground Handling Agreement (IATA Airport Handling Manual 810)
***) Not Applicable
****) Not Confirmed

Appendix 2 – Operational Risk Assessment Checklist for Unaccompanied Baggage

As explained in the IATA position paper on Hold Baggage Reconciliation (2025) aligned with the new ICAO guidance material for Hold Baggage Screening, Handling and Processing (Doc 8973, June 2025), **new options for security controls now include the possibility of not offloading baggage that becomes unaccompanied if it has been screened to a defined high standard before it became unaccompanied, for example using the most advanced and effective screening methodology**.

As **all decisions** related to the security controls applied to unaccompanied baggage **should be based on an operational risk assessment conducted by the aircraft operator**, The following **Unaccompanied HB Operational Risk Assessment Checklist (2025)** can be adapted into Standard Operating Procedures followed by External Service Providers (ESPs).

If any yellow or orange box (#1 to #11) is selected, the unaccompanied baggage should be rescreened.

If all boxes from #1 to #11 are green, but the last #12 is yellow or orange, the ESPs should contact the appropriate Operators for a final decision.

Example of Unaccompanied HB Operational Risk Assessment Checklist (2025):

#	Risk-based security questions	Evaluation			Details
1	Has the hold baggage been accepted from passengers who have checked in for a flight, or from crew members on duty?	Yes ☐	UNK ☐	No ☐	
2	Has the hold baggage been accepted by a responsible agent or an authorized representative of the aircraft operator or accepted at an automated self-service baggage drop station, or accepted as UNAR, in compliance with national security requirements?	Yes ☐	UNK ☐	No ☐	
3	Has the hold baggage (including baggage accepted at off-airport locations) been screened at its point of origin using security systems and appropriate standards of screening as defined by the authorities?	Yes ☐	UNK ☐	No ☐	
4	Has the hold baggage been protected from unauthorized interference from the point of screening or acceptance by the airline or authorized representative until the departure of the aircraft from security-restricted areas?	Yes ☐	UNK ☐	No ☐	
5	Has the integrity of the baggage protection been maintained and not compromised during handling or transfer?	Yes ☐	UNK ☐	No ☐	
6	If the integrity of the protection has been jeopardized, has the hold baggage been rescreened to the appropriate standard?	Yes ☐	N/A ☐	No ☐	
7	Has the hold baggage been misdirected, failed to transfer or loaded onto an aircraft other than that for which it was checked in?	Yes ☐	UNK ☐	No ☐	
8	Has the aircraft operator decided not to load, or unload the hold baggage for operational reasons, and the passenger had not influenced the decision by changing their travel itinerary?	Yes ☐	UNK ☐	No ☐	
9	Has the owner of the hold baggage failed to board the aircraft due to unforeseen circumstances (e.g., short transfer or connection time)?	Yes ☐	UNK ☐	No ☐	
10	Has the owner of the hold baggage been denied boarding for safety or security reasons?	No ☐	UNK ☐	Yes ☐	
11	Has the owner of the hold baggage voluntarily given up their seat?	No ☐	UNK ☐	Yes ☐	
12	Is the State allowing newly unaccompanied hold baggage, already screened to a defined high standard before it became unaccompanied, to be accepted by aircraft operators?	Yes ☐	UNK ☐	No ☐	
	Decision of acceptance for the newly unaccompanied hold baggage, appropriately re-identified, without offloading, nor additional screening measures applied.	YES ☐		NO ☐	

UKN = Unknown – N/A = Not Applicable

Appendix 3 – SECURITY PERFORMANCE INDICATORS (SePIs)

The IATA Security Management System (SeMS) Manual highlights the importance of measuring system performance to ensure its continued relevance. These measurements serve a strategic corporate function by supporting management reviews of the SeMS. In this context, the evaluation of Security Performance Indicators (SePIs) is addressed within the SeMS for ESP Toolkit (see page 4 of this document).

To support ESPs in developing their SeMS, IATA held a SeMS Workshop in 2024 and compiled a list of SePIs, provided below:

SePI Characteristics				
Security Performance Indicator (SePI) name	**Objective**	**Measurement**	**Target**	**Function (Leading / Lagging)**
Security reporting (I)	Enhance awareness of the security posture through timely and complete internal security reporting	Numeric value calculated as the number of findings reported through the internal reporting system prior to or within the specified timeframe relative to authority oversight findings	All security findings identified during authority oversight are already captured through the internal reporting system, thereby eliminating unreported security events ("no surprises").	LE
Security reporting (II)	Strengthen the ability to respond to security issues by enhancing personnel competence in completing security reports	[xx]% year-over-year increase in the proportion of security reports assessed as "adequate" based on predefined quality criteria (e.g., completeness, clarity, relevance, need for clarification)	Progressively increasing percentage of adequately completed reports (target set by each entity).	LE
Security reporting (III)	Enable trend analysis and appropriate action by conducting a prima facie review of all reported occurrences.	[xx]% year-over-year increase of reports with documented prima facie assessment completed within the defined timeframe.	100% of reports assessed and classified (investigation/statistical) within a set timeframe (e.g., 5 days).	LE
Quality Management (I)	Ensuring compliance through findings closed in the defined timeframe, including implementation of appropriate corrective action	[xx]% year-over-year increase of findings closed within specified timeframe (established by the entity and based on risk-ratings and severity)	[xx] days for the finding closure (to be established by the entity and depending on the type of the finding).	LA
Quality Management (II)	Being able to identify and mitigate	[xx]% year-over-year decrease of findings	[xx] % of findings attributable to prioritized root cause(s), or	LE

	prevalent systemic issues (related Root Causes) to prioritize quality control and assurance	attributable to prioritized root cause(s)	[xx]% of findings attributable to specific types of root cause(s) e.g.: [xx]% documentation/procedure related; [xx]% supervision/oversight related; [xx]% awareness related	
Quality Management (III)	Risk based prioritization of findings' resolution Use of Quality Control and Assurance to allow prioritization of the resolution of findings based on assigned criticality of risk	[xx]% year-over-year increase of findings assessed and assigned risk rating	100% findings are assessed and prioritized based on their risk level	LA
Quality Management (IV)	Ensure required services are delivered as per agreed standard	[xx]% year-over-year decrease of supervision/ oversight root cause of findings and security occurrences	[xx]% of findings attributable to supervision/ oversight deficiencies as a primary/ root cause (target set by each entity)	LA
Documentation (I)	Ensuring consistency and adequacy of security documentation	[xx]% year-over-year increase of quality management results (in the scope of documentation assessments)	Entire documentation compliant, standardized, complete and updated within a defined timeframe (target set by each entity).	LA
Documentation (II)	Ensuring documentation reflects security requirements	[xx]% year-over-year decrease of documentation/procedure root cause of findings and security occurrences	[xx]% of findings attributable to documentation/ procedure deficiencies as a primary/ root cause (target set by each entity)	LA
Confidence in Management System (I)	Ensuring security measurement (SePI) is adequate	[xx]% year-over-year increase of management confidence that SePIs are relevant, actionable, and reflective of security policy and objectives established at least once a year during the review and revision of SePIs	Confidence score target set by each entity	LE

Appendix 4 – SeMS-related Guidance, Training and Certification Tools

Since the inception of the Security Management System (SeMS) concept in the IATA Operational Safety Audit (IOSA) Standards Manual (ISM), its mandatory implementation for all IOSA registered airlines since 2007, and the planned extension to all External Service Providers (ESPs), as a Recommended Practice, to in 2025, numerous organizations and associations have already developed several training programs and guidance material related to the Management of Security that are accessible to all ESPs.

In 2004, the International Civil Aviation Organization (ICAO), in collaboration with the John Molson School of Business at Concordia University, Montreal, Canada, launched the innovative Aviation Security Professional Management Course (AVSEC PMC). This course remains a global benchmark, with over 1,100 alumni from all ICAO regions and origins. Many of whom now hold key positions in aviation security.

ICAO introduced its first SeMS guidance material back in 2010, as part of the 7th Edition of its *Aviation Security* Manual (Doc 8973, Restricted). The current edition dedicates a full chapter (Doc 8973, Chapter 9.3) to SeMS. Additionally, ICAO actively promotes Security Culture through a variety of initiatives from States and Organizations accessible via their public website: Security Culture. A strong Security Culture and Corporate Security Policy are essential pillars of an effective SeMS.

ICAO also shares public guidance material on Incident Reporting, AOSP and SSP and other security-related topics that should be of great interest for all SeMS entities.

Together with the Airport Council International (ACI), ICAO developed a 5-day course on Management of Airport Security available both in-person and virtually. ICAO also offers a two-year Master of Science (MSc) in Aviation Security program with Buckinghamshire New University, UK.

IATA's training catalogue for aviation security is extensive and flexible, featuring advanced courses in Aviation Security Management including a 5-day SeMS course offered globally.

A visit to IATA SeMS public webpage provides insight into the wide range of SeMS-related tools currently available ranging from (free-of-charge) Security Awareness and Incident Reporting videos developed in 13 languages as per of the **See it Report it** initiative, to (free-of-charge) SeMS-Quiz and (at a fee) SeMS Competency Test for evaluating SeMS understanding, and annual SeMS Workshops (by invitation),

Since 2017, IATA has maintained up-to-date a dedicated SeMS Manual, which is an essential resource for all security managers navigating SeMS concepts. In 2024, ACI developed the 1st Edition of ACI Security Management System (SeMS) Handbook for promoting a "proactive holistic airport security".

Moreover, following the first SeMS Workshop organized in Madrid in November 2022 and the creation of the SeMS Aviation Community, IATA developed, with the SeMS Aviation Community and for the Community, the freely available SeMS Toolkit for ESPs. This toolkit provides all ESPs and entities of the aviation ecosystem with a straightforward self-assessment method for measuring SeMS maturity of any entities scaling from very small to large ones. Those interested in joining the SeMS Aviation Community and in accessing all tools freely available, can contact aviationsecurity@iata.org. All security professionals can join the SeMS Aviation Community and should promote its existence.

Lastly, IATA has developed a new SeMS certification program offering a structured framework for proactively managing regulatory compliance, security risks, threats, and vulnerabilities. This program facilitates a transition from reactive to proactive security measures, with a focus on risk-based and data-driven strategies. The SeMS certification program is the most advanced SeMS related tool currently available for all entities looking to demonstrate the strength of their SeMS and gain independent, and credible international recognition.