EATM

EUROPEAN AIR TRAFFIC MANAGEMENT

SECURITY

Security Management Handbook

A Framework

EUROCONTROL

Edition 1.0
Edition date: May 2008
Released Issue

EUROCONTROL

EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

EUROCONTROL
Security Management Handbook

- A Framework -

Edition Number	:	1.0
Edition Date	:	May 2008
Status	:	Released Issue
Intended for	:	Restricted Audience

DOCUMENT CHARACTERISTICS

TITLE

EUROCONTROL Security Management Handbook

	Publication Reference:	
	ISBN Number	
Document Identifier	**Edition Number:**	1.0
DAP/SSH/077	**Edition Date:**	May 2008

Abstract

The Security Management Handbook establishes a best practice framework for the implementation of a Security Management System (SecMS).

The framework contains the description of 5 key activities and their 18 elements, which establish the Security Management System. It provides guidance on how to address EC Regulation No. 2096/2005, the Common Requirements, covering security requirements for air navigation service providers.

Keywords

ATM	Security Assurance	Security Plan	Handbook
EC No. 2096/2005	Security Risk Analysis	Security Policy	Best Practice
SecMS	Security Management	Security Promotion	

Authors

EUROCONTROL ATM Security Domain

Contact Person(s)	Tel	Unit
Dr. Bernd TIEMEYER	95038	DAP/SSH

STATUS, AUDIENCE AND ACCESSIBILITY

Status		Intended for		Accessible via	
Working Draft	☐	General Public	☐	Intranet	☐
Draft	☐	EATM Stakeholders	☐	Extranet	☐
Proposed Issue	☐	Restricted Audience	☑	Internet (www.eurocontrol.int)	☐
Released Issue	☑				

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
ATM Security Domain Manager	(Dr. Bernd Tiemeyer)	19.05.2008
Head of DAP/SSH	(Alexander Skoniezki)	19.5.2008
Director DAP	(Guido Kerkhofs)	19.5.2008

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
0.1	03.08.2006	Initial draft for review by ATM Security Domain	All
0.2	25.08.2006	Draft for review by ATM Security Domain	All
0.3	29.09.2006	Draft for review by stakeholders	All
0.4	08.01.2008	Incorporate comments from the SecMS Ad-hoc group	All
0.5	09.04.2008	Incorporate comments from SET/1. Updated to 'proposed issue'	All
1.0	19.05.2008	Released Issue	All

PAGE INTENTIONALLY LEFT BLANK

CONTENTS

PAGE INTENTIONALLY LEFT BLANK

DISCLAIMER

The 'EUROCONTROL Security Management Handbook - A Framework ' is **non-mandatory material**, that is general and procedural information to support effective and harmonised development of Security Management Systems by States and/or their concerned ANSPs. States and/or ANSPs may choose to implement Security Management solutions different to those presented in the Handbook.

The information assembled in this document reflects the legislation in force on the date of publication of EC Regulation No 2096/2005 in the official Journal of the European Union and of Annex 17 (8th Edition) to the Convention on International Civil Aviation.

The compliance of the Member States, and their ANSPS, with their obligations under international law, the Single European Sky (SES) regulations and national legislation remains entirely their own responsibility. EUROCONTROL does not guarantee a particular outcome of an oversight exercise by a NSA on the compliance of the Security Management System developed by the State and/or their ANSP nor does EUROCONTROL assume any liability for claims or damages sustained as a result of the implementation of the Handbook.

Note: It is expected that this Handbook will be updated on an annual basis, based on the development of further material (e.g. the relationship between security, safety and other business processes).

PAGE INTENTIONALLY LEFT BLANK

PART 1 – SECMS FRAMEWORK

1.1 Overview

ATM Security is a growing concern for all those involved in aviation, including air navigation service providers. A formal approach to ATM security has, therefore, become a legal obligation under the European Common Requirements for the Provision of Air Navigation Services (Commission Regulation EC 2096/2005). Details of this regulation can be found in Annex A.

What is Security?

Whilst there is no single or universal definition of security, it is generally agreed that it relates to the protection of assets ("things of value") from unlawful damage or use. It relates to the protection of assets in terms of:

- Confidentiality (limiting knowledge to those that need to know);
- Integrity (ensuring that an asset remains in the form intended);
- Availability (being available when required).

Definition of ATM Security

ATM security[1] is concerned with those threats that are aimed at the ATM System directly, such as attacks on ATM assets, or where ATM plays a key role in the prevention or response to threats aimed at other parts of the aviation system (or national and international assets of high value) and limiting their effects on the overall ATM Network. ATM Security is a subset of Aviation Security which is itself a component of Transport Security

ATM Security Purpose

The purpose of ATM Security is to:

- Protect the assets from:
  - Service degradation;
  - Physical attack (eg terrorist/criminals);
  - Insider ill-doing;
  - Cyber attack on information or data processing (eg by a hacker or computer malware);
  - Electromagnetic attack (eg causing interference with communications, navigation and surveillance equipment);
- Provide collaborative support to the security of the Airspace and "Air Policing" (ATC assistance to airlines, military and law enforcement in responding to renegade aircraft and disruptive passengers on board);

[1] SET/1 agreed to adopt the common understanding on ATM Security derived at the ATM Security Workshop, Dec 2006 and subsequently endorsed by SCG/6.

[3] Derived from ISO 17799, 2700, ISO/IEC 13335-1:2004 and BS EN ISO 9000:2005

- Respond effectively to security incidents affecting the ATM infrastructure or airspace;

- Plan for Service/Business Continuity and Recovery.

ATM Security should be analysed in terms of the key elements of the ATM system:

- People;
- Procedures - the operational, maintenance and administrative practises that people follow;.
- Technical equipment for Communications, Navigation and Surveillance, the technical operational systems upon which the ATM system depends;
- Buildings - includes the physical infrastructure and supporting facilities like power, water, food etc.;
- Information and Information systems, both operational and administrative.

The Value of Security to ATM

In order to be of value to the ATM System security must support the ATM services and business needs and when applied effectively it:

- Supports Service and Business Risk Management;
- Assures employees;
- Assures customers;
- Builds Confidence;
- Protects & enhances reputation and share value;
- Meets legislative requirements (e.g. Data Protection Act);
- Meets Regulatory requirements (e.g. SES Common Requirements);
- Makes sound Business Best Practice;
- Influences Insurance Premiums;
- Provides Marketing leverage;
- Keeps people and assets safe;
- Contributes to safeguarding the Critical National Infrastructure;
- Plays a key role in meeting Corporate Governance.

1.2 Purpose of this Handbook

This handbook describes a framework and best practices for the implementation of a Security Management System (SecMS). It provides guidance on how to address the European Common Requirements.

ATM Security must not restrict itself to considerations of ATM systems in isolation, but must also take into account their contributions to incident management in general and its role in the security of the aviation industry as a whole.

The SecMS provides a framework for an organisation to assess, in a systematic manner, the security environment in which it operates, to determine if adequate preventive, responsive and contingency measures are in place, to implement and maintain security measures, and to review the ongoing effectiveness of the system.

The origin of the SecMS can be traced to the ISO/PAS 28000 series, which is a high level management standard, developed to establish an overall 'supply chain' Security Management System. It is a generic standard which easily translates to the services of ATM and which is compatible to existing quality and environmental standards; ISO 9001:2000 and ISO 14001:2004. The framework supports a common cross industry approach to security and allows, if desired, seamless integration of the SecMS in an existing organisation management system. It is aligned to a number of other standards currently in use. A discussion of these standards is given in Annex B.

The SecMS can be viewed as the framework within which other security activities and standards are incorporated, for example security risk assessment, the identification of security measures, the development of security programmes or external standards with which ATM service providers must comply.

The SecMS is divided into five Key Activities:

1. **Policy;**
2. **Security risk assessment & planning;**
3. **Implementation & operation;**
4. **Checking & corrective action;**
5. **Management review.**

Figure 1.1 illustrates these five Key Activities arranged into a continuous improvement loop. After the SecMS has been implemented and is operational, each activity can be reviewed and updated on an individual basis. However any change or update must be assessed on its impact on the other activities.

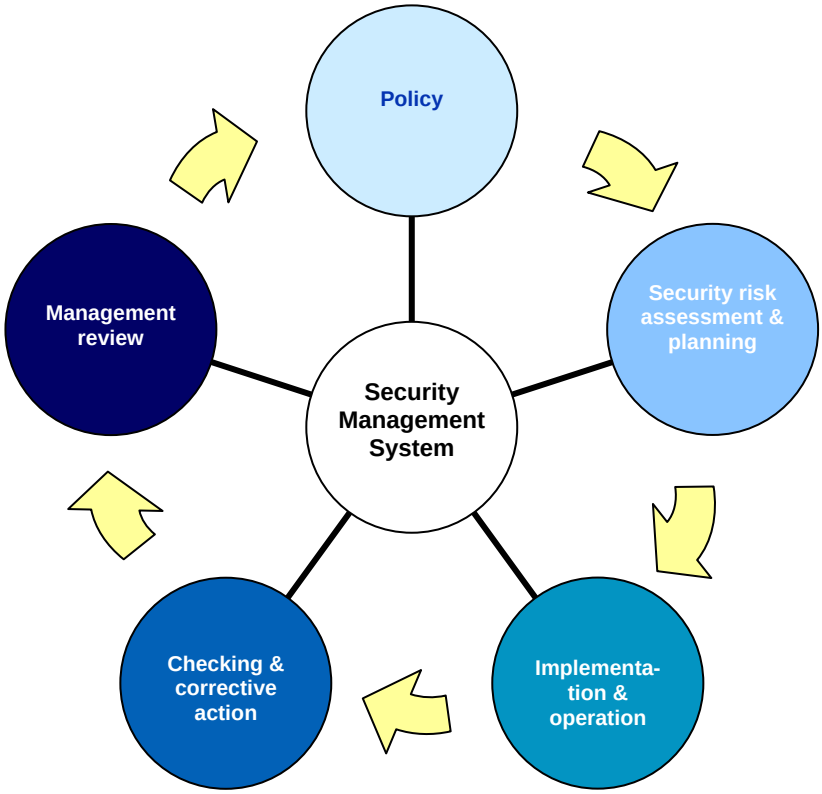


Figure 1.1 SecMS - Key Activities and Continuous Improvement

These Key Activities are further sub-divided into **18 Elements** (see Figure 1.2). Key Activities and Elements are designed to ensure that processes, responsibilities and expectations are clear. This framework can be used across the respective organisational levels so that individual customisation is easily possible. The framework is flexible enough to allow a variety of different management styles to be applied.

1.3 Key Activities and Elements

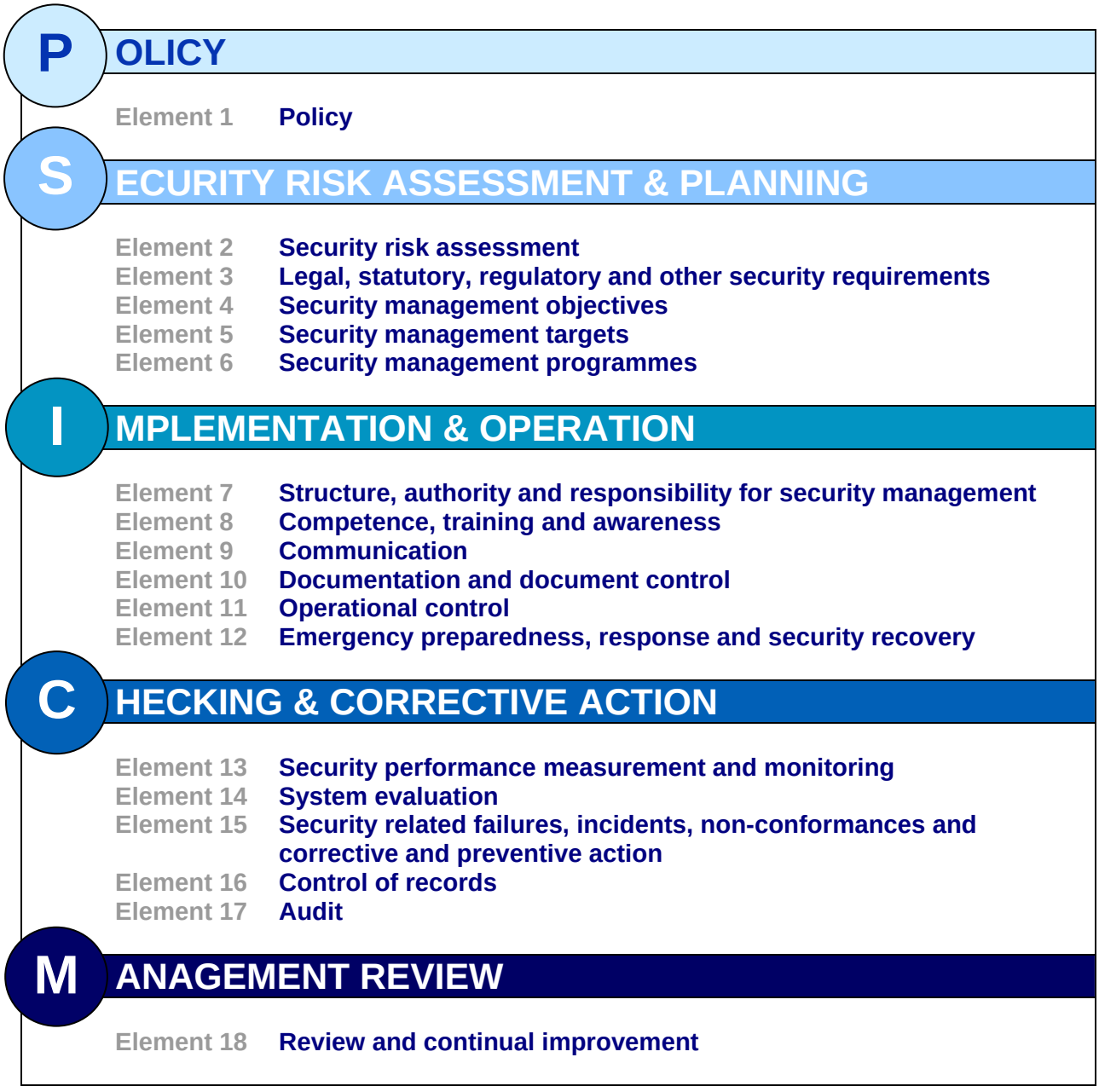
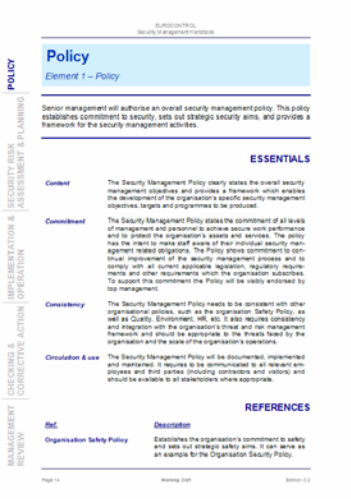


Figure 1.2 Key Activities and 18 Elements

1.4 Element Descriptions

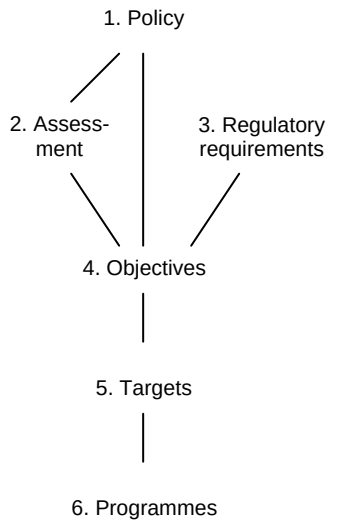
The following section presents the 18 Elements in detail. As shown below, each Element is described in a format covering:



Element	Description of the Element in 2 or 3 sentences
Essentials	Key aspects of the Element
References	Examples of methodologies and references

1.5 Sequencing of Elements

While some of the elements can be implemented in parallel fashion, others follow a sequential pattern where one element needs to be completed before the second element is initiated. In particular, in the Key Activities 'Policy' and 'Security risk assessment and planning' the implementation follows a sequential approach. Because these two activities form the foundation of the SecMS, the chosen sequencing of elements is further clarified and discussed below to provide a clear overview of the reasoning behind it.



Policy is top management commitment to security. Overall sense of direction and sets principles of action

The assessment identifies the security risks based on threats, vulnerabilities and consequences. Regulatory requirements are additional security requirements from regulation. The assessment is performed before analysis of regulatory requirements to prevent regulations from steering the assessment. The assessment needs to be a creative and influence free activity to ensure comprehensiveness. Based on the assessment, coverage of the requirements can be analysed.

Based on the needs (assessment and the regulatory requirements) and in line with the Security Policy, objectives are defined and prioritised. They describe what needs to be done.

Targets are set to achieve the objectives within a specified time frame. Several targets can contribute to one objective.

Translation into defined actions so that targets and consequently the objectives are achieved. Requires the development of strategies and plans of actions to be taken.

1.6 Security definitions

The following are commonly used[3] terms with the Security community

Asset	anything that has value to the organization
Business continuity	strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level
Business continuity management (BCM)	holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities[4]
Business impact analysis (BIA)	process of analysing business functions and the effect that a business disruption might have upon them
Consequence	outcome of an incident that will have an impact on an organization's objectives[5], [6]
Control, safeguard, countermeasure	means of addressing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
Contingency plan	a plan to provide service continuity at an alternative location(s) in the event of a severe disruptive/denial event
Critical activities	those activities which have to be performed in order to deliver the key products and services which enable an organization to meet its most important and time-sensitive objectives
Disruption	an event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organization's objectives
Emergency planning	development and maintenance of agreed procedures to prevent, reduce, control, mitigate and take other actions in

[4] NOTE Business continuity management involves managing the recovery or continuation of business activities in the event of a business disruption, and management of the overall programme through training, exercises and reviews, to ensure the business continuity plan(s) stays current and up-to-date

[5] There can be a range of consequences from one incident

[6] A consequence can be certain or uncertain and can have positive or negative impact on objectives

	the event of an emergency
Guideline	a description that clarifies what should be done and how, to achieve the objectives set out in policies
Impact	an evaluated consequence of a particular event
Incident	a situation that might be, or could lead to, a business disruption, loss, emergency or crisis
Incident management plan	clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process
Information security	preservation of confidentiality, integrity and availability of information. Other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved
Likelihood	the chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities
Loss	a negative consequence
Policy	overall intention and direction as formally expressed by management.
Resilience	The ability of an organization to resist being affected by an incident
Risk	a combination of the probability of an event and its consequence or something that might happen and its effect(s) on the achievement of objectives
Rsk analysis	systematic use of information to identify sources and to estimate the risk
Risk appetite	the total amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time
Risk assessment	the overall process of risk identification, analysis and evaluation
Risk evaluation	process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk management	the structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling risks
Threat	a potential cause of an unwanted incident, which may result in harm to a system or organization. It is a function of

	intention and capability.
Vulnerability	a weakness of an asset or group of assets that can be exploited by one or more threats

1.7 Security regulation

The Single European Sky (SES) is a European Union initiative aimed at reinforcing safety and restructuring the European airspace to better accommodate air traffic flows, thus creating additional capacity and increasing the overall efficiency of the ATM system.

The SES legislation is intended to encourage an integrated approach to air navigation service provision, mainly through the de-fragmentation of European airspace. To ensure that service provision can be maintained efficiently and continually across the SES, the Service Provision Regulation (EC Regulation No 550/2004) includes the requirement for a common system of certification of service providers which enables the definition of their governing rules and obligations.

In accordance with the Service Provision Regulation the European Commission introduced in December 2005 the Commission Regulation (EC) No 2096/2005, laying down common requirements for the provision of navigation services throughout the Community.

Element four of the common requirements covers security and dictates that air navigation service providers shall establish a Security Management System to ensure:

- The security of its facilities and personnel so as to prevent unlawful interference with the provision of services;
- The security of operational data it receives or produces or otherwise employs, so that access to it is restricted only to those authorised.

In addition the Security Management System shall define:

- The procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lessons dissemination;
- The means designed to detect security breaches and to alert personnel with appropriate security warnings;
- The means of containing the effects of security breaches and to identify recovery action and mitigation procedures to prevent re-occurrence.

The air navigation service provider shall ensure the security clearance of its personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of its facilities, personnel and data.

In Annex A the requirements are mapped and cross referenced to the SecMS Key Activities and Elements, to illustrate the framework meets all security requirements.

PAGE INTENTIONALLY LEFT BLANK

Policy

Element 1 – Policy

Senior management will authorise a comprehensive, concise and understandable security management policy. This policy establishes commitment to security, sets out strategic security aims, and provides a framework for security management activities.

ESSENTIALS

Content	The Security Management Policy clearly states the overall security management goals and provides a framework which enables the development of the organisation's specific security management objectives, targets and programmes to be produced.
Commitment	The Security Management Policy states the commitment of all levels of management and personnel to achieve secure work performance and to protect the organisation's assets and services. The policy has the intent to make staff aware of their individual security management related obligations. The Policy shows commitment to continual improvement of the security management process and to comply with all current applicable requirements.
Internal consistency	The Security Management Policy needs to be consistent with other organisational policies, such as those for Safety, Quality, Environment, HR, etc. It requires consistency and integration with the organisation's threat and risk management framework and should be appropriate to the threats faced by the organisation and the scale of the organisation's operations.
External consistency	The policy should define the scope of security management and the relationship with other external parties such as ANSP's, military, airports etc. These interfaces need to be agreed with NSA.
Circulation & use	The Security Management Policy will be documented, implemented and maintained. It requires to be communicated to all relevant employees and third parties (including contractors and visitors) and should be available to all stakeholders where appropriate.

REFERENCES

Ref.	***Description***
Organisation Safety Policy	Can serve as an example for the Security Policy.

Security risk assessment & planning

Element 2 – Security risk assessment

Security risk assessment and the identification of necessary security control measures will form the basis of the whole security system. It is an ongoing identification and assessment of asset criticality, security threats, vulnerability and risks, and the identification and implementation of necessary management control measures. Once completed it should provide a total appreciation of the significant security threats, vulnerabilities and risks within the domain of the organisation.

ESSENTIALS

Scope

Security risk identification, assessment and control methods should be appropriate to the scale of the organisation's operations. They should be applied both to normal as well as degraded and special operations / procedures. The assessment should consider the likelihood of an event, in terms of threat and vulnerability, its consequences and all the measures in place or additionally required. The entire spectrum of threats should be considered as should the shared ownership of assets.
After an initial assessment, periodic reviews should take place. This can be in a regular cycle that depends on the threat level or after changes in the organisation.

Threats

The assessment should consider the threats against:

- Physical assets: e.g. control centres, radar sites, navigation beacons;
- Human assets: staff both operational and administrative;
- Communication systems: e.g. ground networks and data link between aircraft and control centre;
- Service provision;
- Information and data.

The threats may have a criminal (e.g. theft of equipment) or terrorist intent.

Consequences

The consequences could affect, for example:

- the provision of service;
- the cost impact on the ANSP;
- Loss of life, both internal and external to the organisation.

In addition, events which may not be of a direct threat to the organisation, but which impact the integrity of aviation in general should be considered as well.

Output

The result of the assessment provides input into:

- Security management objectives, targets and programmes;
- Requirements for design, specification and installation;
- Identification of adequate resources, including staffing;
- Identification of training needs and skills;
- Development of operational controls;
- The organisation's overall threat and risk management framework, contingency and recovery measures.

Methodology

The assessment requires a proactive approach instead of reactive and needs to include classification of the risks to determine which are to be avoided, eliminated or controlled. Approaches for the assessment are available, references are provided below. Part 2 includes processes and procedures for each of the elements, including methodologies for performing the risk assessment.

REFERENCES

Ref.	***Description***
Security Management Handbook Part 2	Provides guidance on Critical Asset identification, Security Risk Assessment Methodology and ICT security guidelines
ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (ICAO Doc 8973)	Manual developed for the purpose of assisting States to promote safety and security in civil aviation. Provides details of how states can comply with Annex 17 (Security) to the Chicago Convention. Includes a threat assessment methodology and a risk assessment model (Chapter 3.6).
ISO/PAS 28001 – Best practices for implementing supply chain security, assessments and plans	Whereas ISO/PAS 28000 provides the framework for the SecMS, the 28001 provides requirements and guidelines for the development and implementation of the security processes. Includes methodologies for security risk assessment and counter measure analysis (Chapter 5 and Annex A and B).
ISO/IEC 13335-3:2004 – Information Technology – Techniques for the management of IT security	Deals with management aspects of planning, implementation and operations of ICT security during the life cycle of an ICT project. Includes a detailed security risk analysis approach (Chapter 9).
ISO/IEC 17799 Information Technology – code of practice for information security management	Recommendations for information security management. Intended to provide a common basis for developing security standards and effective security management practice and to provide confidence in inter-organizational dealings. Only a suitable set of controls can achieve information security.
ASIS International: General security risk assessment	A methodology by which security risks at a specific location are identified and communicated, along with appropriate solutions.

Security risk assessment & planning

Element 3 – Legal, statutory, regulatory and other requirements

All security related requirements impacting the activities at each respective level of the organisation will be identified. Identification will take place after completion of the initial security risk assessment. This will prevent the requirements from steering the assessment and disrupting the assessment's objectivity. Monitoring will be carried out to ensure compliance with legal, statutory regulatory and other security requirements, to which the organisation subscribes.

ESSENTIALS

Identification of Compliance Issues	All applicable legal, statutory and other security regulatory requirements related to the organisation's security threat and risks will be identified. The organisation will establish, implement, and maintain procedures to identify and have access to the applicable requirements. Monitoring systems will ensure that new requirements are identified at an early stage. Best practices will be shared and lessons learnt from other organisations to deal with the requirements in the most effective manner.
External Interface	Interfaces with bodies external to the organisation, such as NSA, Military, other ANSP's, etc, will be defined including communications and management issues. External reporting requirements to such bodies need to be identified. Requirements should be agreed with NSA.
Means of Compliance	Monitoring of compliance and assessment and corrective action of non compliant issues will be discussed in Elements 14 through 18.

REFERENCES

Ref.	***Description***
European Commission Regulation N°2096/2005	Common Requirements for the Provision of Air Navigation Services. Element 4 covers security and requires ANSP's to establish a SecMS.
ICAO Annex 17 to the Convention on International Civil Aviation	Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference. Chapter 5 defines the management of response to acts of unlawful interference to an aircraft, including the role of ANSP's.

Security risk assessment & planning

Element 4 – Security management objectives

The organisation will establish, implement and maintain documented (and where practical) measurable security management objectives. These are prioritised objectives derived from the security risk assessment and regulatory requirements and consistent with the organisation's security policy.

ESSENTIALS

Input

The formulated objectives need to take account of:

- Legal, statutory and other security regulatory requirements;
- Security threats and risks;
- Technological options and operational requirements;
- Inputs from appropriate stakeholders and external sources such as intelligence agencies.

Relevancy & Consistency

The objectives need to be:

- Consistent with the commitment to continuous improvement;
- Quantified (where practicable);
- Reviewed periodically to ensure consistency with the Policy.

Regard should be given to information from those most likely to be affected by individual security objectives, as this can assist in ensuring they are reasonable, achievable and more widely accepted.

Communication

The security management objectives will be communicated to all employees and third parties, including contractors, with the intent to create awareness of individual obligations.

Examples

Objectives are higher level goals to be achieved through security management. 'What must the Security Management System accomplish?'

- Reduction of risk levels;
- Introduction of additional features into the SecMS;
- Improvement to existing facilities;
- Elimination / reduction in frequency of a particular undesired event.
- Reduction of impact levels and improvement recovery time

REFERENCES

Ref.	***Description***

Security risk assessment & planning

Element 5 – Security management targets

The organisation will establish, implement and maintain documented security management targets appropriate to the needs of the organisation. These targets are derived from and consistent with security management policy and objectives. Security targets are achievable goals to meet the objectives within a specified time frame.

ESSENTIALS

Requirements

The security management targets need to be of an appropriate level of detail for the organisation and the different levels of operation. The targets should prioritised, and where practicable, be 'SMART':

- Specific;
- Measurable;
- Achievable;
- Relevant;
- Time based.

Regard should be given to information from those most likely to be affected by individual security targets, as this can assist in ensuring they are reasonable, achievable and more widely accepted.

Relevancy & Consistency

The security management targets need to be consistent with the formulated security management policy and objectives. To ensure continuous relevancy and consistency with the security management objectives, the targets will be reviewed periodically. Where necessary targets need to be amended.

Communication

The security management targets will be communicated to all employees and third parties, including contractors, with the intent to create awareness of individual obligations.

Examples

The targets define what needs to be done and the means (the necessary steps) with which the security objectives can be achieved.

- Reduction of risk levels through introduction of new technologies and the timeframe of introduction;
- Steps taken to improve existing facilities and the timeframe.

REFERENCES

Ref.	***Description***

Security risk assessment & planning

Element 6 – Security management programmes

The organisation will establish, implement and maintain security management programmes. Each programme should describe how the organisation will translate its goals and policy commitments into defined actions so that security objectives and targets are achieved. The programme will require the development of strategies and plans of actions to be taken. The deterrence and mitigation strategy of the programme should be based on the measures identified in the security risk assessment.

ESSENTIALS

Security Case

The outputs from the security risk assessment will be brought together into a Security Case within the programme. A Security Case contains arguments and evidence that substantiate claims for achievement of acceptable levels of security. Based on the Security Case the programmes can be optimised, prioritised and ensure efficient and cost effective implementation of these programmes. Where significant alterations in working practices are expected, the programme should also provide for a new threat and risk assessment.

Planning

The security management programme will define the means in terms of resources and the time scale by which the security management objectives and targets are achieved.

Responsibility

For each security management programme the responsibility and authority for each task and allocated timescales will be designated, in order to meet the overall timescale of the related security objective. The programme owner will be responsible for setting and maintaining the Security Case.

Security Manual

A distinction can be made between one-time implementation programmes, e.g. construction of physical security barriers, and continuous security programmes, such as organisational procedures. Aspects such as organisational security procedures should be included in a Security Manual.

Relevancy & Consistency

To ensure effectiveness and continuous consistency with the security management objectives and targets, programmes need to be reviewed periodically. The programme should take account of operational and organisational requirements when considering the necessary methodological and technological options.

REFERENCES

Ref.	Description
ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (Doc 8973)	The Manual developed for the purpose of assisting States to promote safety and security in civil aviation. It provides details of how states can comply with Annex 17 (Security) to the Chicago Convention. It includes models and templates for national civil aviation, airport and aircraft operator's security programmes (Chapters 3.11 and 3.15). Both Annex 17 and the Manual are however focussed on airports and airlines. Air navigation services are only discussed in relation to their required response in case of unlawful interference to aircraft.
ISO/PAS 28001 – Best practices for implementing supply chain security, assessments and plans	Whereas ISO/PAS 28000 provides the framework for the SecMS, the 28001 provides requirements and guidelines for the development and implementation of the security processes. Includes methodologies for security risk assessment and development of counter measures (Chapter 5 and Annex A and B).
ISO/IEC 13335-3:2004 – Information Technology – Techniques for the management of IT security	Deals with management aspects of planning, implementation and operations of ICT security during the life cycle of an ICT project. Includes implementation of IT security plans (Chapter 10).
ISO/IEC 17799:2000 – Information Technology – Code of practice for information security management	This standard gives recommendations for information security management. It is intended to provide a common basis for developing organisational security standards and effective security management practice. Aspects covered in the standard include: • Organisational security (Chapter 4) • Asset control (Chapter 5) • Personnel security (Chapter 6) • Physical security (Chapter 7) • Access control (Chapter 9)

Implementation & operation

Element 7 – Structure, authority and responsibility

Responsibilities for security management will be defined at each level of the organisation, to ensure security is integrated with overall management activities. Element 7 establishes the roles, responsibilities and authorities, consistent with the achievement of the security management policy, objectives, targets and programmes.

ESSENTIALS

Management structure

The management structure will be clear, appropriately documented, communicated and effectively implemented. The interfaces between the line management structure and the security management function should be identified.

Roles and Responsibilities

The roles, responsibilities and authorities will be defined, documented and communicated to staff and contractors. Personnel will be evaluated regularly to monitor their effectiveness against the requirements.

Management Procedures

Management procedures for controlling security related activities will be developed. These include approval procedures for new or changed operations and procedures for SecMS maintenance. Process descriptions will help underpin these procedures and ensure consistency.

Top Management

Top management will provide evidence of its commitment to the development and implementation of the Security Management System (processes) and continually improving its effectiveness by:

- appointing a (top) management responsible for security;
- ensuring availability of adequate resources;
- managing stakeholder expectations;
- ensuring viability of the objectives, targets and programmes.

External Structures

According to ICAO's Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, ATM should participate in:

- National aviation security committee;
- Airport security programmes / airport security committee;
- Response to unlawful interference / seizure of aircraft.

In addition consideration should be given to external parties and interfaces, as identified in Element 3: NSA, Military, other ANSP's, etc.

REFERENCES

Ref.	***Description***

Implementation & operation

Element 8 – Competence, training and awareness

To ensure that personnel responsible for the design, operation and management of security equipment, processes and programmes are suitably qualified to carry out the activities to a satisfactory standard. Staff members will be adequately trained, motivated and competent for the job they are required to do.

ESSENTIALS

Awareness	Awareness of operational risk is the key to security. Competence and training procedures should make personnel aware of the importance of compliance with the security management policy, procedures and requirements of the SecMS, and the potential consequences to the organisation's security by departing from the specified operating procedures.
Training Needs Analysis	Training Needs Analysis will be carried out for each position, based on job requirements and specific responsibilities within the SecMS. The needs analysis will define competency requirements including general safety competence. These requirements can then be fed into training and the development of selection criteria.
Delivery	Formal training and coaching will be provided to a high standard using assessed internal and external resources. Projects will be covered as well as ongoing operational requirements.
Competence Review	All training and coaching activities will be monitored regularly to ensure high quality delivery and suitability. Training will focus on workplace benefits measured immediately after training, and also at a later date, when the skills and procedures are being put into practice.
Vetting	All personnel (including staff members, external suppliers and (sub) contractors) performing activities or functions pertinent to security will undergo background checks and selection procedures (particularly those working in security sensitive areas, with security sensitive data or implementing security controls). Until screening has been completed the individual cannot be appointed to their position.

REFERENCES

Ref.	***Description***

Implementation & operation

Element 9 – Communication

Approved security management information will be communicated to relevant employees, contractors and other stakeholders. The organisation will have procedures for ensuring that pertinent security management is communicated.

ESSENTIALS

Meetings

There should be an organisation-wide structure for meetings, which is used for cascading information down and filtering up information necessary for managing security, informing and motivating all employees. Appropriate records of meetings are to be retained and meeting effectiveness monitored.

Communication and consultation structures should encourage participation in good security practices from all those affected by its operations. This should include arrangements in:

- Consultation over development and review of policies and objectives and decisions on implementation of processes and procedures;
- Consultation over changes affecting workplace security.

Information sensitivity

Procedures should be in place to ensure the right information is communicated to all relevant parties. Due to the sensitive nature of certain security related information, consideration should be given to the sensitivity prior to dissemination of information.

REFERENCES

Ref.	***Description***

Implementation & operation

Element 10 – Documentation and document control

The organisation will establish and maintain a security management documentation system in which to document and maintain up-to-date documentation to ensure its SecMS can be understood and effectively implemented and operated. In addition the organisation will establish and maintain procedures for controlling documents and data critical to the operation of the SecMS and the organisation's security activities.

ESSENTIALS

Content

The organisation should identify the data and information that is needed for the SecMS, before developing the necessary documentation. The content of the documentation system can include:

- Security policy, objectives and targets;
- Description of the scope and elements of the SecMS;
- Documents and records required for standards;
- Operational documents;
- Results of security risk assessments;
- Other documents deemed necessary for security processes.

Document control and accessibility

A system of procedures will determine document sensitivity and will ensure documents, data and information can only be located and accessed by authorised personnel. Security arrangements should be in place for the use and storage of sensitive documentation, including the control of documentation during temporary withdrawal from storage.

In addition, the system should identify and control documentation to ensure they are periodically reviewed, revised as necessary and approved for adequacy by authorised personnel. Documents, data and information are to be secure, adequately backed up and recoverable.

Retention procedures

Retention procedures should make a distinction between:

- *Current version* of relevant documents should be available at locations where operations of the SecMS are performed.
- *Obsolete* documents are to be promptly removed from all points of issue and points of use.
- *Archival* documents, data and information retained for legal or knowledge preservation purposes.

REFERENCES

Ref.	***Description***

Implementation & operation

Element 11 – Operational control

The organisation will establish and maintain arrangements to ensure the effective application of control and counter measures, wherever these are required to control operational security risks, fulfil the security policy and objectives, achieve security targets and conform to legal and other requirements.

ESSENTIALS

Operational Practices

The organisation will identify and control operations and activities that are necessary for achieving the following:

- Security management policy
- Control of identified security threats and risks
- Compliance with regulatory security requirements
- Security management objectives
- Delivery of security management programmes

Operational Procedures

The organisation will establish, implement and maintain documented procedures (controls) to control operations where their absence could lead to failure to achieve the operations and activities as specified above. These controls will be based upon operational needs and risk assessments.

All controls and procedures will be developed / reviewed by appropriate staff and operators, familiar with the relevant processes. All procedures are required to be verified and validated before being documented.

Management of Change

Where monitoring indicates a need for changes, a formal change system should be used. Where existing arrangements are revised or new arrangements introduced, that could impact security management operations and activities, the organisation will consider the associated security threats and risks before implementation.

Revised arrangements include revised organisation structure, roles or responsibility, revised security management policy, objectives, targets or programmes, revised processes or procedures, introduction of new infrastructure, equipment or technology.

REFERENCES

Ref.	***Description***

Implementation & operation

Element 12 – Emergency preparedness, response & recovery

Plans and procedures will be established, implemented and maintained to identify the potential for and response to security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them. The plans include information on provision and maintenance of equipment, facilities or services required during or after an incident, responsibilities, procedures, contingency arrangements and a plan for business recovery.

ESSENTIALS

Identification of Emergency and Crisis Scenarios

Evaluations are carried out of any aviation security related incident scenarios, and their potential development, which may require emergency and/or crisis actions by the organisation. Emergency scenarios may include emergencies within an Operational Centre or other facility. Crises may also include the need for the organisation's response to aviation related incidents. E.g. ICAO's Security Manual prescribes the required response from air traffic control to acts of unlawful interference involving aircraft.

Consideration should be given to both immediate response and other supporting roles (e.g. the provision of information, media releases etc). Evaluations need to be documented, accessible and communicated to all relevant staff.

Emergency Plans

Emergency Plans, based upon identified scenarios should be developed and put in place. They should cover fallback arrangements and planned contingency measures. These plans need to be regularly drilled, reviewed and assessed.

Crisis Plan

A Crisis Plan is developed and is subject to regular testing and review. The Crisis Plan will include major escalation of events covered in the current Emergency Plans.

Communication

Personnel, including contractors and visitors, should be knowledgeable about the Emergency and Crisis Plans and any specific responses required. Site inductions are a prerequisite to attendance either for hands-on work, or for meetings.

Larger scheme

The emergency preparedness, response and recovery plans to a security incident need to be incorporated in the overall plans covering all aviation incident or accident scenarios.

REFERENCES

Ref.	Description
ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (Doc 8973)	Manual developed for the purpose of assisting States to promote safety and security in civil aviation. Provides details of how states can comply with Annex 17 (Security) to the Chicago Convention. Includes chapter on management of response to acts of unlawful interference and the role of air traffic control (Chapter 5). Both Annex 17 and the Manual are however focussed on airports and airlines. Air navigation services are only discussed in relation to their required response in case of unlawful interference to aircraft.
Organisation's overall emergency and crisis plans	Covers all aviation related incident and accident scenarios. The emergency preparedness response and recovery to security incidents will become part of the organisations overall emergency and crisis plans.

Checking & corrective action

Element 13 – Security performance measurement and monitoring

The security performance of the organisation as well as the performance of the Security Management System will be monitored and measured on a continual basis. It will involve the measurement of SecMS implementation and security occurrences. Regular monitoring enables the detection of changes in systems or operations, which may suggest any element is approaching a point at which acceptable standards can no longer be met and corrective action should be taken.

ESSENTIALS

Indicators	The organisation will identify key performance indicators for its security performance across the organisation that it either controls or has influence over.
Frequency	The organisation will consider the associated security threats and risks, including potential deterioration mechanisms and their consequences, when setting the frequency for measuring and monitoring the key performance indicators.
Proactive Measures of Performance	Monitors compliance with the security management programs, operational control criteria and applicable legislation and requirements. Defines degree to which the SecMS is being implemented using leading indicators which indicate which specific SecMS processes are being applied.
Reactive Measures of Performance	Monitors security-related deteriorations, failures, incidents, non conformances and other historical evidence of deficient SecMS performance. Enables to determine how effective the SecMS has been in contributing to security and to identify potential precursors to security occurrences. Occurrence statistics should be continually measured and trended for comparison against year on year data.
Measurement techniques	Examples of methods to measure security performance include security inspections, behaviour sampling, analysis of documentation, benchmarking, surveys, etc.

REFERENCES

Ref.	***Description***

Checking & corrective action

Element 14 – System evaluation

Security management plans, procedures and the organisation's capabilities to meet the security policy, objectives and targets will be evaluated periodically. In addition the organisation shall periodically review their compliance with applicable regulatory requirements. Significant changes must be reflected immediately in the procedures, in order to ensure security plans and procedures are maintained up-to-date.

ESSENTIALS

Methods of Analysis

The plans, procedures and capabilities of the system can be evaluated through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations and exercises.

Evaluations should be undertaken periodically or after an event to ensure that procedures are consistently applied. For high security risk activities, task observation techniques should be used to ensure that security critical procedures are well defined and followed. General security behaviour needs to be surveyed in area inspections.

Compliance

Evaluations should also cover SecMS documentation to ensure the effectiveness of the SecMS in achieving conformance with its policy and objectives.

In addition compliance with relevant legislation, regulations and industry best practices will be evaluated.

Documentation

Records of the results of the periodic evaluations will be kept by the organisation.

REFERENCES

Ref.	***Description***

Checking & corrective action

Element 15 – Failures, incidents, non-conformances and action

The organisation will have effective procedures for reporting and evaluating and/or investigating emergencies, security incidents and non-conformances. Deficient SecMS performance can be due to incorrect implementation or operation of the management system or due to unidentified risks and/or control measures during the risk assessment and planning phase. The purpose of these procedures is to prevent further occurrences of the situation and eliminate future non-conformities by identifying and dealing with the root causes.

ESSENTIALS

Preventive Actions	Evaluating and initiating preventive actions to identify potential failures of security in order to prevent them from re-occurring.
Corrective Actions	Identification and investigation of security related failures, including near misses and false alarms, incidents and emergency situations and non conformances. Actions will be focussed on either mitigation of consequences arising from such failures, or the initiation and completion of corrective actions to eliminate the causes.
Threat & Risk Assessment	Proposed preventive and corrective actions should be reviewed through the security threat and risk assessment process prior to implementation, unless immediate implementation forestalls imminent exposure to life or public safety.
Proportionality	Any preventive or corrective action taken to eliminate the causes of actual and potential non-conformances should be appropriate to the magnitude of the problems and commensurate with the security management related threats and risks likely to be encountered.
Changes in procedures	Changes will be implemented and recorded in documented procedures and follow the management of change procedure as described in Element 12: Operational control.

REFERENCES

Ref.	***Description***

Checking & corrective action

Element 16 – Control of records

In order to be able to demonstrate conformity to the requirements of the Security Management System, but also to legal, statutory or other security regulatory requirements, records will be established and maintained. These records demonstrate that the SecMS operates effectively.

ESSENTIALS

Actions

Procedures will be established, implemented and maintained for the identification, storage protection, retrieval, retention and the disposal of records.

Requirements

Records are required to be legible, identifiable and traceable. In addition, electronic and digital documentation should be rendered tamper proof, securely backed-up and only accessible to authorised personnel.

Examples

- Training and competence records
- Security inspection reports
- Security non-conformances
- Results of preventive and corrective actions
- Security Management System audit reports
- Security meeting minutes
- Reports of security exercises and drills
- Management review

Element 10

All records which need to be retained can be stored in the document management system and controlled according to the document control procedures, as described in element 10.

REFERENCES

Ref.	***Description***

Checking & corrective action

Element 17 – Audit

Formal auditing will be carried out to confirm the degree of implementation and operation of the SecMS and to assess compliance issues. In addition the audits can also be used to identify opportunities for improvement. A proportion of the audits should be carried out by independent authorised 3rd parties. The audits will be included in an established, implemented and maintained audit program which insures that the audits are carried out at planned intervals.

ESSENTIALS

Implementation and Operation

The audit program sets out to determine whether the Security Management System conforms to planned arrangements, including possible regulatory requirements, as defined in Element 3 (and agreed with NSA). Whether it has been properly implemented and maintained and if it is effective in achieving the organisation's policy and objectives.

The audit process should consider the results of previous audits and actions taken to rectify non-conformances; provide information on to management and verify that security equipment and personnel are properly deployed.

Auditors should be independent of the part of the organisation or activity that is to be audited and if necessary security cleared for the areas being audited. The audits should be conducted according to planned arrangements or if circumstances require, such as after incidents or changes.

Threat & Risk Assessment

The audit program, including any schedule, will be based on the results of threat and risk assessments and the results of previous audits.

Audit Procedure

The audit procedures cover the scope, frequency, methodology and competencies, as well as the responsibility and requirements for conducting audits and reporting results.

Top management

For SecMS auditing to be of value it is necessary that top management is fully committed to the concept of auditing. Top management should consider the audit findings and recommendations and take appropriate action as necessary, within an appropriate time.

REFERENCES

Ref.	***Description***

Management review

Element 18 - Review and continual improvement

The Security Management System will be reviewed by top management at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. These reviews will include assessment of opportunities for improvement and the need for changes. The review should consider whether the security policy continues to be appropriate and establish new or updated security objectives for continual improvement.

ESSENTIALS

Inputs

Inputs for the management review include:

- Audit results and compliance evaluations
- Communications from stakeholders
- Security performance
- Extent to which objectives and targets have been met
- Status of preventive and corrective actions
- Follow-up actions from previous management reviews
- Changing circumstances / environment
- Recommendations for improvement

Focus

The management review process normally includes a meeting carried out by top management, on a regular basis. The review should focus on the overall performance of the SecMS and not on specific details, since these should be handled by normal means within the SecMS.

Actions

Actions as a result of management review include decisions and actions related to possible changes to security policy, objectives, targets and other elements of the Security Management System, consistent with commitment to continual improvements.

REFERENCES

Ref.	***Description***

PART 2 – SECURITY PROCESSES AND PROCEDURES

Security Risk Assessment Methodology

Security Risk Assessment and Planning (Element 2)

Overview

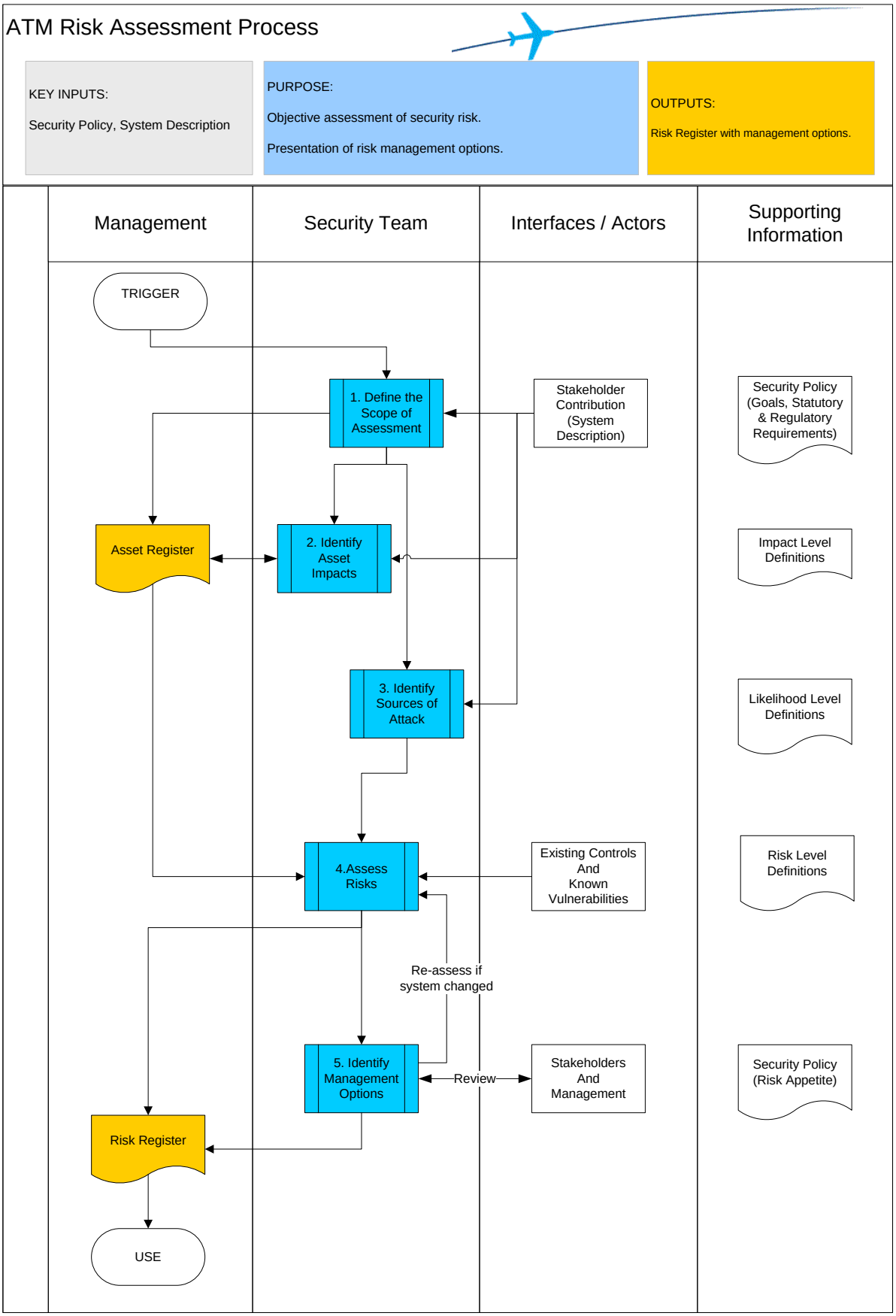
This ATM Security Risk Assessment Methodology (*SecRAM*) provides Air Navigation Service Providers (ANSPs) with a systematic approach to security risk assessment, to assist them with compliance with EC Regulation 2096/2005 (the Common Requirements).

The methodology described is applicable to a whole ANSP, or to an ATM project, system or facility. The assessment process is systematically defined; it includes input/output requirements and describes the documentation that flows between process steps.

The process first establishes the scope and inputs to the assessment, identifies assets and attackers (threat agents), then identifies risks that result from potential ways that attackers could impact assets. Finally, management options to reduce the severity of unacceptable risks are identified, selected and documented.

This methodology also describes the essential contribution of stakeholders outside the security team that carries out the assessment. An effective assessment depends on stakeholders who have specialist operational or design knowledge of the domain. Equally important is the relationship of the security team to its manager or customer. Management involvement is needed to interpret security goals, decide what security management options are possible or acceptable, and accept any residual risks that are regarded as tolerable.

This process is designed to be used by those who are skilled in security assessment, as well as by those who are less experienced. Accordingly, this methodology specifies the framework of actions that are needed to carry out an assessment, but does not provide a guide to how these may be carried out, or how to overcome common difficulties.


ATM Risk Assessment Process
KEY INPUTS:
Security Policy, System Description
PURPOSE:
Objective assessment of security risk.
Presentation of risk management options.
OUTPUTS:
Risk Register with management options.
Management
Security Team
Interfaces / Actors
Supporting Information
TRIGGER
1. Define the Scope of Assessment
Stakeholder Contribution (System Description)
Security Policy (Goals, Statutory & Regulatory Requirements)
Asset Register
2. Identify Asset Impacts
Impact Level Definitions
3. Identify Sources of Attack
Likelihood Level Definitions
4.Assess Risks
Existing Controls And Known Vulnerabilities
Risk Level Definitions
Re-assess if system changed
5. Identify Management Options
Review
Stakeholders And Management
Security Policy (Risk Appetite)
Risk Register
USE

PAGE INTENTIONALLY LEFT BLANK

Information Communication Technology Guidelines

Security Risk Assessment and Planning (Element 2)

Overview

The Information and Communication Technology (ICT) guidance provides Air Navigation Service Providers (ANSPs) in Europe with the practical implementation of regulatory requirements for ICT Security, in particular EC Regulation 2096/2005 (the Common Requirements).

The scope of ICT security includes computer systems and networks, information assets such as operational data, and software; it also includes the environment in which these systems function, and is therefore concerned with management, organisation, operation, personnel, physical security, supporting contractors, infrastructure and services, and third parties such as law enforcement, security and regulatory authorities.

ICT security is part of the wider security management system (SecMS) that must be established by an ANSP; this wider system is described in the EUROCONTROL Security Management Handbook, which this guidance supports.

The predominant standard for ICT security is ISO/IEC 27001:2005; all the requirements of this standard are included in this guidance, in order to enable ANSPs to implement conforming management. However, security requirements are also included from other standards, particularly from COBIT and the ISO/IEC 13335 family, and from current best practice, where they are needed to ensure that this guidance is modern and well-balanced.

In addition to providing advice on standards conformance, this guidance is organised to address two other issues:

- The wide range of ANSP organisation types; and
- The need to assist ANSPs in selecting appropriate security controls from the large number specified in ICT standards.

PAGE INTENTIONALLY LEFT BLANK

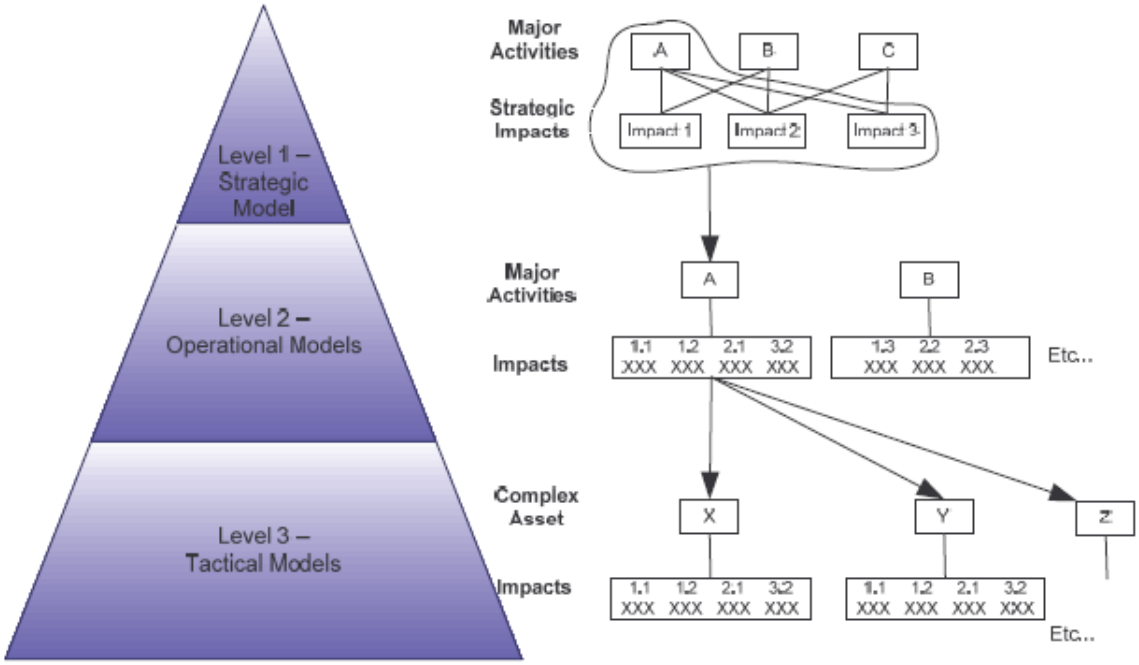
Threat Model

Security Risk Assessment and Planning (Element 2)

Overview

As part of the Risk Assessment, a model will need to be developed to aid in the definition and scope of a system and identify threats and vulnerabilities. The model provide valuable tools for the analysis of the security issues that could affect organisations. They are able to view the systems as a whole and aim to identify all potential security threats and not just expose the vulnerabilities.

The Model is developed in three hierarchical levels that are applicable to different levels of operation within ATM organisations which provide flexibility and adaptability to the variety of service providers with Europe.



This Model proposes a common framework for the development of the ATM Threat Model which will allow ANSPs and ATM organisations to construct their own ATM Threat Models using a consistent approach. Furthermore the Model provides a common terminology for discussing threat, controls, attack methods and impacts, allowing for improved inter and intra organisation discussion concerning security.

PAGE INTENTIONALLY LEFT BLANK

ANNEX A – COMMISSION REGULATION (EC) NO 2096/2005

Links to Regulation (EC) No 2096/2005

In accordance with Commission Regulation (EC) No 2096/2005 an air navigation service provider shall be able to provide services in a safe, efficient, continuous and sustainable manner consistent with any reasonable level of overall demand for a given airspace. To this end the Regulation lays down common requirements for the provision of air navigation services throughout the Community.

The fourth element of these requirements covers security, requiring the air navigation service provider to establish a Security Management System. In table A.1 the requirements concerning security, as specified in the Regulation, are directly linked to the SecMS key activities and elements as defined in Part 1 of this document.

SecMS key activities & elements Commission Regulation (EC) No 2096/2005: Annex 1. Requirements relevant to security	1. Policy	Security risk assessment & planning					Implementation & Operation						Checking & Corrective action					18. Review and continual improvement
		2. Security risk assessment	3. Legal, statutory and other security regulatory requirements	4. Security management objectives	5. Security management targets	6. Security management programmes	7. Structure, authority and responsibility for security management	8. Competence, training, and awareness	9. Communication	10. Documentation & document control	11. Operational control	12. Emergency preparedness, response and security recovery	13. Security performance measurement and monitoring	14. System evaluation	15. Security related failures, incidents, non-conformances and corrective and preventive action	16. Control of records	17. Audit	
2. ORGANISATIONAL STRUCTURE AND MANAGEMENT																		
a. The ANSP shall define the authority, duties and responsibilities of the nominated post holders in charge of safety, quality, **security**, finance and human resources							■	■										
b. The ANSP shall set out a business and annual plan to define aims, goals, objectives and indicators	■	■	■	■	■	■												
4. SECURITY																		
a. Security of facilities & personnel as to prevent unlawful interference with provision of services		■		■	■	■					■							
b. Security of operational data so that access is restricted to those authorised		■		■	■	■				■	■							
c. Procedures relating to security risk assessment and mitigation		■	■	■	■	■					■	■						
d. Procedures relating to security monitoring and improvement													■	■	■	■	■	■
e. Procedures for security reviews													■	■	■	■	■	■
f. Procedures for learning dissemination							■	■	■	■								
g. Means designed to detect security breaches and alert personnel		■									■	■	■		■			
h. Means of containing effects of security breaches and to identify recovery action and procedures to prevent re-occurrence		■										■			■			
i. Ensure security clearance of its personnel							■	■										
j. Coordinate with civil & military authorities			■				■		■									
5. HUMAN RESOURCES																		
a. An ANSP shall employ appropriately skilled personnel to ensure the provision of its services in a safe, efficient, continuous and sustainable manner.							■	■										
8.2 CONTINGENCY PLANS																		
a. The ANSP shall have in place contingency plans in the case of events which result in significant degradation or interruption of its services.												■						

Figure A.1 Relation EC requirements and SecMS key activities

PAGE INTENTIONALLY LEFT BLANK

ANNEX B – ICAO DOCUMENTS

Background and objective

Annex 17 to the Convention on International Civil Aviation covers Security, safeguarding international civil aviation against acts of unlawful interference. The annex was first adopted in 1974 and includes Standards and Recommended Practices on Security.

The objectives of the Annex are:

- Each Contracting State shall have as its primary objective the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation.
- Each Contracting State shall establish an organisation and develop and implement regulations, practices and procedures to safeguard civil aviation against acts of unlawful interference taking into account the safety, regularity and efficiency of flights.
- Each Contracting State shall ensure that such an organisation and such regulations, practices and procedures:
    - Protect the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation; and
    - Are capable of responding rapidly to meet any increased security threat.

Guidance material to the Annex is provided in the Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (Doc 8973). It provides detailed procedures and guidance on aspects of civil aviation security and is intended to assist States in the implementation of their respective national civil aviation security programmes required by the specifications in the Annexes to the Convention on International Civil Aviation.

Focus of the Annex and Security Manual

Annex 17 and the Security Manual are built around three main themes:

- **Organisation:** defines the organisational structure entrusted with security in civil aviation. Three core groups are identified: The National organisation and appropriate authority, Airport operations and Aircraft operators. The theme discusses policy, programmes, cooperation and training for each of the defined organisational levels, including the response to incidents and contingency plans.

- **Preventive security measures:** The measures identified in the Annex and the Security Manual are built up around
    - Access control,
    - Aircraft,
    - Passengers and their cabin luggage,
    - Hold luggage,
    - Cargo, Mail and other goods, and
    - Special categories of passengers.

  These measures cover aspects such as terminal security, screening of passengers and luggage, security of catering and supplies, airport design, protection of aircraft etc.

- **Management of response to acts of unlawful interference:** defines the required measures when reliable information exists that an aircraft may be subjected to an act of unlawful interference. Discusses aspects such as the role of air

traffic control, the set up of an emergency operations centre, how to deal with explosive devices etc.

The role of the ANSP's

The Annex and the Security Manual are primarily focused on the national authorities entrusted with the security in the civil aviation, airports and aircraft operators. The three organisational groups are extensively discussed in the first theme on organisation. In addition, all preventive measures discussed in the second theme mainly focus on the security at the airport and around aircraft, such as access control and screening measures.

The role of the ANSP's is only discussed in the third theme on response to acts of unlawful interference.

- Air traffic controllers should collect all necessary information from the aircraft subjected to an unlawful interference, and transmit this information to the appropriate authorities and stakeholders.
- In addition the air traffic controllers shall provide assistance to the aircraft with air navigation services and shall render all assistance possible.

Comparison with structure SecMS

The visualisation on the next page (figure B.2) provides an overview of the structure of SecMS compared to the structure of the Security Manual. The overview shows that the structure of the Security Manual is limited in comparison to the SecMS. In particular, the checking & corrective action and the review & continual improvement phases in the SecMS are not covered by the Security Manual. In addition the Security Manual has no structured approach to translating the security policy into objectives and targets. The Security Manual has an unbalanced focus on the security programmes, specific security measures and the required organisation structures.

The SecMS as overall framework

The SecMS can be considered as an overall framework in which a variety of regulations, standards and requirements can be incorporated. This not only includes the European Regulation EC No. 2096/2005, but also ICAO Annex 17 or others. Accordingly, implementation of the SecMS can ensure that requirements, from Annex 17 and the ICAO Security Manual are also met.

The requirements for ANSP's, as stated in Annex 17 and the Security Manual, will be covered in elements:

- Element 2: Security risk assessment
- Element 6: Security management programmes
- Element 9: Communication
- Element 11: Operational Control
- Element 12: Emergency preparedness, response and security recovery.

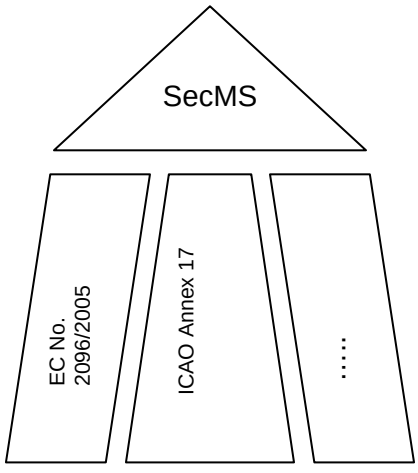


Figure B.1: SecMS as framework

SecMS key activities & elements / Content ICAO Security Manual (Doc 8973)	1. Policy	Security risk assessment & planning					Implementation & Operation						Checking & Corrective action					18. Review and continual improvement
		2. Security risk assessment	3. Legal, statutory and other security regulatory requirements	4. Security management objectives	5. Security management targets	6. Security management programmes	7. Structure, authority and responsibility for security management	8. Competence, training, and awareness	9. Communication	10. Documentation & document control	11. Operational control	12. Emergency preparedness, response and security recovery	13. Security performance measurement and monitoring	14. System evaluation	15. Security related failures, incidents, non-conformances and corrective and preventive action	16. Control of records	17. Audit	
3. Organisation																		
3.1 Appropriate authority of security							■											
3.2 Civil Aviation Security policy & regulatory section	■		■															
3.3 National aviation security programme						■												
3.4 National aviation security coordination							■		■									
3.5 International cooperation							■		■									
3.6 Threat assessment and risk assessment		■																
3.7 Research and development security equipment											■							
3.8 Security training programmes								■										
3.9 Supporting facilities at airports							■											
3.10 Airport security programme						■												
3.11 Airport security authority							■											
3.12 Airport security coordination							■		■									
3.13 Response to airport incidents						■					■	■						
3.14 Contingency plans												■						
3.15 Aircraft operator's security programme						■												
4. Preventive security measures		■				■					■							
5. Management of response to acts of unlawful interference		■				■			■		■	■						

Figure B.2 Relationship between ICAO Doc 8973 and the SecMS

SecMS key activities & elements Title: **ICAO Annex 17 Security**	1. Policy	Security risk assessment & planning					Implementation & Operation						Checking & Corrective action					18. Review and continual improvement
		2. Security risk assessment	3. Legal, statutory and other security regulatory requirements	4. Security management objectives	5. Security management targets	6. Security management programmes	7. Structure, authority and responsibility for security management	8. Competence, training, and awareness	9. Communication	10. Documentation & document control	11. Operational control	12. Emergency preparedness, response and security recovery	13. Security performance measurement and monitoring	14. System evaluation	15. Security related failures, incidents, non-conformances and corrective and preventive action	16. Control of records	17. Audit	
2.1 Objectives	■		■	■			■											
2.2 Applicability		■																
2.3 Security Facilitation				■														
2.4International Cooperation				■														
2.5 Equipment, Research and Development																		
3.1 National Organisation and Appropriate Authority																		
3.4 Quality Control								■					■		■		■	■
5.2.3 Each Contracting State shall provide assistance to an aircraft subjected to an act of unlawful seizure, including the provision of navigation aids, air traffic services and permission to land as may be necessitated by the circumstances.			■															
Annex 2 3.7 Unlawful interference An aircraft which is being subjected to unlawful interference shall endeavour to notify the appropriate ATS unit of this fact, any significant circumstances associated therewith and any deviation from the current flight plan necessitated by the circumstances, in order to enable the ATS unit to give priority to the aircraft and to inimize conflict with other aircraft.			■															
Annex 11 2.22.1 An aircraft known or believed to be in a state of emergency, including being subjected to unlawful interference, shall be given maximum consideration, assistance and priority over other aircraft as may be necessitated by the circumstances. 2.22.2 When an occurrence of unlawful interference with an aircraft takes place or is suspected, ATS units shall attend promptly to requests by the aircraft. Information pertinent to the safe conduct of the flight shall continue to be transmitted and necessary action shall be taken to expedite the conduct of all phases of the flight, especially the safe landing of the aircraft. 5.1.1 Alerting service shall be provided: c) to any aircraft known or believed to be the subject of unlawful interference.			■															

Figure B.3 Relationship between ICAO Annex 17 and the SecMS

PAGE INTENTIONALLY LEFT BLANK

ANNEX C - ECAC DOCUMENT 30

Background and objective

ECAC Doc 30 is concerned with the responsibilities and activities of the State with respect to the security of air transport operators and airports. It deals with the setting up of a National Aviation Security Programme that, in its widest interpretation, could be understood also to include the activities of the ANSP. The references given above are not in themselves responsibilities of the ANSP but are indications of what could be required by the state, depending on the national interpretation of this regulation.

SecMS key activities & elements / Title: **ECAC Doc 30 10th edition**	1. Policy	Security risk assessment & planning					Implementation & Operation						Checking & Corrective action					
		2. Security risk assessment	3. Legal, statutory and other security regulatory requirements	4. Security management objectives	5. Security management targets	6. Security management programmes	7. Structure, authority and responsibility for security management	8. Competence, training, and awareness	9. Communication	10. Documentation & document control	11. Operational control	12. Emergency preparedness, response and security recovery	13. Security performance measurement and monitoring	14. System evaluation	15. Security related failures, incidents, non-conformances and corrective and preventive action	16. Control of records	17. Audit	18. Review and continual improvement
Chapter 3.1.6						■												
Chapter 3.1.7																		■
Chapter 3.1.8						■												

Figure C.1 Relation ECAC Doc 30 and SecMS key activities

ANNEX D – STANDARDS & GUIDELINES

Relevant aviation security standards

Standard	Description
European Commission Regulation (EC) No 2096/2005	The Regulation lays down common requirements for the provision of air navigation services throughout the Community. Herewith to ensure that providers shall be able to provide services in a safe, efficient, continuous and sustainable manner consistent with any reasonable level of overall demand for a given airspace. Element four of the requirements covers security and requires air navigation service providers to establish a Security Management System.
ICAO Annex 17 to the Convention on International Civil Aviation: SECURITY – Safeguarding International Civil Aviation Against Acts of Unlawful Interference	Standards and recommended practices to assure the protection and safety of passengers, crew, ground personnel, general public, aircraft and facilities of an airport serving civil aviation, against acts of unlawful interference perpetrated on the ground or in flight. This is carried out at an international, national and airport level. However, Annex 17 is mainly focussed on airports and aircraft operators. Air navigation services are only discussed in relation to their required response actions in case of a renegade or other acts of unlawful interference to an aircraft (Chapter 5).
ICAO Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference (Doc 8973)	Manual developed for the purpose of assisting States to promote safety and security in civil aviation. Provides detailed procedures and guidance on aspects of aviation security and is intended to assist with the implementation of and ensure compliance with Annex 17. In accordance with Annex 17, the guideline is focused on national aviation authorities, airports and aircraft operators. Air navigation services are only discussed in relation to acts of unlawful interference to an aircraft. Includes extensive templates and examples: • Model national civil aviation security programme • Model airport security programme • Model aircraft operator security programme • Guidance on recruitment, selection, training and certification of aviation security staff • Model aviation security training programme • Threat assessment methodology

- Risk assessment model
- Physical security measures
- Aviation inspections, audits and surveys

Commission Regulation (EC) No 2320/2002

Mandatory regulation in effect since January 2003, setting standards in aviation security at all EU airports. Regulation 2320/2002 is based on standards contained in ICAO Annex 17, recommendations of European Civil Aviation Conference and Commissions proposals. Hereby providing a comprehensive and advance base for EU aviation security standards.

The Common standards of regulation 2320/2002 include detailed rules in the areas of airport and aircraft security and are therefore similar in scope as ICAO Annex 17.

ICAO Annex 11: Air Traffic Services

Chapter 2: provisions on service to aircraft in the event of an emergency, including unlawful interference.

Chapter 5: alerting provisions in case of an unlawful interference: notification to rescue coordination centres, information to operator and information to other aircraft in the vicinity

ICAO Doc 4444: Procedures for Air Navigation Services

Chapter 5: General provisions for the separation of controlled traffic in case of unlawful interference.

Chapter 15: Procedures related to emergencies, communication failure and contingencies, including unlawful interference and aircraft bomb threat

IATA Security Management Systems for Air Transport Operators

Guidance material / template of a Security Management System for Air Transport Operators. Based on ICAO Annex 17 and the ICAO Security Manual.

Provides detailed overview of:

- Organisation & management
- Training programmes
- Security control
- Contingency & response
- Quality assurance

Other standards & guidelines

The standards and guidelines in the overview below include standards supporting implementation of the SecMS or specific security measures, guidelines on how to perform activities such as the security risk assessment and examples of Security Management Systems and/ or its elements.

Standard/ Guideline	***Description***
ISO/PAS 28000: Specification for Security Management Systems for the supply chain	Security management standard for the establishment of an overall supply chain Security Management System. It requires the organisation to assess the security environment in which it operates and determine if adequate security measures are in place. If security needs are identify by this process, the organisation should implement mechanisms and processes to meet these needs. The PAS specifies the requirements for a Security Management System, including those aspects critical to security assurance of the supply chain. It is intended for organisations that wish to: • establish, implement, maintain and improve a SecMS • Assure compliance with a stated security management policy • Demonstrate such compliance to others • Seek certification/registration of its SecMS • Make a self determination and self declaration of compliance. Acts as the template for developed framework in Part 1.
ISO/PAS 28001: Best practices for implementing supply chain security, assessments and plans	Whereas ISO/PAS 28000 provides the framework for the SecMS, the 28001 provides requirements and guidelines for the development and implementation of the security processes and establish and document a minimum level of security. The standard includes guidelines on • Security assessments • Development and execution of security plan • Documentation and monitoring of security processes • Continuous improvement • Actions after a security incident • Protection of security information

ISO/IEC 15408:1999 Information Technology – security techniques – Evaluation criteria for IT security

ISO/IEC 15408 defines Common Criteria (CC) to be used as the basis for evaluation of security properties of IT products and systems. The CC permits comparability between the results of independent security evaluations.

The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use, are tolerable.

Under scrutiny are for example operating systems, computer networks, distributed systems, and applications. The CC addresses confidentiality, integrity, and availability of the IT system. The CC is applicable to IT security measures implemented in hardware, firmware or software.

The ISO/IEC 15408 standard can be applied to evaluate IT systems supporting the SecMS and its documentation, as well as a security control measure to control IT security of operations and operational data. (Activity: Security risk assessment and planning).

ISO/IEC 17799 Information Technology – code of practice for information security management

This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.

Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Information security is characterized here as the preservation of:

a. confidentiality: ensuring information is accessible only to those authorised;
b. integrity: safeguarding accuracy and completeness of information and processing methods;
c. availability: ensuring that authorised users have access to information and associated assets when required.

	Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met. The standard can be applied to support the risk assessment and mitigation analysis for information and communication risks. (Activity: Security risk assessment and planning).
ISO/IEC 13335:2004 Information technology – security techniques – management of information and communications technology security	This standard deals with management aspects of planning, implementation and operations, including maintenance, of information and communications technology (ICT) security The standard contains a general discussion of useful concepts and models for the management of ICT security. This material is suitable for managers and those who have responsibility for ICT security, for an organisation's overall security program or an organisation's ICT systems. The second part of the standard describes security risk management techniques appropriate for use by those involved with management activities. The standard can be used to support the security risk assessment for information, data and communication security threats and to develop security programmes and plans for ICT security as part of the organisation's overall security plans.
ISO/IEC 27001:2005 Information technology – security techniques – information Security Management Systems requirements	This standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System. All aspects are covered in the framework as described in part 1 of this report.
ASIS International: Chief Security Officer Guideline (www.asisonline.org)	A guideline that addresses key responsibilities and accountabilities, skills and competencies, and qualifications for an organisation's senior security executive. Supports implementation of element 7: Structure, authority and responsibility for security management and element 8: Competence, training and awareness.

ASIS International: General security risk assessment (www.asisonline.org)	A seven-step process that creates a methodology by which security risks at a specific location can be identified and communicated, along with appropriate solutions. Supports implementation of element 2: security risk assessment.

PAGE INTENTIONALLY LEFT BLANK

ANNEX E – ISO/PAS 28000

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on the committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 28000 was prepared by Technical Committee ISO/TC 8, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.

Introduction

This Publicly Available Specification has been developed in response to demand from industry for a security management standard. Its ultimate objective is to improve the security of supply chains. This Specification is a high level management standard that enables an organization to establish an overall supply chain security management system. It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs. Since supply chains are dynamic in nature, some organizations managing multiple supply chains may look to their service providers to meet related governmental or ISO supply chain security standards as a condition of being included in that supply chain in order to simplify security management as illustrated in Figure 1.

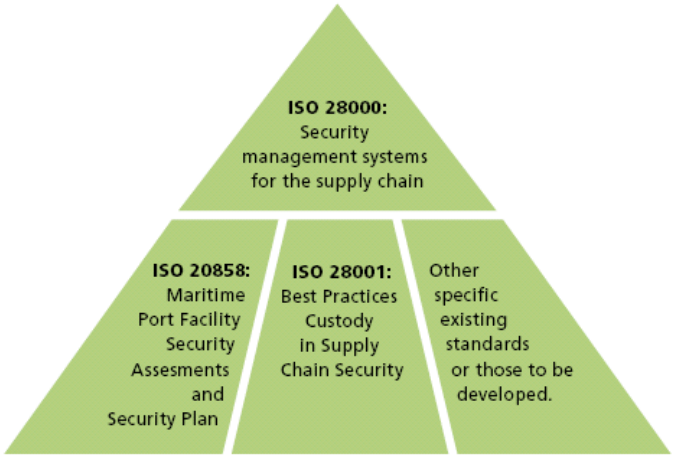


Figure 1 – Relationship between ISO PAS 28000 and other relevant standards

This Specification is intended to apply in cases where an organization's supply chains are required to be managed in a secure manner. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

Compliance with a Specification does not in itself confer immunity from legal obligations. For organizations that so wish, compliance of the security management system to this Specification may be verified by an external or internal auditing process.

This Specification is based on the ISO format adopted by ISO 14001:2004 because of its risk based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2000) may be able to use their existing management system as a foundation for a security management system as prescribed in this Specification. It is not the intention of this specification to duplicate governmental requirements and standards regarding supply chain security management to which the organization has already been certified or verified compliant. Verification may be by an acceptable first, second, or third party organization.

Note: This specification is based on the methodology known as Plan-Do-Check-Act (PDCA). PDCA can be described as follows:

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organization's security policy
- Do: implement the processes
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results
- Act: take actions to continually improve performance of the security management system

1. Scope

This Specification specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. Security management is linked to many other aspects of business management. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

This Specification is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

a) Establish, implement, maintain and improve a security management system;
b) Assure compliance with stated security management policy;
c) Demonstrate such compliance to others;
d) Seek certification/registration of its security management system by an Accredited third party Certification Body; or
e) Make a self-determination and self-declaration of compliance with this Specification.

There are legislative and regulatory codes that address some of the requirements in this specification. It is not the intention of this standard to require duplicative demonstration of compliance.

Organizations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.

2. Normative references

None

3. Terms and Definitions

For the purposes of this specification, the following terms and definitions apply:

3.1 Facility(ies): plant, machinery, property, buildings, vehicles, ships, port facilities and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function or service.
NOTE: This definition includes any software code that is critical to the delivery of security and the application of security management.

3.2 Security: resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain.

3.3 Security management: systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts there from.

3.4 Security management objective: specific outcome or achievement required of security in order to meet the security management policy.
NOTE: It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.

3.5 Security management policy: overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.

3.6 Security management programmes: the means by which a security management objective is achieved.

3.7 Security management target: specific level of performance required to achieve a security management objective.

3.8 Stakeholder: person or entity having a vested interest in the organization's performance, success or the impact of its activities.
NOTE: Examples include customers, shareholders, financiers, insurers, regulators, statutory bodies, employees, contractors, suppliers, labour organizations, or society.

3.9 Supply chain: the linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user.

3.9.1 Downstream: refers to the actions, processes and movements of the cargo in the supply chain that occur after the cargo leaves the direct operational control of the organization, including but not limited to insurance, finance, data management, and the packing, storing and transferring of cargo.

3.9.2 Upstream: refers to the actions, processes and movements of the cargo in the supply chain that occur before the cargo comes under the direct operational control of the organization. Including but not limited to insurance, finance, data management, and the packing, storing and transferring of cargo.

3.10 Top Management: person or group of people who directs and controls an organization at the highest level.
NOTE: Top management, especially in a large multinational organization, may not be personally involved as described in the Specification; however top management accountability through the chain of command shall be manifest.

3.11 Continual Improvement: recurring process of enhancing the security management system in order to achieve improvements in overall security performance consistent with the organization's security policy.

4. Security management system elements

Figure 2 — Security management system elements

In the paragraphs below a summary of the text included in ISO/PAS 28000 for each of the elements will be provided.

4.1 General requirements

The organization shall establish, document, implement, maintain and continually improve an effective security management system for identifying security risks and controlling and mitigating their consequences.

The organization shall continually improve its effectiveness in accordance with the requirements set out in the whole of Clause 4.

The organization shall define the scope of its security management system. Where an organization chooses to outsource any process that affects conformity with these requirements, the organization shall ensure that such processes are controlled. The necessary controls and responsibilities of such outsourced processes shall be identified within the security management system.

4.2 Security management policy

The organization's top management shall authorize an overall security management policy.

NOTE: Organizations may choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive the security management system (parts of which may be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to its stakeholders and other interested parties.

4.3 Security risk assessment and planning

4.3.1 Security risk assessment

The organization shall establish and maintain procedures for the ongoing identification and assessment of security threats and security management-related threats and risks, and the identification and implementation of necessary management control measures. Security threats and risk identification, assessment and control methods should, as a minimum, be appropriate to the nature and scale of the operations. This assessment shall consider the likelihood of an event and all of its consequences.

4.3.2 Legal, statutory and other security regulatory requirements

The organization shall establish, implement and maintain a procedure to identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks, and to determine how these requirements apply to its security threats and risks.

4.3.3 Security management objectives

The organization shall establish, implement and maintain documented security management objectives at relevant functions and levels within the organization. The objectives shall be derived from and consistent with the policy.

4.3.4 Security management targets

The organization shall establish, implement and maintain documented security management targets appropriate to the needs of the organization. The targets shall be derived from and be consistent with the security management objectives.

4.3.5 Security management programmes

The organization shall establish, implement and maintain security management programmes for achieving its objectives and targets. The programmes shall be optimized and then prioritized, and the organization shall provide for the efficient and cost effective implementation of these programmes.

This shall include documentation which describes the designated responsibility and authority and the means and time-scale by which security management objectives and targets are to be achieved.

The security management programmes shall be reviewed periodically to ensure that they remain effective and consistent with the objectives and targets. Where necessary the programmes shall be amended accordingly.

4.4 Implementation and operation

4.4.1 Structure, authority and responsibilities for security management

The organization shall establish and maintain an organizational structure of roles, responsibilities and authorities, consistent with the achievement of its security management policy, objectives, targets and programmes. These roles, responsibilities and authorities shall be defined, documented and communicated to the individuals responsible for implementation and maintenance. Top management shall provide evidence of its commitment to the development and implementation of the security management system (processes).

4.4.2 Competence, training and awareness

The organization shall ensure that personnel responsible for the design, operation and management of security equipment and processes are suitably qualified in terms of education, training and/or experience.

4.4.3 Communication

The organization shall have procedures for ensuring that pertinent security management information is communicated to and from relevant employees, contractors and other stakeholders. Because of the sensitive nature of certain security related information, due consideration should be given to the sensitivity of information prior to dissemination.

4.4.4 Documentation

The organization shall establish and maintain a security management documentation system. The organization shall determine the security sensitivity of information and shall take steps to prevent unauthorized access.

4.4.5 Document and data control

The organization shall establish and maintain procedures for controlling all documents, data and information required by Clause 4 of this Specification

4.4.6 Operational control

The organization shall identify those operations and activities necessary for achieving:

a) Its security management policy;
b) The control of identified security threats and risks;
c) Compliance with legal, statutory and other regulatory security requirements;
d) Its security management objectives;
e) The delivery of its security management programmes;
f) The required level of supply chain security.

The organization shall ensure these operations and activities are carried out under specified conditions by:

a) Establishing, implementing and maintaining documented procedures to control situations where their absence could lead to failure to achieve the operations and activities;
b) Evaluating any threats posed from upstream supply chain activities and applying controls to mitigate theses impacts to the organization and other downstream supply chain operators;
c) Establishing and maintaining the requirements for goods or services which impact on security and communicating these to suppliers and contractors.

These procedures shall include controls for the design, installation, operation, refurbishment, and modification of security related items of equipment, instrumentation, etc., as appropriate. Where existing arrangements are revised or new arrangements introduced, that could impact on security management operations and activities, the organization shall consider the associated security threats and risks before their implementation.

4.4.7 Emergency preparedness, response and security recovery

The organization shall establish, implement and maintain appropriate plans and procedures to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them. The plans and procedures shall include information on the provision and maintenance of any identified equipment, facilities or services that can be required during or after incidents or emergency situations. The organization shall periodically review the effectiveness of its emergency preparedness, response and security recovery plans and procedures, in particular after the occurrence of incidents or emergency situations caused by security breaches and threats. The organization shall periodically test these procedures where practicable.

4.5 Checking and corrective action

4.5.1 Security performance measurement and monitoring

The organization shall establish and maintain procedures to monitor and measure the performance of its security management system. It shall also establish and maintain procedures to monitor and measure the security performance. The organization shall consider the associated security threats and risks, including potential deterioration mechanisms and their consequences, when setting the frequency for measuring and monitoring the key performance parameters.

4.5.2 System evaluation

The organization shall evaluate security management plans, procedures, and capabilities through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors must be reflected immediately in the procedure(s).

4.5.3 Security-related failures, incidents, non-conformances & corrective/preventive action

The organization shall establish, implement and maintain procedures for defining responsibility and authority for:

a) Evaluating and initiating preventive actions to identify potential failures of security in order that that may be prevented from occurring;
b) The investigation of security-related:
   i) Failures including near misses and false alarms;
   ii) Incidents and emergency situations;
   iii) Non-conformances;
c) Taking action to mitigate any consequences arising from such failures, incidents or non-conformances;
d) The initiation and completion of corrective actions;
e) The confirmation of the effectiveness of corrective actions taken.

These procedures shall require that all proposed corrective and preventive actions are reviewed through the security threat and risk assessment process prior to implementation unless immediate implementation forestalls imminent exposures to life or public safety. Any corrective or preventive action taken to eliminate the causes of actual and potential non-conformances shall be appropriate to the magnitude of the problems and commensurate with the security management-related threats and risks likely to be encountered.

4.5.4 Control of Records

The organization shall establish and maintain records as necessary to demonstrate conformity to the requirements of its security management system and of this standard, and the results achieved. The organization shall establish, implement and maintain a procedure(s) for the identification, storage, protection, retrieval, retention and disposal of records.

4.5.5 Audit

The organization shall establish, implement and maintain a security management audit program and shall insure that audits of the security management system are carried out at planned intervals.

4.6 Management review and continual improvement

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. Reviews shall include assessing opportunities for improvement and the need for changes to the security management system, including the security policy and security objectives and threats and risks. Records of the management reviews shall be retained.

The outputs from management reviews shall include any decisions and actions related to possible changes to security policy, objectives, targets and other elements of the security management system, consistent with the commitment to continual improvement.