SECURITY MANAGEMENT SYSTEMS - SeMS

15 - 19 JULY 2013 • SINGAPORE

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Security Management Systems

Module 2
IATA's SeMS Initiative

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

Although we may sometime refer to "Airlines", concepts and guidance are equally applicable to Airports.

At the end of this module you will be able:

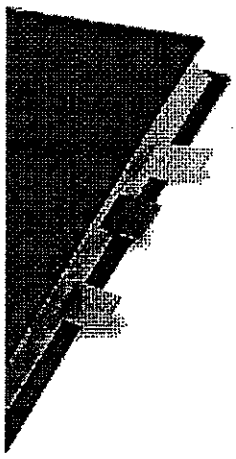
- To understand and describe specific Aviation Security terminology and introduce IATA's initiative & terms of references regarding Security Management System.

Topics covered

- Defining SeMS
- Genesis of SeMS at IATA
- The IATA SeMS Project
- IATA SeMS Guidance Material
- The Way Forward: IATA Integrated Airline Management Systems (I-AMS)
- Challenges

SeMS Definition

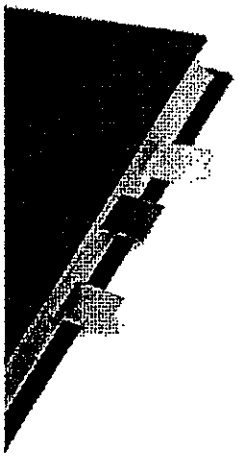
Begin but understand the objective first
/ keep the end in your mind.



- What, in practice, do we mean by "Management" ?
  realizing the question . finding out the goal, use the resource to achieve.
- What, in practice, do we mean by "System" ?
- "Responsibility" vs "Accountability"

change language → problem to solve
⇒ challenge to overcome

SeMS Definition



- "Quality" vs "Security"
- From "Binary" compliance to "Risk/Performance Based" regulations
- "Approved" vs "Accepted"

Re-Thinking Security

Problems with traditional vision of Security:

- Lack of communication and co-operation between stakeholders (especially between Governmental Organizations and Airlines/Airports)
- Security information is Secret & related Risk assessment is mainly carried out by Authorities
- Security viewed as imposed by external parties rather than integral part of aviation
- Focused on meeting minimum requirements
- Reactive

Defining SeMS

SeMS is a standardized approach for implementing the security processes outlined in our air carrier security Programme, SeMS' **business like approach** is helping us integrate security into the culture and guiding principles of our corporation."

Rich Davis, Director, Corporate Security United Airlines

Defining SeMS

"In times of steadily rising real security threats and legal security restraints, SeMS will help in making security processes more effective, proactive and far reaching by promoting a business-like approach to security."

Peter Andres Vice President, Corporate Security
Lufthansa German Airlines

Defining SeMS

"The documented system of an Operator based on threat assessment to ensure security operations consistently fulfill all requirements mandated in the National Civil Aviation Security Programme of the State of the Operator in the most efficient and cost effective manner considering the operational environment of the airline."

IATA Reference Manual for Audit Programmes (IRM)
1nd Edition

Defining SeMS

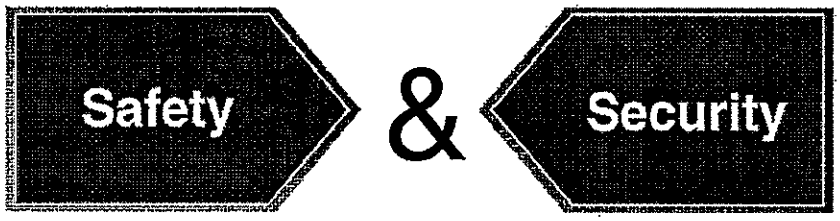
Objective + KPI ⇒ SeMS
(評価対象)
Construction Process

- A performance-based approach to aviation security,
- Based on threat assessment,
- Most efficient, effective and reliable security measures and procedures are implemented in the operational environment, as applicable.

Working Definition
IATA Security Department

Getting the "Picture"

- In many States there is no difference between SAFETY and SECURITY
- A single word may be used for both , so.....



Aviation Security

human element
ergonomics

A combination of measures and resources (human and material) intended to safeguard civil aviation against acts of unlawful interference*

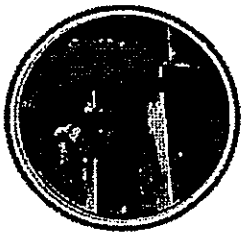
comfortable and natural

*Act or Omissions which may jeopardise or put in danger: passengers, crew, aircrafts or airports

Few examples…

1. **unlawful seizure of aircraft** in flight-on the ground
2. **hostage taking** on board aircraft or on aerodromes
3. **forcible intrusion on board an aircraft, at an airport** or on the premises of an aeronautical facility
4. **introduction on board an aircraft or at an airport of a weapon,** hazardous device, or material intended for criminal purposes
5. **communication of false information** such as to jeopardize the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel, general public at an airport or on the premises of civil aviation facility.

Unfortunately, we also have….



Aircraft as a weapon / Mass destruction

Unruly/Disruptive" Passengers

"MANPADS"

SeMS in summary

- Based on proven Safety

  Management Systems (evolution)

- Safety → Errors
- Security → Violations

} LOSS

Reducing the

SeMS in summary

- Business approach to Security
  - Goals and objectives
  - Processes to attain goals
  - Flexible
- Becomes integral part of the organization
- Whole of Business solutions for security problems, not security solutions alone
- SeMS formalises existing organisation disciplines

Security Management Systems

Module 3

The Management System (MS) in SeMS

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

At the end of this module you will be able to understand and describe :

- specific Aviation Security Management System dimensions,
- Elements of a MS,
- Roles of AVSEC international organizations,
- Aviation Security Measures.

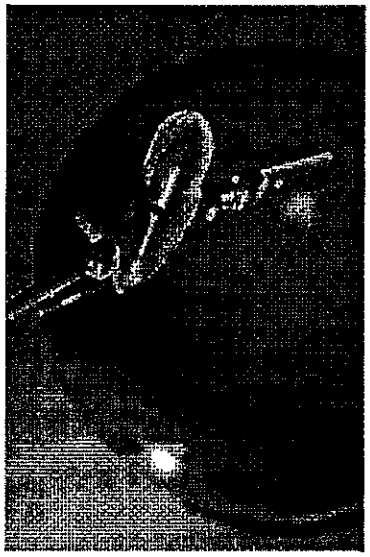
Topics covered

- Aviation: A System of Systems
- 3 Dimensional Management Systems
- Management Systems Elements
- The role of International Organizations
- IOSA's Commitment to Management Systems
- Aviation security measures

Aviation: A System of Systems

System Definition (Compact Oxford Dictionary):

- A set of things working together as a mechanism or interconnecting network
- Computing a group of related hardware units or Programmes or both, especially when dedicated to a single application.
- This is how an airline operates
- An organized scheme or method
- What we need to ensure through Management Systems



Airlines: A System of Systems

An Organizational Management System

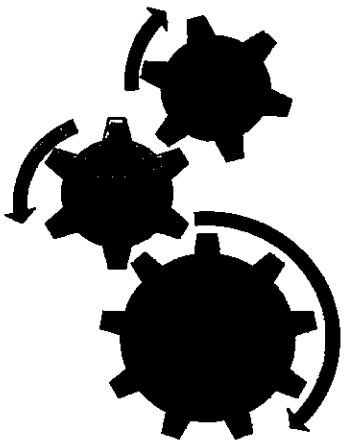
- **Corporate Governance**
- **Strategy**
- **Structure**
- **Systems** (include subsystem)
- **Resources**
- **Capabilities** ① knowledge + practice ② experience

e.g. : 75% manpower use as 100% manpower dynamic routine...

- A Safety Management System
- A Quality Management System
- A Security Management System
- An Enterprise Risk Management System

Aviation: A System of Systems (continue...)

- Documentation Management System
- Flight Operations Management System*
- Cabin Operations Management System*
- Aircraft Maintenance Management System
- Dispatch Management System*
- Cargo Operations Management System
- Ground Handling Management System
- Airside Management System
- Landside Management System



** Airline operations*

Aviation: A System of Systems (continue...)

multi-dusting

Support Systems:

- Personnel Management System
- Supplier Management System
- Financial Management System
- Environmental Management System
- Marketing Management System
- Generally not regulated by the Aviation Authorities, yet essential to Air Carrier operations

3 Dimensional Management Systems

staff arrangement

important

Most Management Systems are 2 dimensional

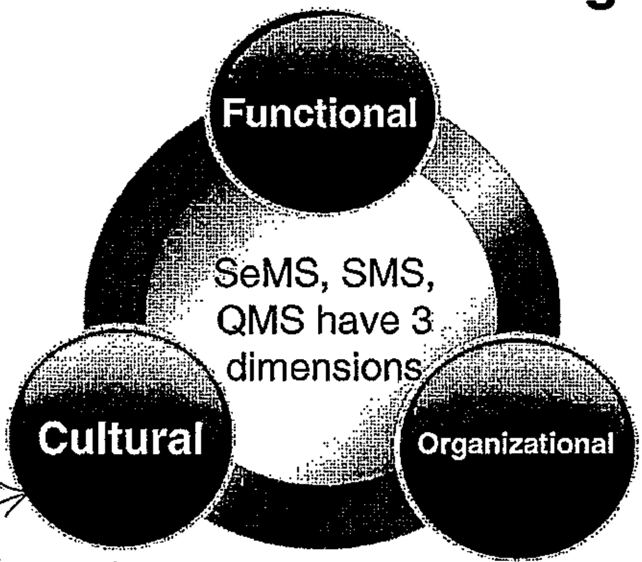
Organizational

- Leadership, team & management staff
- Operational control and supervision
- Resource allocation – people, finance

Functional

- Work process design and documentation
- Technical training
- Control of process & service quality
- Measurement, analysis & evaluation

3 Dimensional Management Systems



Other management system may not have these three elements.

new thing · coorperate

These system work as an one unity

3 Dimensional Management Systems

Organizational

- There is an Accountable Executive
  - CEO/COO
  - No more plausible deniability
- Security Manager (Head of Security)
- Support Staff
- No need to implement a specific organizational model, if the current one..
  - works
  - is clear and concise
  - is GOOD!

3 Dimensional Management Systems

Functional

- Independent of operational functions
- Supports the entire enterprise
- Examples:
  - Crew layover threat assessment
  - Pre-flight security briefing
  - Screener testing with TIPs (at Airport level)

Threat Image Projections

- The Security Department is not on the frontline
  - Under normal operations, it manages Security through oversight of the various systems
  - Centralized control, but decentralized delivery

3 Dimensional Management Systems

Cultural

Skill + knowledge + attitudes
=> training

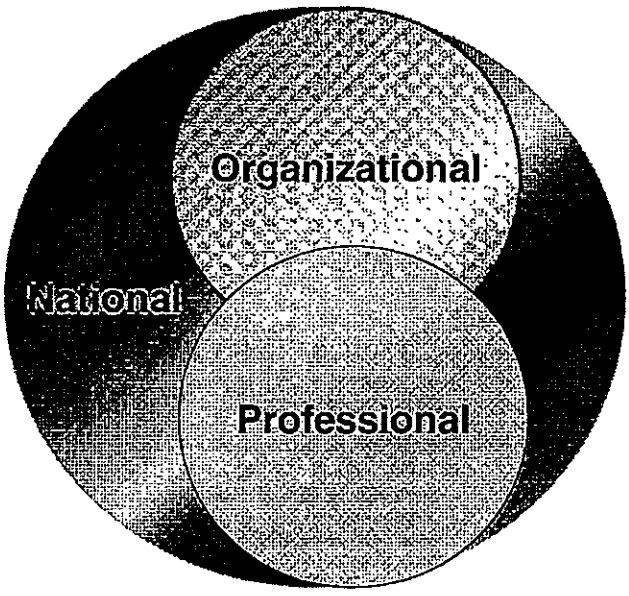
- Each employee must demonstrate:
  - **Healthy Attitudes**
  - **Appropriate Behaviour**
  - **Self-Discipline**
- Each employee must be aware of the current security threat and remain constantly vigilant for potential security lapses and acts of unlawful interference
- Culture IS – **"...the way things are done around here..."** which includes norms, expectations, rules.

3 Dimensional Management Systems

Cultural

- The Challenge is to "convince" line and operational managers that security is part of their responsibilities
- This is achieved by:
  - Training & Education
  - Improvement efforts & Motivation
  - Assigning Security responsibilities in all systems
- Culture cannot be changed quickly, but influenced over time.

Types of Cultures



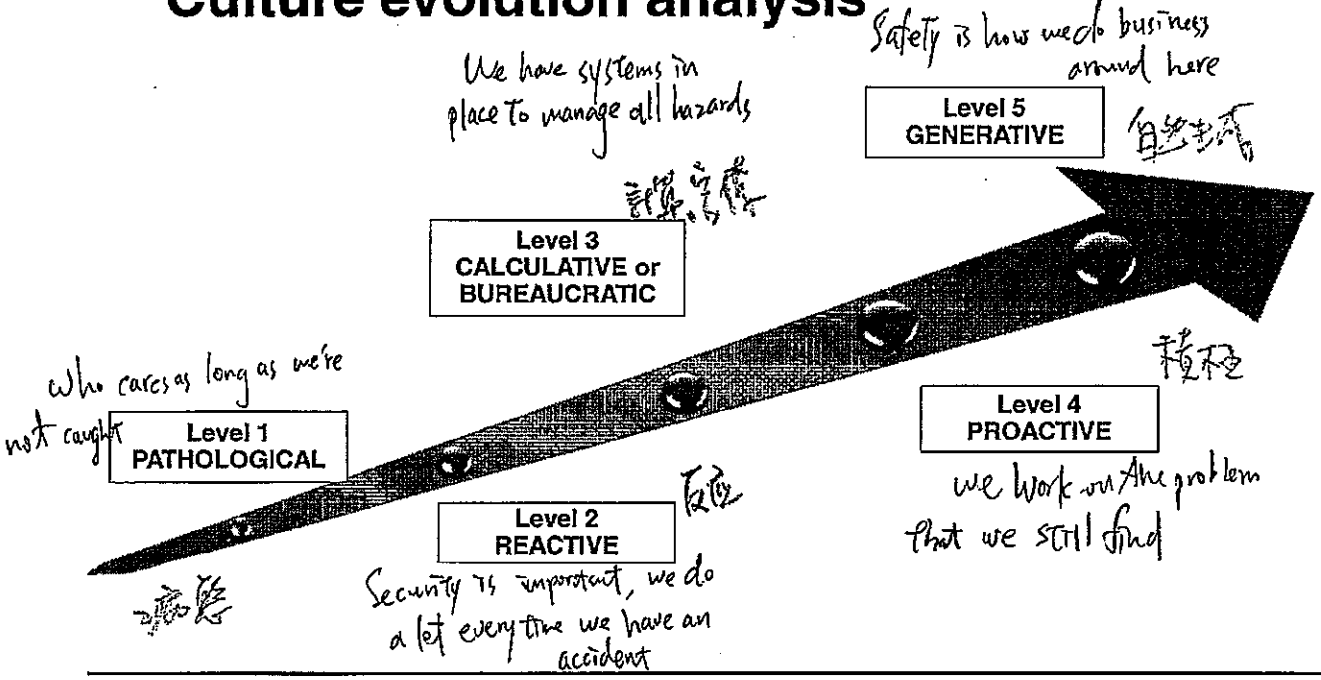
3 Dimensional Management Systems

Culture

Professor James Reason outlines 5 sub-cultures of a Safety Management System, that can equally apply to Security:

- ↗ **Reporting culture**
- ↗ **Just Culture**
- ↗ **Learning culture**
- ↗ **Flexible culture**
- ↗ **Informed culture**

Culture evolution analysis



Possible Outcomes

	Pathological	Bureaucratic	Generative
Information	Hidden	Ignored	Sought
Messengers	Shouted	Tolerated	Trained
Responsibilities	Shirked	Boxed	Shared
Reports	Discouraged	Allowed	Rewarded
Failures	Covered up	Merciful	Scrutinized
New Ideas	Crushed	Problematic	Welcomed
Resulting Organization	Conflicted Organization	Red tape "Organization"	Reliable Organization

3 Dimensional Management Systems

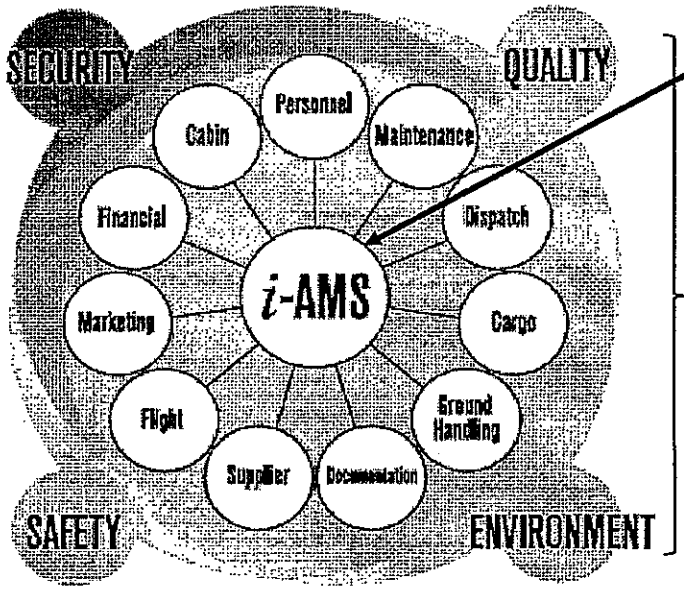
Organizational, Functional and Cultural in AVSEC

- An independent Security organization
  - Separated from other systems
  - Unbiased view
  - Expert view
  - Provide the Security perspective
- It's transforming the Security department from the necessary evil to a core element of the organization

3 Dimensional Management Systems

Emergency Response Planning shall be included in every MS

Risk Mgt

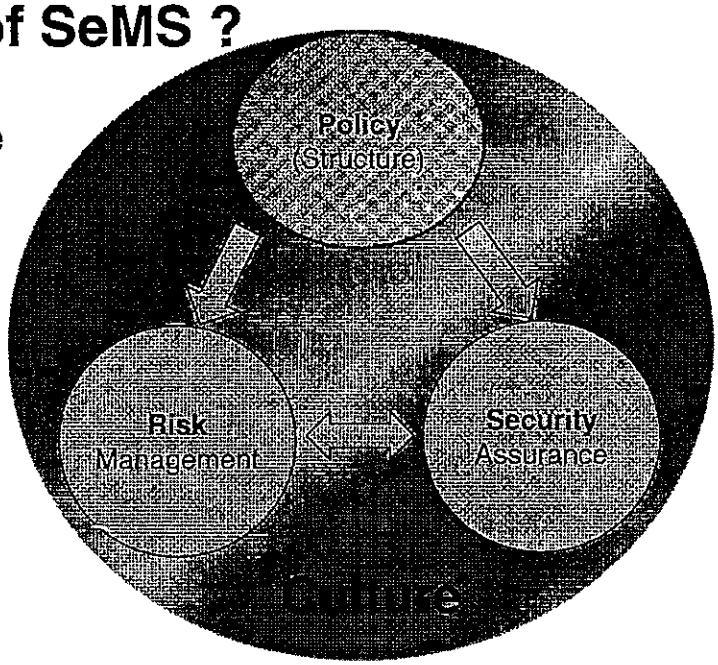


Executive Team
Corporate Governance

Culture

The 4 Pillars of SeMS ?

As for the SMS, we can assume the same for SeMS...



Security Management Systems

Module 4

Building a Security Organization

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

At the end of this module you will be able:

- To understand, describe and plan an Aviation Security organization & the related management.

management commitment
Security structure – department
Selection of personnel
Training/ Security Awareness Train
Communication
Contracted service

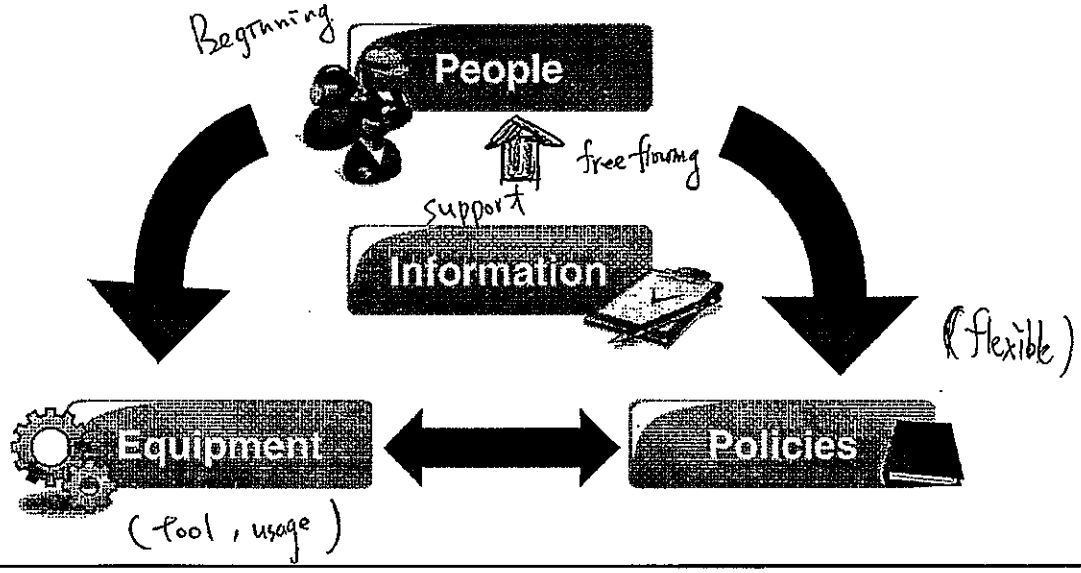
Human Resource Management / Development
→ HRM & HRD

Topics covered

- Introduction
- Executive Commitment to Security
- Head of Security
- Security Department
- Security Staff Selection
- Training
- Security Awareness Training
- Communication
- Contracted Services

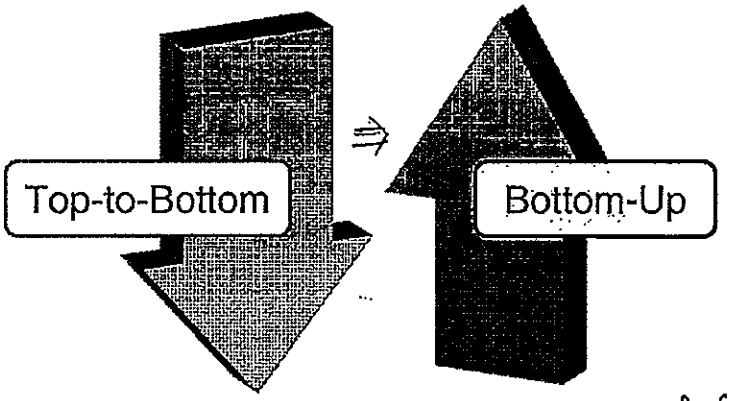
Introduction

The 4 Critical element of Aviation Security



Executive Commitment to Security

SeMS addresses AVSEC both:



start

result: kind of feedback

Bottom-up is a result of a solid Top-to Bottom Commitment

Executive Commitment to Security

Senior Management :

- Is the Accountable Executive for Security
- Establishes the organization's attitude on Security
- Is the Originator of the Security Culture
- Is Responsible to set (approve) the acceptable AVSEC standard

Executive Commitment to Security

Senior Management AVSEC policy content (approved & endorsed by the CEO):

- ☑ The organisation's core values
- ☑ The fundamental beliefs & core elements of the security approach
- ☑ Senior management commitment
- ☑ Security organization
- ☑ Responsibility and accountability of all employees
- ☑ Oversight & Continuous improvement
- ☑ Reporting system and No-Blame policy
- ☑ Clearly communicated expectations & objectives of the security process

Executive Commitment to Security

The Senior Management AVSEC policy must be:

- ↗In line with overall corporate vision and mission
- ↗Put in writing
- ↗Included in the organization's security Programme
- ↗Actively promoted
- ↗Living : Reviewed and updated as necessary !!

↳ continuous changing

Head of Security

Section 1 - ORG 1.1.2 (Organization & Accountability)

Section 8 - SEC 1.1.2

The Operator shall have an appointed Head of Security who has direct access to the highest management level of the company and, regardless of the reporting structure, is responsible for the development, implementation and maintenance of the Security Programme.

IOSA Standards Manual

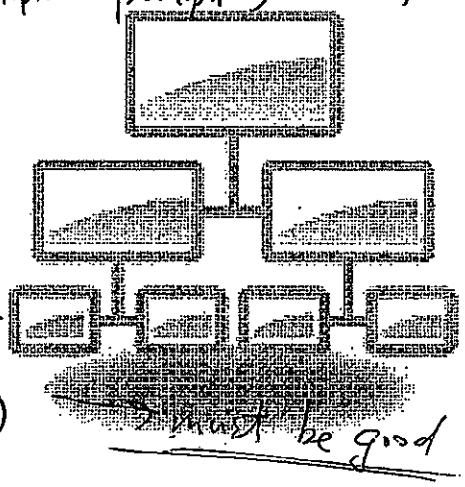
Head of Security

Security is everybody's business

make sure about the information delivery (multiple ways adopt)

Team Leader or Senior Captain*

- Reports directly to Senior Management
  - Security is a core element
  - In times of crisis, communication has to be easy → To realized and operated.
- Knowledge of Aviation Operations or Aviation Security, or both (preferable)
- Respected by all staff
- Clear list of responsibilities



must be good

Head of Security

Key Tasks:

- Formulate overall security strategy & security department structure
  - To be approved by senior management
- Define company-wide security standards (to be approved by the CEO/Senior Executive)
  - Direction for line management
  - Consultation and remediation for line management
  - Promote security culture
- Ensure Security Programme is compliant with national requirements
- Build relationships with regulators, airports and other key stakeholders – ensure high levels of interoperability

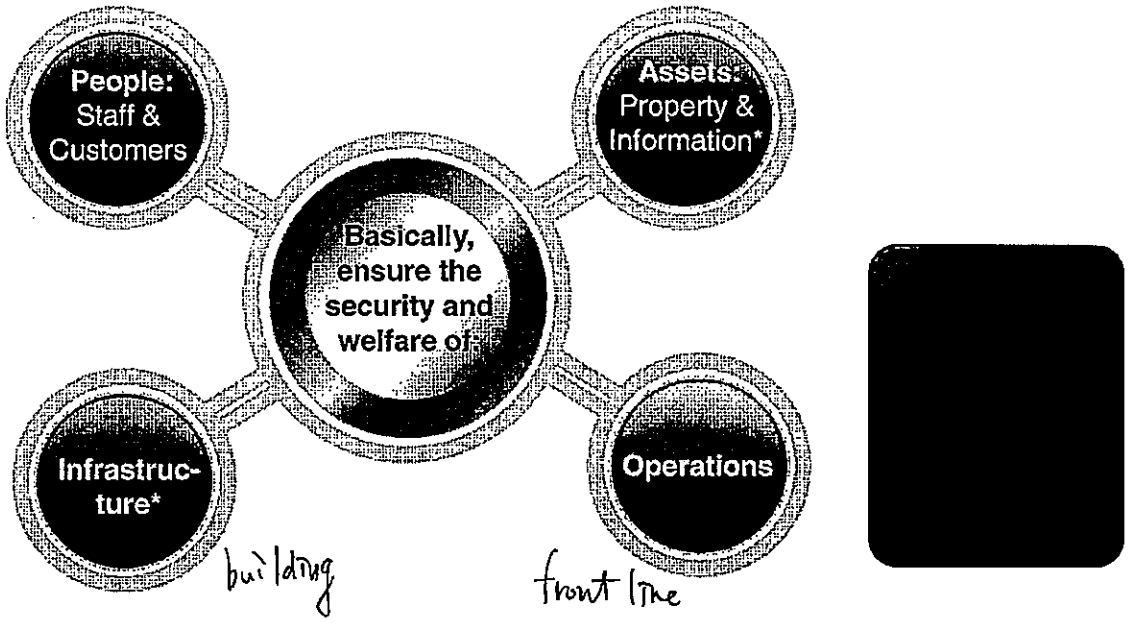
Head of Security

Key Tasks (2):

- Threat Assessment and Risk Management oversight
  - Implement appropriate countermeasures based on risk (the implementation of which shall be approved by senior management)
- Responsible for internal Quality Control mechanisms
- Develop & oversee the security training Programme
- Develop & manage information systems
- Ensure that all contractors have implemented security measures to acceptable standards*

** May be accomplished together with the Quality Management function*

Head of Security



Security Department: Roles and Responsibilities

Supervision

Oversight

- Central of point of delegation & control to decentralized operational delivery
- Information collection, analysis & dissemination
- Based on data gathered, establish and/or review the security policy
- Policy dissemination

  How to manage the information

  - **Consider Security Sensitive Information (SSI)**
- Training to comply with policy
- Promote the Security Culture

Security Department: Considerations

definition, no overlap responsibility

Clear terms of reference based on the responsibilities of the Head of Security

- Clear Command structure
- Line Management-Security Department relationship clearly established and understood
  - Cross-functionality is the key
- Relationship with all departments of the organization
- Support for home based and foreign stations
- Security can be delivered by different people from different departments undertaking different roles

Security Department

Organizational Chart Guidelines

- Direct reporting line between Head of Security and Senior Management
- Departmental/line managers should report to the Head of Security
- Staffing volume and job description must account for times of crisis. Consider:
  - Specific responsibilities
  - Appropriate workload
  - ERP (Contingency Plan) Organizational Chart

enterprise resource planning.

Security Department

Organizational Chart Guidelines

- Non-operational but critical elements must be considered
  - "Dotted line" in or out of Security Department

These include:

- Risk Management
- Training
- Communication
- Quality
- Emergency Management
- Others

Security Staff Selection

a lot of skill to select a Security staff and make them fit

Not always the Security Department's responsibility, however:

- Final say on who is selected, generally rests with the Head of the Security Department (Direct report)
- Security staff are on the frontline ensuring protection of Staff, Customers and Property
- Hiring the wrong people is expensive

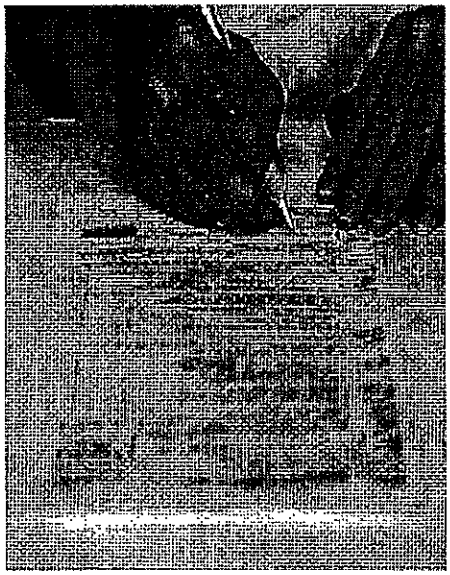
tell the reality to test their honesty

- You need to understand the process, be part of it!

Security Staff Selection

Selection Process Elements

- Job Description
- Candidate Selection/Interview
- Background Check
- Performance Appraisal



Security Staff Selection

Job Description

- Every position needs a regularly updated job description
- Proper job description will attract suitable candidates
- The elements of a good job description:
  - Summary of the job
  - List of duties
  - Overview of reporting structure
  - Required qualification for the positions
  - Training and experience required
- **Management job descriptions must be in SeMS**

Security Management Systems - SeMS

Module 5
Human Factor

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

At the end of this module you will be able:

- To understand and describe Human Performance and Limitations, and how they can affect Aviation Security.

Topics covered

- Fundamentals of Human Factors
- Human Factors Management
- Ergonomics
- Resource Management
- SHELL Model

Fundamentals of Human Factors

- ICAO Annex 17 Definitions
- **Human Factors principles.** Principles which apply to design, certification, training, operations and maintenance and which seek safe interface between the human and other system components by proper consideration to human performance.
- **Human performance.** Human capabilities and limitations which have an impact on the safety, security and efficiency of aeronautical operations.

Fundamentals of Human Factors

- Human Factors help determine the limitations of human performance
- Helps manage human error in Security
  - Reduce the likelihood
  - Reduce the consequence (impact)
- Helps improve efficiency
- Look at humans in an interactive role with its surroundings
  - E.g. ground handling shift workers – fatigue, weather, equipment

tiredness

Human Factors Management

Ensuring Human Factors are considered to:

- Define Safety / Security Regulations
- Integrate Human Factors knowledge in the design and certification process of equipment (such as in security screening)
- Consider Human factors when designing the infrastructure
- Develop and define procedures designed to enhance error resilience
- Provide guidance for selection, training and assessment, and performance management

Resource Management

Roster/Shift Management

- Roster rotation needs to be carefully designed to avoid "quick returns"
- Quick rotation to avoid multiple consecutive night shifts
- Duty Periods limited to 8 hours x day
- Consider high throughput periods – peak screening: oversight Security Contractor rosters
- Task Rotation
- Rest periods during duty periods

Resource Management

Roster/Shift Management

- Provide adequate rest facilities
- Consideration of commuting times
- Give some choice to your staff based on preference

not bias, but specific

Resource Management

Performance Management

- Individual Performance
- Team resource management
  - Commitment, communication and co-operation
  - Team performance evaluation
- Effectiveness (Threat detection)
- Efficiency (Time)

Resource Management

Team resource management

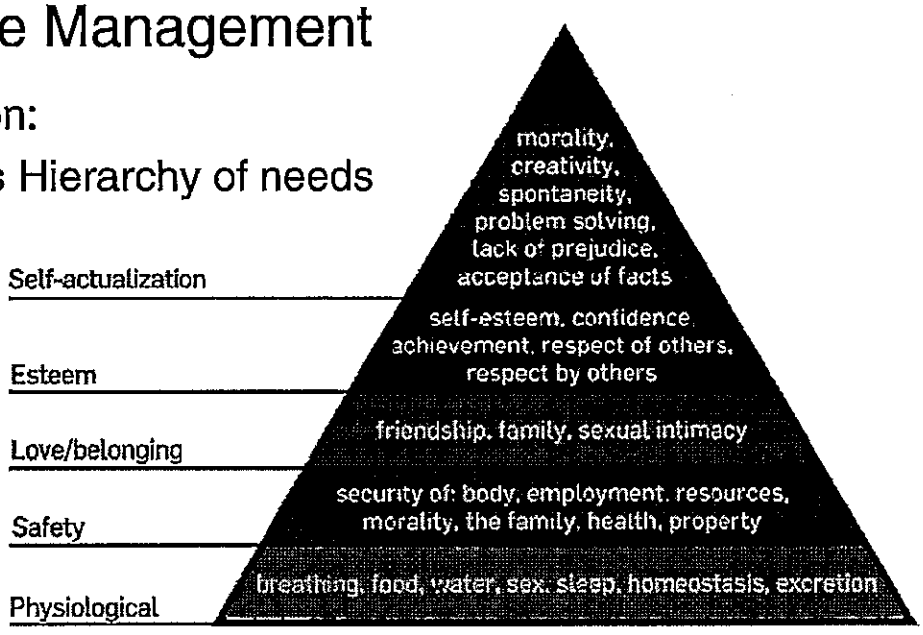
- Many security functions are based on teamwork
  - Staff rotation
  - Division of responsibility
- Hire team players (commitment)
- Train teams instead of individuals
  - Confidence of peers
  - Team problem solving attitude
- Manage & Evaluate the team
- Don't forget: a team is made up of individuals
  - With different styles

Resource Management

- **Motivation**
- **Some formulas...**
  - **Performance** = Capability x Motivation
  - **Capability** = Skill x Knowledge x Resources
  - **Motivation** = Personal Factors x Information x Rewards (includes Bonuses) x Type of Job x Discretionary Power

Resource Management

- Motivation:
- Maslow's Hierarchy of needs



Herzberg's Motivators and Hygiene Factors

Factors for Satisfaction	Factors for Dissatisfaction
Achievement	Company Policies
Recognition	Supervision
The work itself	Relationship with Supervisor and Peers
Responsibility	Work conditions
Advancement	Salary
Growth	Status
	Security

- Job satisfaction and job dissatisfaction are not opposites.
  - The opposite of *Satisfaction is No Satisfaction.*
  - The opposite of *Dissatisfaction is No Dissatisfaction.*

Step 1: Eliminate Job Dissatisfaction

Herzberg called the causes of dissatisfaction "Hygiene factors". To get rid of them, you need to:

- Fix poor and obstructive company policies.
- Provide effective, supportive and non-intrusive supervision.
- Create and support a culture of respect and dignity for all team members.
- Ensure that wages are competitive.
- Build job status by providing meaningful work for all positions.
- Provide job safety & security.

Step 2: Create Conditions for Job Satisfaction

To create satisfaction, motivating factors associated with work ("job enrichment") shall be address. Every job should be examined to determine how it could be made better and more satisfying to the person doing the work. Things to consider include:

- Providing opportunities for achievement.
- Recognizing workers' contributions.
- Creating work that is rewarding and that matches the skills and abilities of the worker.
- Giving as much responsibility to each team member as possible.
- Providing opportunities to advance in the company through internal promotions.
- Offering training and development opportunities, to become a more knowledgeable professional and be a "Better Person".

Resource Management

Motivation in practice

- Acknowledgement and rewarding of outstanding performance
- Attractiveness of the job
- Fairness
- Opportunity to advance and get promoted
- Advance training to facilitate promotion
- Appropriate remuneration
- Financial rewards for consistent achievements
- Delegate other tasks
  - Security awareness session
  - Job rotation increases interest

Resource Management

Motivation in practice

- Team meetings – allow members to express to voice their views
- Provide transportation, car parking
- Take into account commuting time/costs
- Reasonably priced dining arrangements
- Well-tailored uniform
- Badge or medals for superior achievement
- Make security more visible
  - Workplace inspection and ID Checks

Resource Management

Staff Retention

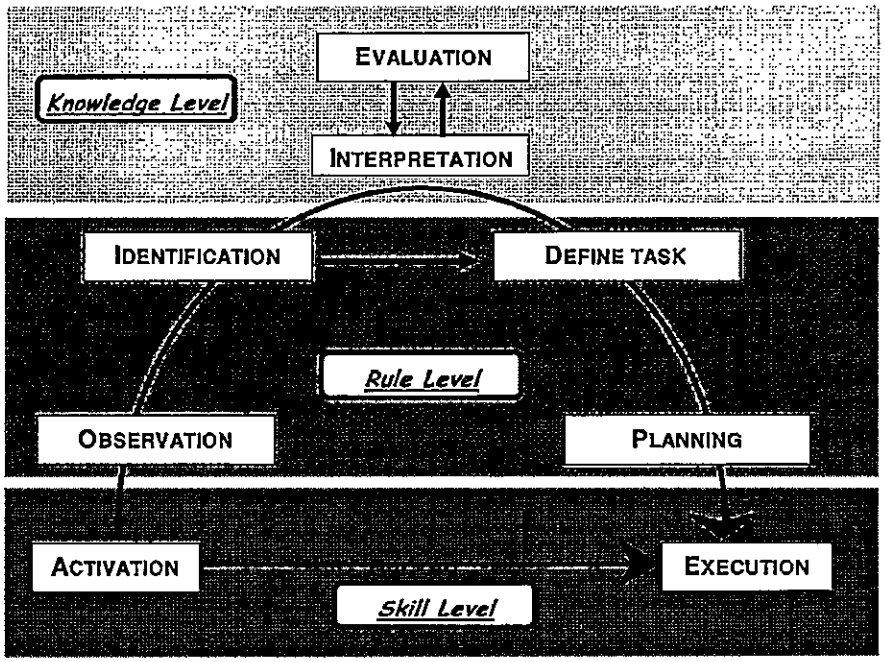
- Motivated staff will be less tempted to leave
- Experience staff performs better
- Recruitment and training is more expensive than giving a high performing screener a raise
- Important indirect costs:
  - All those trained to be security personnel will have had access to security sensitive information
  - Ensure proper termination processes
- Reality: best people will leave

Resource Management : Human Error

- Human error may be defined on basis of 3 dimensions:
  - **Skill based behaviour** (routine tasks requiring little attention and allow other tasks to be performed simultaneously),
  - **Rule based behaviour** : normal activities requiring decision making,
  - **Knowledge based behaviour:** problem solving required and solution not yet known.

J. Rasmussen 1983

Error Dimensions



J. Reason, 1990

Security Management Systems

Module 7

Integrated Risk Management

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

At the end of this module you will be able:

- To understand and describe principles & benefits of Integrated Risk Management, which means integrating in a unique assessment all risk facing a company/operator.

Topics covered

- Review what Is Risk Management?
- What Is Integrated Risk Management (IRM)?
- What are the Benefits?
- A Few Certainties about Risk Management
- Operational Risk vs. Enterprise Wide Risk
- Integrated Risk Management Guiding Principles
- Next Steps

Review: What Is Risk Management?

- A process that identifies a company's risk exposures and seeks to minimize risk levels
- Integral part of organizational processes
- A Critical component of SeMS
  - Threat Assessment drives all hazards approach
  - Risk Management balances risk and opportunity
- Informed decision making
- Explicitly addresses uncertainty
- Systematic, structured and timely process

Review: What Is Risk Management?

- Based on best available information
- Takes human and cultural factors in
- Transparent and inclusive
- Dynamic and iterative
- Facilitates continual improvement
- It is NOT the purchase of insurance – that is only one way to finance a company's risk exposure

Why is important & How is Linked to Corporate Governance?

- Board must generally manage the risks of company
- Corporate governance laws now:
  - Requires board to identify risks and implement systems to manage them, and
  - Require review of adequacy and integrity of company's internal control systems.
- Risk management disciplines support Governance
- Compliance systems need to be integrated with Governance and Risk Management

Who are the Stakeholders?

- Board of Directors
- Shareholders
- Regulators
- Customers
- Employees
- Sub-Contractors
- Rating Agencies
- Media

What are the Benefits?

- Creates Value:
  - Make consistent and informed decisions across the company
  - Meet stakeholder objectives
  - Support overall strategic direction
  - Maximize opportunities*
  - Reduce losses to all assets
  - Reduce insurance premiums
  - Reduce overall operating cost
  - Protect your bottom line
  - Safeguard your reputation, brand

A Few Certainties about Risk Management

- Risk is the chance of something happening that impacts organizational objectives
- Hazards and threats can create risks – and both can lead to losses
- No one airline/airport risk management approach is the same as another, nor should it be
- Foreseeable risks must be identified

A Few Certainties about Risk Management

- If a significant risk is foreseeable but it is not reported, it is a severe managerial error,
- The aim is that there should be no surprises,
- Don't replace one risk with a risk of another kind,
- The greatest risk in business is to take no risk at all.

identifying wrongly

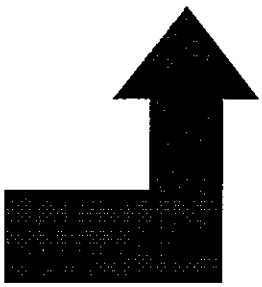
What Is Integrated Risk Management?

- Managing risk across the entire company
- Applying principles both vertically and horizontally in a company
  - Cross functionality is critical
- Establishing a company-wide culture of risk management
- Aligning risk appetite with company strategy – tolerance levels need to be established
- Keep it simple

Airline Integrated Risk Management

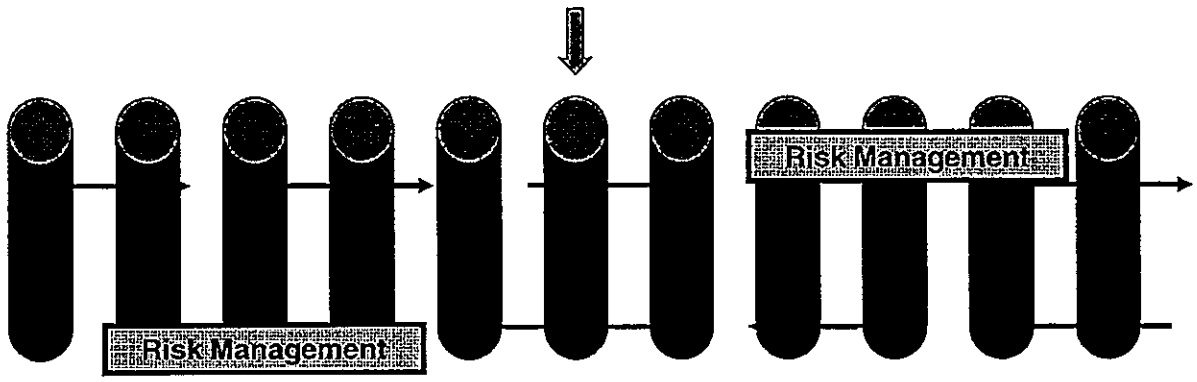
Principal Risk Exposure Areas

Financial	Legal/Compliance	Strategic	Reputation	**Operational**



- **Operational risk exposure** is a key component of an airline's overall exposure
- **This is our focus**

Integrated Risk Management/IRM



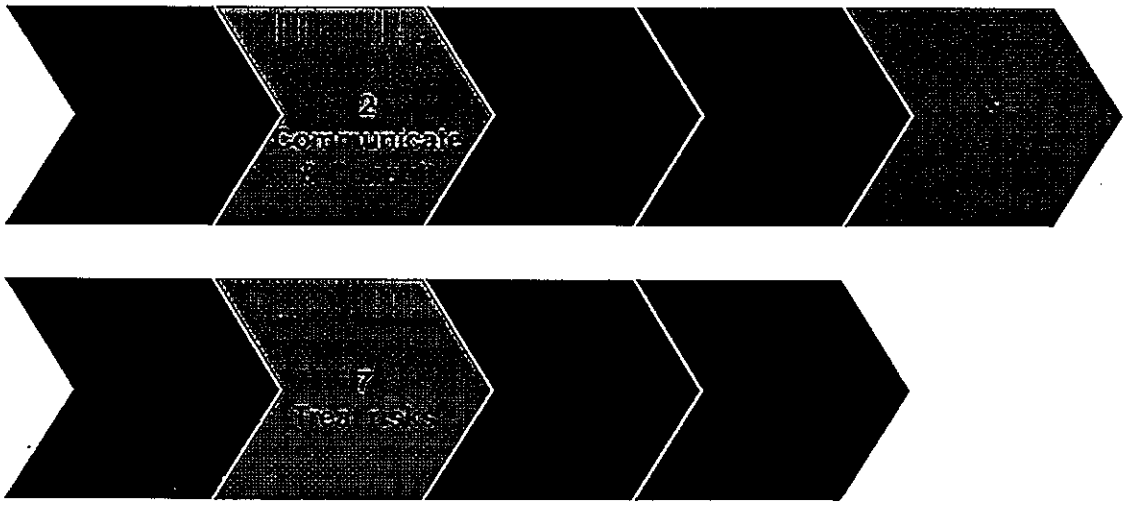
Operational Risk

- Airlines/airports focus on Operational risks due to the hazardous nature of operations
- Operational risk is a component of company's overall, or enterprise wide risk
- Security is a component of operational risk, as is flight ops and safety, etc.
- Management systems are in place, e.g. SeMS, QMS, SMS, but not fully integrated

IRM Process

- ISO 31000 – new International Standard – common framework, methodology & language
- Establish Risk Management Framework
- Communicate and consult
- Establish the Contexts
- Identify risks
- Analyze risks
- Evaluate risks
- Treat risks
- Monitor & review

Risk Management Process



IRM Step 1

Risk Management Framework

- Begin at the Top
  - Board must be engaged and promote it
  - Establish risk appetite, priorities, objectives, risk model
  - Link with business/ corporate strategy
  - Senior management must set tone & direction of the IRM Programme
  - Establish Risk Management Committee
  - Define and communicate roles and responsibilities
  - Identify Risk Champions – each department

IRM Step 1

- Definitions & Roles
- Chief Risk Officer
- Risk Management Committee
- Risk Champion Method
- Risk Owner Job
- Centralized control (policy, process, framework) but decentralized operations

IRM Step 2 – Communicate & Consult

- Involve all stakeholders – internal and external
- Use many mediums – email, document, poster
- Engage those most likely to contribute – 'Risk Champions' in each Department
- Establish committees
- Meet and discuss regularly
- Communications plan essential

IRM Step 3 – Establish the Contexts

- What are the external and internal environments the organization operates in
- What are the hazards and potential risks that would impact an organization's objectives
- How does the organization deliver risk management
- What levels of risk is the company prepared to accept when balanced with opportunity?

Security Management Systems

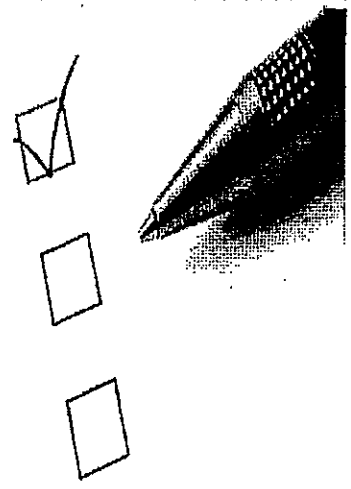
Module 9

Quality Assurance of SeMS

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module Objective



At the end of this module you will be able to understand and describe:

- What is Quality Assurance
- Goals of Quality Assurance
- The Quality Management System, as a mean of Quality Assurance
- The sharing of responsibilities within an Operator as far as QC is concerned

Topics covered

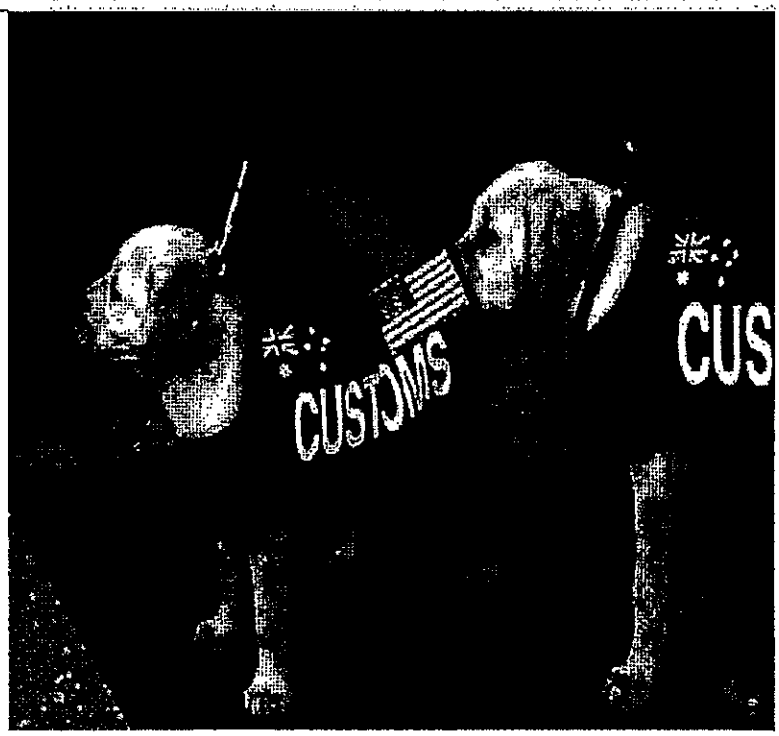
- Background
- Quality Assurance
- Quality Management System
- Security Audits and Inspections

Background

- Operational compliance must be looked at from an organizational point of view
- Quality Assurance is an internal independent assessment
  - Corporate Quality Assurance function is independent of the Quality Control responsibilities
- Quality Assurance verifies compliance on behalf of the accountable executive
  - All the technical components are audited (measures, training, quality control, etc.)
- Basically, it provides a solution to the question:

Background

How do you control your Quality Control mechanisms?



Quality Assurance

- Establish a dedicated Quality department
- The Quality department is "operationally independent" to ensure that auditors remain objective and immune from bias due to conflicting responsibilities
- The Quality department looks at all operations, not just AVSEC.

Quality Assurance (QA)

- Quality Assurance programme
- Appointment of a highly qualified manager to oversee the program
- Operational independence of the quality assurance function and staff
- Documented operational manager responsibility to implement corrective actions
- Design lines of communication and reporting to senior management
- QA is a part of the organizational Quality Management System

Quality Management Systems

- Elements of QMS
  - Organizational structure
  - Accountabilities
  - Corporate resources
  - Processes and Procedures
  - Under senior management control
    - It is a 3 dimensional system

Quality Management Systems

- Objectives of QMS
- Continuous improvement
- Proactively enhance Security through the organization
- Different toolkit than SeMS
- Complimentary to SeMS and strives to achieve the same goal
  - An acceptable level of operational security
- Reduces redundancy in Quality Assurance mechanisms.

Quality Management Systems

- Objectives of QMS
- Identify weaknesses in
  - Management system
  - Corporate documentation
  - Processes
  - Operational procedures
  - Employee training
- SeMS - QMS partnership
  - Level of integration will vary based on organizational structure

Quality Management System

Why?

- Central component to ensure regulatory compliance
- Senior Management drives the message to division head to comply with regulation
  - Senior management is ultimately accountable
    - Ensure procedures are documented
    - Error proofs processes and procedures for all staff to comply
- Verifies a specific system operates as desired in the organization

Quality Management System

Why?

- QMS process is auditing
- Many types of audits within QMS:
  - Compliance audit (with regulators and internal procedures)
  - Product quality audit
  - Service quality audit
  - Process audit
  - System audit (management system)

EXAMPLE

Responsibilities of Airline's Managers, regarding Security Compliance

All PHs

- Entire OPS**
- Annex 6
- Annex 17

SAFETY Mngr

- AP&FSP*
- Reporting Sys.

SECURITY Mngr

- Annex 17
- Doc 8973
- OPS**-Subpart S
- Annex 6 - Chpt. 13

EXAMPLE: Allocation of Specific responsibilities from Annex 6 - Ch 13*

PHs

Flight Ops, Maint., GND Ops

- All requirements, as applicable
- Training of own personnel
- Implementation of security measures
- *Design of measures in cooperation with Sec Manager*

PH- Crew Training

- Organisation of security Training with AA-Certified AVSEC Instructors
- Logistic
- Training documentation management

SECURITY**

- Security Program/Manual + Validation from AA
- Security Training Program + Approval from AA
- Design Security Check-Lists/Measures & Procedures together with relevant PHs
- Company-ASQCP

Company - ASQCP

Activities on Company Service Providers/Suppliers

- **Performed by : Quality Mngr / PHs**
- **Type of control:** Provider/Supplier management of security documentation and security training ***("Administrative Control")***, such as checking if the provider has :
  - **a Security Program** (which shall include Security Organization, Security Measures, Training Programs, Internal ASQCP) Validated by the AA;
  - **Certifications/qualifications** for its Staff as required by norms or regulations;
  - **Evidences** of performed training.

Company - ASQCP

SECURITY Manager* Specific responsibilities:

- Accountable to the A.A. for the correct implementation of security measures and thus responsible to manage the Company ASQCP (which is part of the Security Manual)
- **To develop check-lists for Quality Control activities**
- **To conduct Audits, Inspections, Investigations & Tests** on Company Service Providers/Suppliers and over all areas of the **Company** to verify the correct implementation of security measures (***"Technical Control"***)
- **"VISITs"** (if and/or how Authorized by the AA/Airport Authority) to verify the correct implementation of security measures at the airport.

How & When

Carried out as specified in the Company-ASQCP with related CHECK-LISTS, when..

- Foreseen by the Yearly Plan,
- Opening a New Destinations,
- Reports show significant NON-Conformities
- .....

Summary

1. **Audits**
2. **Inspections**
3. **Tests**

Carried out by the A.A. and/or, **internally**, by the Company (also including Providers/Suppliers)

4. **Surveys**
5. **Exercises**
6. **Investigations**

Carried out by the A.A. and/or, **internally**, by the Company (also including , providers/suppliers) if/when required

7. **«Visits»***

Carried out by the Company at the Airport to "**observe**" Screening, Access Control Activities, Apt surveillance, etc.*

8. **Observations**
9. **Interviews**
10. **Documentation Review**

Quality Control "TOOLS"

Evaluation*

Classification of Compliance	Security audit	Inspection	Test (1)
1 - Fully compliant	✓	✓	✓
2 - Compliant, but improvement desirable	✓	✓	✓
3 - Not compliant (minor deficiencies only)	✓	✓	✓
4 - Not compliant - Serious deficiencies	✓	✓	✓
N/A - Not applicable	✓	✓	
N/C - Not confirmed	✓	✓	✓

(1) TESTs can **only** be performed by the A.A.
The Company may perform Tests only INTERNALLY; if carried out on Providers/Suppliers, it must be formally provided for by agreement/contract.

Summary of QC responsibilities

1. **Security Manager** (also qualified as Security Auditor*)
"Technical Control" of Security Measures on…
   - Company Departments, Company Procedures, Company Providers/Suppliers, Airports
2. **Quality Manager***
"Administrative Control/ Document Management" on…
   - Security Manager
   - PHs Position Holder
   - Providers/Suppliers

Follow-up of Security Non-Conformities raised by the Security Manager

- **Internal Management** of ***FINDINGS*** (to be applied also to Providers/Suppliers through related PHs) > **Corrective ACTIONS: are obligations** since the Security Manager is accountable to the AA for the correct implementation of security measures within the company.
- **With Airport Administrator/Airport Authority** > Highlight the NEGATIVE impact on company operations of possible security incidents/accidents as a result (probably) of security measures not in place or not in compliance with requirements.
- NON-Conformities raised up by the **Quality Manager** shall be jointly managed by all relevant PHs and the Security Manager.

Module summary exercise

- Understand what is Quality Assurance
- Understand goals of Quality Assurance
- Quality Management System as a mean of Quality Assurance
- Sharing of responsibilities within an Operator as far as QC is concerned

Questions?

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Security Management Systems

Module 10

IATA Operational Safety Audit (IOSA)

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

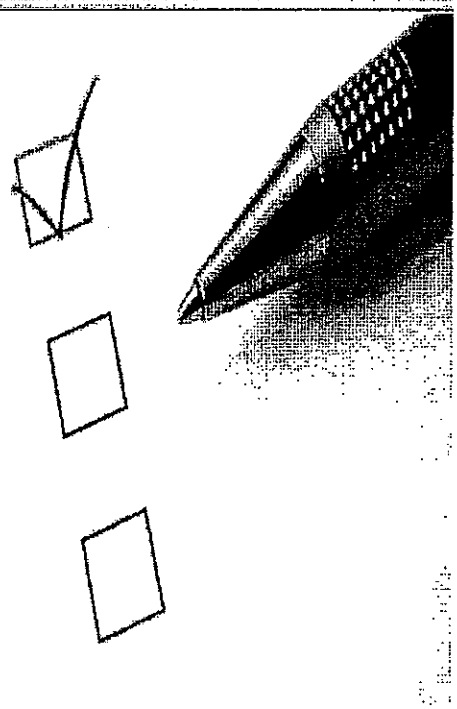
At the end of this module you will be able to understand & describe:

- IOSA
- The objectives of the IOSA Programme
- The root of IOSA Security Provisions
- The IOSA audit process
- The importance of IOSA for SeMS.

Topics covered

- Overview of IOSA
- IOSA Reference Manuals
- IOSA audit process
- IOSA as a Security audit
- The Role of IOSA in SeMS

Session Outline



- Overview of IOSA
- IOSA Reference Manuals
- IOSA audit process
- IOSA as a Security audit
- The Role of IOSA in SeMS

Overview of IOSA

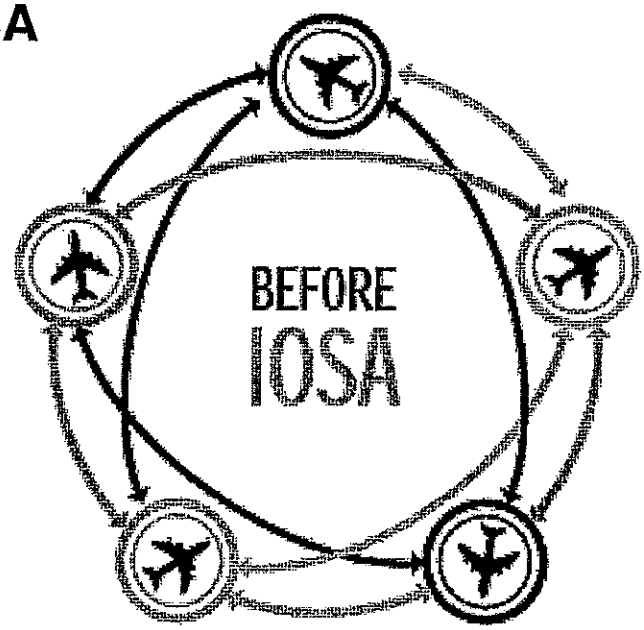
- IOSA aims to provide a standardized audit program of the operational management and control systems of an airline that is based on internationally-recognized standards and supported by a rigorous quality assurance process
- Recognized by:
  - ICAO
  - US FAA
  - Junta de Areonáutica Civil (Chile)
  - Mexican DGAC
  - CAAC (China)
  - Many others
- Can be used by Airports and Civil Aviation

Overview of IOSA

- Implementation and international acceptance of IOSA - Airlines and Regulators achievements:
  - Establishment of the first internationally recognized operational audit standards
  - Reduction of costs and audit resource requirements for airlines and regulators
  - Quality audit program under the continuing assistance of IATA
  - Structured audit methodology, including standardized checklists
  - Elimination of audit redundancy through mutual acceptance of audit reports.

Overview of IOSA

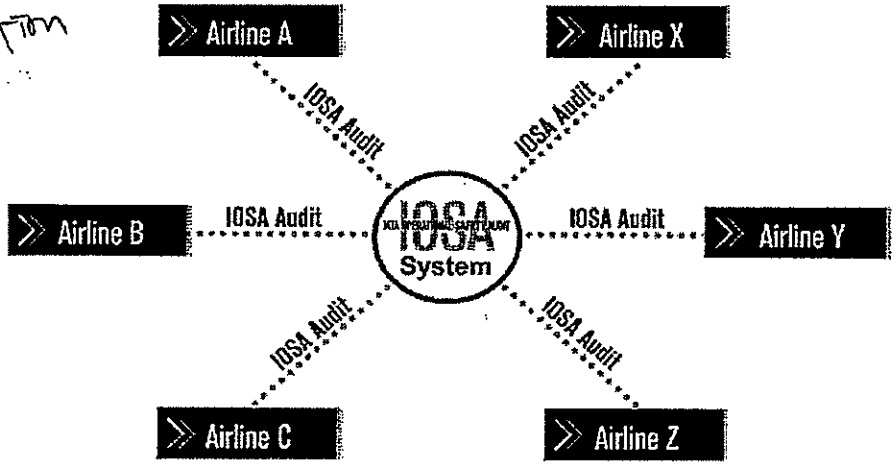
- OLD Audit Mode



Overview of IOSA

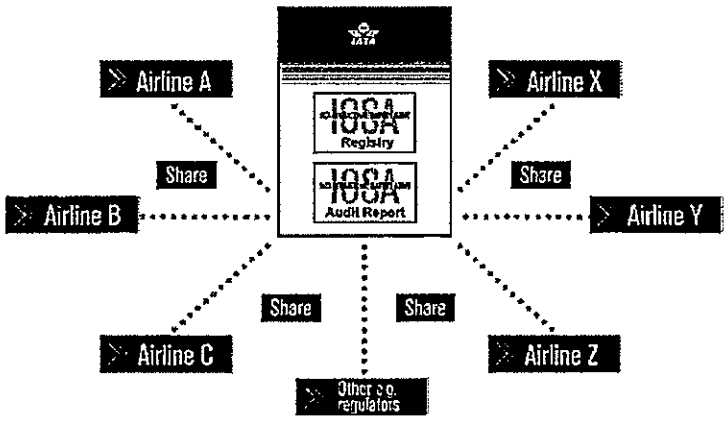
- NEW Audit Model
- One Audit per Airline (***24-month Interval***): renewal process usually activated 4 months before expiry.

Certification



Overview of IOSA

- **NEW Audit Sharing Model**
- If airline agrees, **audit** can be released to other airlines.



Overview of IOSA

IATA behaves as a Quality Association

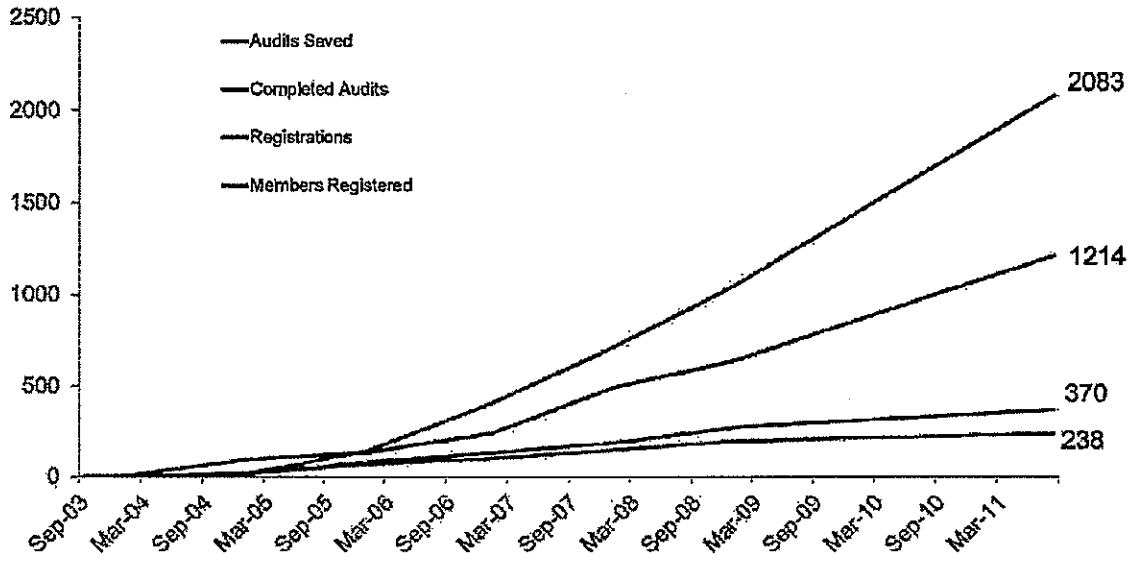
- Any airline wanting to join IATA must pass an IOSA audit first (cost: ~ US $ 40,000)
- All existing Members had to:
  - Commit to an IOSA audit by end 2006
  - Carry out their IOSA audit by end 2007
  - Close all Corrective Actions (generated by "findings") and be Registered by end 2008
  - Maintain IOSA Registration by being successfully audited biennially thereafter.

Overview of IOSA

IOSA Progress

- 100% of IATA Members have done an IOSA audit
  - Almost 30% of all audits are on non-IATA members
- Over 700 audits conducted
- IOSA Standards Manual Edition 4, Revision 1 released July 2011 - effective 1 December 2011
- IOSA Standards Manual Edition 6, effective 1 September 2012
- IATA is making a difference to Safety & Security

Programme Status September 2011



IOSA Reference Manuals

- IOSA Program Manual (IPM) - 5th Edition
- IOSA Standard Manual (ISM) - 5th Edition
- IOSA Reference Manual for Audit Programs (IRM) - 2nd Edition
- IOSA Standard Manual - 5th Edition - Check Lists
- ISAGO* Standard Manual - 2nd Edition
- ISAGO* Q5 Auditee Manual - 2nd Edition
- Electronic document, available free for download (***http://www.iata.org/ps/certification/iosa/index.htm***)

IOSA Standards Manual 4th Edition

- More focus on SMS: 6 new provisions on SMS bringing the total to 68
- Released July 2011 - Effective 1 December 2011
- 9 new standards
- 3 new recommended practices

IOSA Standards Manual – 5th Edition

Effective April 2012 with following changes:

- Rewording of text in some provision.
- New provision incorporating the IOSA Standards Special Review process with the IOSA Change Management process.
- New provision associating the Correlation of specifications with data from industry accidents and incidents with the IOSA Change Management process.
- Incorporation of the IPM Ed. 4 Temporary Revision 1 provision.
- New flow Chart: "IOSA Standards Accident-Incident Correlation Process Flow"

IOSA Audit Process

Process to become an IOSA registered airline

- IOSA standards Integration
  - Download IOSA Standards Manual and Checklist and review compliance
- **Audit Organization (AO)*** Integration
  - Contact an AO to schedule an Audit (~ 8 AOs certified by IATA)
- Contract Signing
  - Get a contract signed (Operator, IOSA, AO)
- IOSA Audit Hosting
  - Conduct audit (approx. 25 on site man-days)
- Corrective Action Phase
  - 12 Months to close all findings, then AO recommends for registration
- IOSA Registration (***www.iata.org/registry***)
  - Valid for 2 years

IOSA Audit Process

- **STANDARDS** always contain the word "shall" (e.g. The Operator shall ensure..) in order to denote an IOSA requirement.
  - The Operator must ("Shall") conform with all these standards to attain IOSA registration
- **RECOMMENDED PRACTICES** always contain the word "should" (e.g. The Operator should have...) and are considered under IOSA as operationally desirable or highly recommended.
  - Conformity is optional ("Should") by the Operator.

IOSA Audit Process

- To determine conformity with any standard or recommended practice, the IOSA Auditor will assess the degree to which specifications are documented and implemented by the operator
  - **Documented**
  - **Implemented**

IOSA Audit Process

Audit Scope

- **Section 1:** Organization & Management System
- **Section 2:** Flight Operations
- **Section 3:** Operational Control/Flight Dispatch
- **Section 4:** Engineering & Maintenance
- **Section 5:** Cabin Operations
- **Section 6:** Ground Handling
- **Section 7:** Cargo Operations
- **Section 8: Operational Security**

Still, separated.

IOSA as a Security Audit

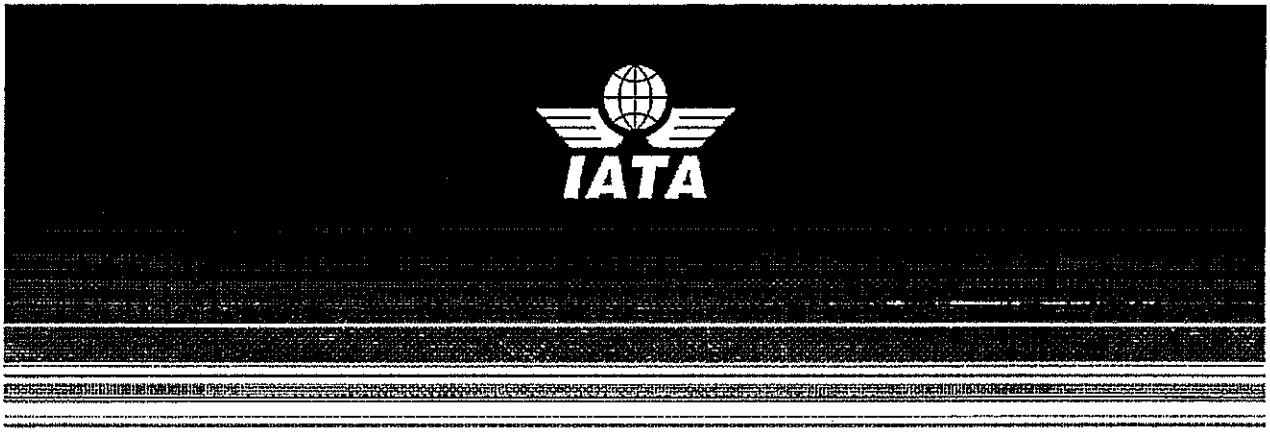
- IATA does not have a dedicated "Security Audit programme".
- IOSA *(differently from other international audits, such as: USAP, ECAC, TSA)* audits all aspects of operations.
- IOSA is the only global Airline audit that covers Security, since Security is a major part of airline operations.
- IOSA follows the SeMS approach to Security:
- Implemented system-wide
- Compliance with IOSA standards provides another boost to aviation security
  - ***All airlines – IATA member or not – can benefit by being audited under IOSA***

The Role of IOSA in SeMS

- To further enhance operational security, SeMS principles are incorporated in IOSA:
- IOSA provides Core Elements of SeMS regulatory requirements
  - When not provided by State of Registration
- SeMS audited within IOSA Standard Manual (5th Edition)
  - SeMS becoming an entry requirement for IATA Membership
- Objections by Airline to AO findings allowed
- Non-resolution handled by IATA.

Module summary exercise

- Have a better understanding of what IOSA is
- Understand the objectives of the IOSA Programme
- Know the root of IOSA Security Provisions
- Understand the IOSA audit process
- Understand the importance of IOSA for SeMS



Questions?

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Security Management Systems

Module 11

Contingency Planning

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

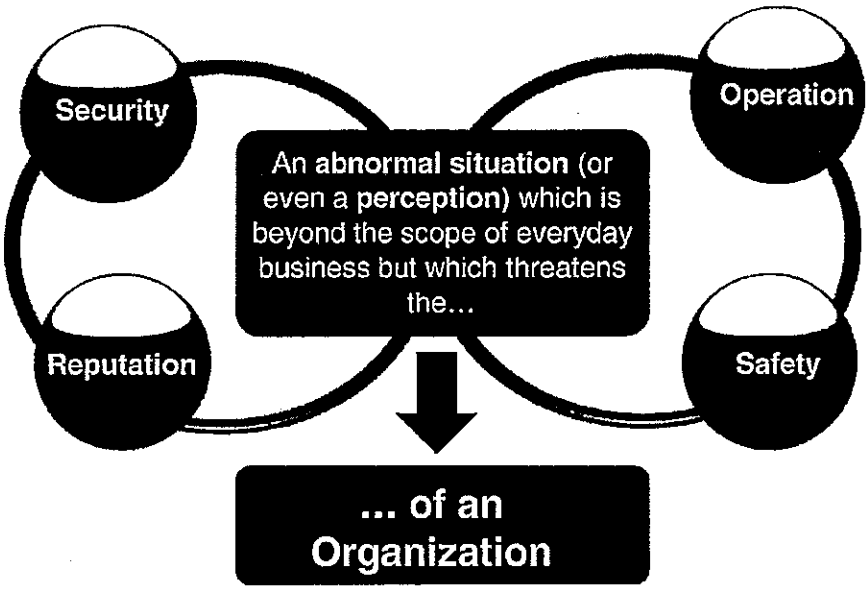
At the end of this module you will be able understand & describe:

- why Crisis Management is needed
- the goals of Crisis Management
- the different steps of a crisis management plan
- the different components involved in Crisis Management and how to design them
- the importance of investigating and reporting all security incidents

Topics covered

- Elements of Contingency Planning
- Crisis Management
- Crisis Control Area
- Emergency Operations Centre (EOC)
- Crisis Management Team (CMT)
- Incident Investigation and Reporting

What is a Crisis*?



Characteristics or Common Elements in Crises

- Confusion
- Rapid escalation of events
- Communication problems
- Failure of routine structures
- Resources isolated or inaccessible
- Routine decision-making fractured
- Media attention focused
- Demand for information

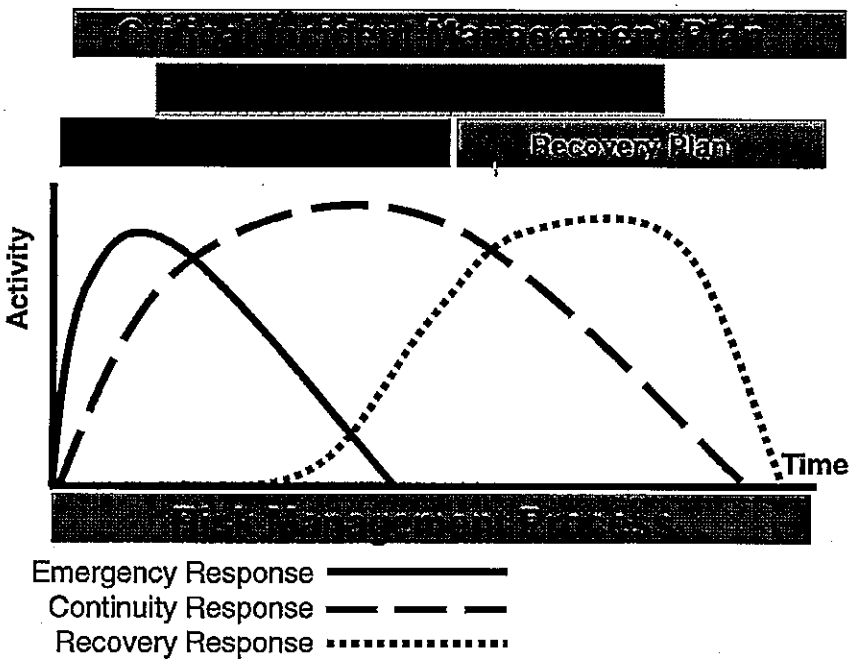
What is Crisis Management?

The process by which the Organisation manages a wider impact and enables it to commence Recovery

Strategies of Contingency Planning

- **Identify** – threat/risk assessments
- **Prevent** – strategic risk management
- **Respond** – initiate plans, teams, facilities
- **Recover** – business continuity & resumption

Crisis Management Phases



Crisis Management

- Objective
  - Bring about successful termination of crisis with minimum disruption and return to normal operations as soon as possible
- How – create..
  - Crisis Management Plan
  - Crisis Management Facilities
  - Crisis Management Team

To minimize the extent and duration of the Consequence (impact) of an event!

Crisis Management

Security Contingency Plans to deal with:

- Threat items found during screening
- Hijacking or aircraft sabotage
- Armed attack on airport property
- Armed attack against aircraft
- Bomb threat
- Explosive ordinance disposal
- Evacuation
- Increase in National/Airline/Airport Threat Level increased security measures and procedures

Crisis Management

Need to ensure:

- Orderly and efficient transition to emergency operations
- Clear command person and chain of command
- Delegation of airport emergency authority;
- Assignment of emergency responsibilities;
- Proper authorization for actions;
- Co-ordination of efforts to cope with incident;
- Safe continuation of aircraft operations or return to operations as soon as possible;
- Provision of additional security personnel and other staff resources.

Lessons learned

- Ignoring the Problem: it won't go away
- Lives may be lost
- Resources may be lost
- Reputations & confidence destroyed
- Company under strict scrutiny from Authorities
- Manage Media carefully and keep them properly informed
- Crisis Management: conduct regular exercises and Follow-Up

When the time comes to use the plan, the time to plan is over !

Failing to plan is planning to fail !

Enabling Crisis Management

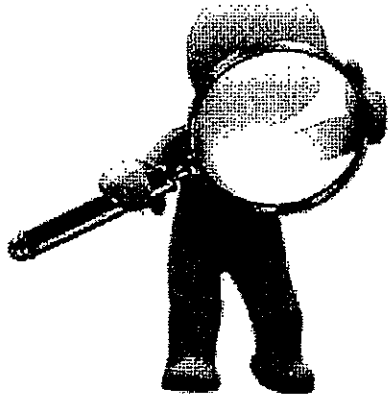
A. Know Your Oganisation & Formulate Internal Policy

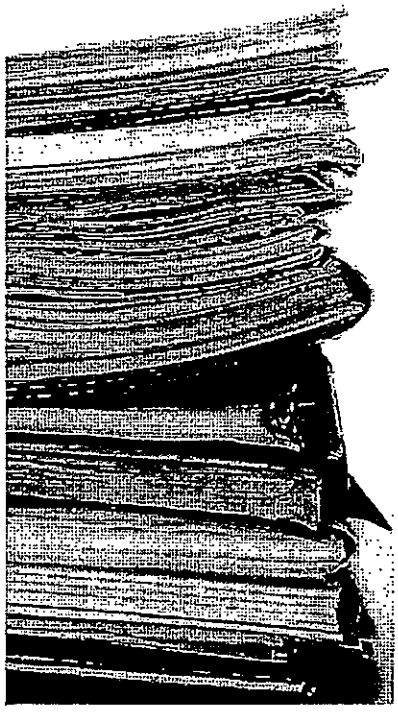
B. Pre-Planning

C. Implementation and Operation

D. Monitoring and Corrective Action

E. Management Review





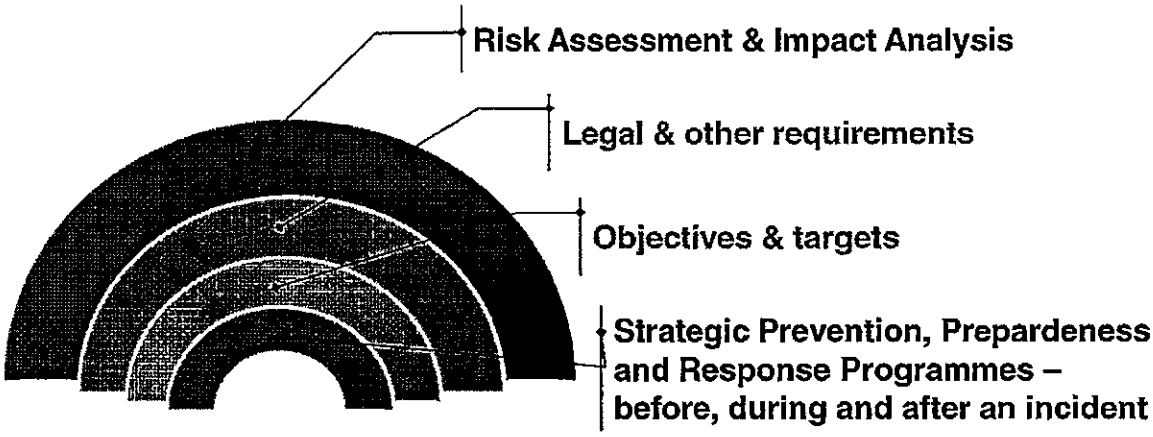
Enabling Crisis Management

A. Know Your Oganisation & Formulate Internal Policy

- Ensure Management Committment to:
  - protection of critical assests
  - continuous improvement via regular exercises
  - Ensure allocation of resources

Enabling Crisis Management

B. Pre-Planning



Enabling Crisis Management

C. Implementation & Operation

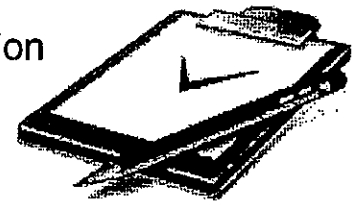
- ↗ Structure and responsibility
- ↗ Training, awareness, competence
- ↗ Communication

- ↗ Documentation
- ↗ Operational control
- ↗ Incident Prevention, Prepardeness and Response

Enabling Crisis Management

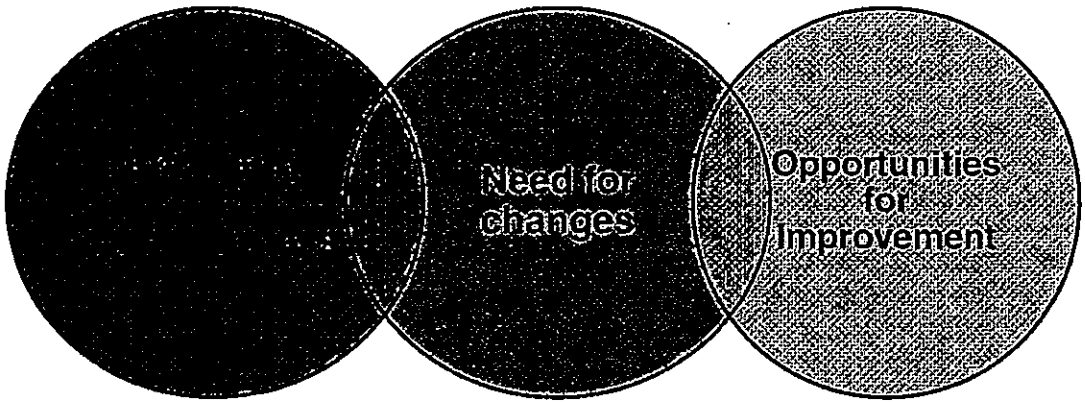
D. Monitoring and Corrective Action

- Monitoring and measuring system performance (also through internal audits)
- Identifying non-conformity/evaluating compliance
- Investigating corrective/preventive Action
- Maintaining records



Enabling Crisis Management

E. Management Review



Principles

Major Objective

Protection of life
(Humanitarian aspects are n° 1 priority)

Legal obligations

Preserving Company assets/image

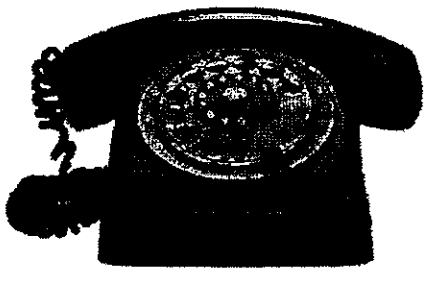
Resumption of normal operations (BCP*)

Secondary Objective

Investigation to establish if the crisis was an accident or a crime (normally carried out already by Investigating authorities**).

Crisis Management Process

- Response to Crisis must be handled by special team: the **Crisis Management Team (CMT).**
- CMT adopts/adapts existing management structure,
- Existing communications and
- Involves all necessary agencies



Security Management System

Module 12
Designing a SeMS

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

At the end of this module you will be able to understand & describe:

- why you need SeMS
- the relationship between regulatory requirements and SeMS elements
- why you need core elements as a foundation to SeMS
- what the IOSA Security core elements are.

Topics covered

- Why Design SeMS?
- Core Elements
- IOSA Core Elements
  - Management and Control
  - Training and Qualification
  - Security Operations
  - Security Threat and Contingency Management

Why Design SeMS?

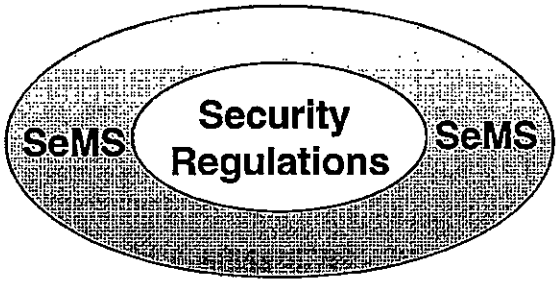
- Change in organizational security management philosophy
- Improve operational security effectiveness and efficiency – bringing together all core elements
- Ensuring compliance with Contracting State regulatory regime
  - ICAO recognizes SeMS, but not yet part of Annex 17
- Ensuring "best practice" in aviation security management

Core Elements

- Organization wide Security Management System
  - SeMS provides the "best practice" processes
- Regulatory compliance
  - ***Most important core element & primary driver*** - ICAO Annex 17
  - Contracting State Aviation Security Programs
- IATA Security Manual
- IOSA Core Elements
  - Documented & Implemented
  - Audit compliance

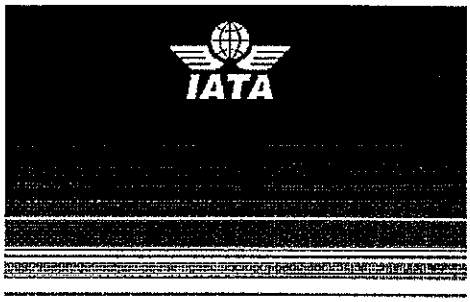
Core Elements

- "SeMS elements" are:
  - Quality Management segment in place (= QMS becomes complimentary system*)
  - Value-added
  - Support baseline security regulatory compliance
  - Essential to have security "best practices"



Core Elements*

- Regulatory requirements and SeMS elements shall be fully integrated
- Even if the Regulator has no SeMS requirement, there is still a need to have a regulatory framework;
- IOSA can provide that framework;
- IOSA mirrors or exceeds ICAO.



IOSA - SeMS Core Elements

- **IOSA Standard Manual** - Core elements in the Sections 8 - Security Management:
  1. **Management and Control**
  2. **Training and Qualification**
  3. **Security Operations**
  4. **Security Threat and Contingency Management**

1. Management and Control

Management Systems

↗SeMS*

↗Head of Security that reports to Senior Management

Security Program**

↗It contains security provisions that **shall always meet:**

- ↗ Requirement of State of Registration
- ↗ Requirements of State(s) of Operation
- ↗ Requirements of Security policy of the organization

***The Security Programme could be included in the more detailed and full comprehensive Security Manual*

1. Management and Control

- ↗ **Authority & Responsibility**
  - ↗ Definition of responsibilities for all management positions
  - ↗ Delegation of Tasks/Power
  - ↗ Reporting structure
  - ↗ Liaison with external stakeholders
- ↗ **Communication**
  - ↗ Process to exchange security information

1. Management and Control

- **Provision of Resources**
  - Work environment conducive to efficient security operations
  - Staff recruitment process to ensure competency
  - Pre-employment background check process
- **Documentation**
  - Management and control system for Security Programme and security manual elements
  - System to ensure service providers have access to security documentation

1. Management and Control

- **Security Manual**
  - Documented and up to date
  - Can be in separate parts (for the ***"Need to know"*** principle)
  - Contains SeMS descriptions and all elements/security provisions (such as: Organization, **Security Measures,** Security Training Programs, Security Quality Control, Local Procedures, Contingency Plans, etc.) that must be implemented by the company.
- **Records Systems**
  - Method to record operational security and management data
  - Back up process for electronic systems

1. Management and Control

- **Internal Security Quality Control**
  - Procedures for systems audit
  - Procedures for Quality Control Mechanism
- **Outsourcing and Product Control**
  - Monitoring contract agreement and performance
  - Auditing process for contractors
  - When not under organization's control, ensure measure are be applied
  - Equipment* *should* meet required technical specifications

2. Training and Qualification*

- **Training Programme**
  - Initial and recurrent training for frontline personnel
  - Security awareness training programme
  - Oversight of contractor training programmes
  - Certification of screeners**
  - Review and update of training programme content
  - Record system for training of security personnel

* *Normally includes also Recruitment*

3. Security Operations

- **Access Control**
  - Security Restricted Area Permit system
  - Prevention of introduction of dangerous items on aircraft
- **Aircraft Security**
  - Aircraft Security Checks & Searches
    - Bomb search procedures (*and Check-List*)
  - Aircraft Protection
  - In-Flight Security
    - Prevent unauthorized cockpit access - Reinforced cockpit door
    - Unruly/Disruptive Passengers

3. Security Operations

- **Carriage of Weapons**
  - Procedures for In-flight Security Officers (IFSO)
  - Procedures for law enforcement carrying weapons
  - Procedures for carriage of weapons as baggage
- **Passengers, Supernumeraries & Cargo Attendants, and Cabin Baggage**
  - Screening measures and security controls
  - Screening of all supernumeraries and cargo attendant
  - Measures to avoid passenger mixing
  - Right to deny boarding

3. Security Operations

- **Special Category Passengers**
  - Measures (*pre-flight & in-flight*) for passengers subject to judicial or administrative procedures.
- **Hold Baggage**
  - 100% Hold Baggage Screening*
  - Hold Baggage System levels at the Airport
  - Passenger-Hold Baggage Reconciliation & measures
  - Secure storage for mishandled bags
  - Screening of courier consignments

** Provisions applicable to international flights*

3. Security Operations

- **Cargo, Mail and Supplies**
  - Section 7 of IOSA Manual covers cargo operations
- **Cargo Security**
  - Security controls for all cargo
  - Protection of cargo from unauthorized interference
  - Cargo not accepted from regulated agents subjected to security controls
  - Acceptance procedures
  - Protection from unauthorized access of all catering and stores after security control

4. Security Threat and Contingency Management

- **Threat Assessment & Risk Management**
  - Assess risk factors of threats
  - Develop countermeasures for new threats
  - Develop countermeasures for multiple threat levels
  - Have a means of evaluating performance and effectiveness of countermeasures (RP)
- **Contingency Planning**
  - Have well-rehearsed contingency plans in place to respond to incidents

4. Security Threat and Contingency Management

- **Investigation and Notification**
  - Investigation process for:
    - Acts of unlawful interference
    - Failure of implementation of security controls
  - Process to notify the civil aviation security authority

Module summary exercise

- Know why you need SeMS
- Understand the relationship between regulatory requirements and SeMS elements
- Know why you need core elements as a foundation to SeMS
- Know what the IOSA Security core elements are

Questions?

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Security Management Systems

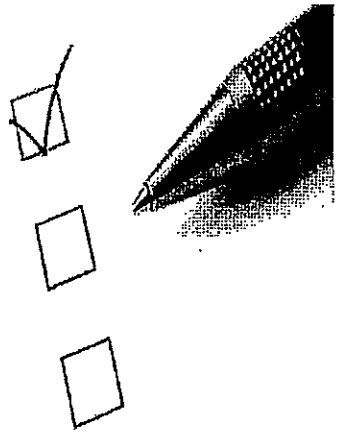
Module 13

Project Management

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives



At the end of this module you will be able to understand and describe:

- the basic components of Project Management
- how to draft a SeMS project proposal
- the importance of developing a project management plan when implementing SeMS.

Topics covered

- Defining Project Management
- Project Identification
- Project Initiation
- Project Planning
- Project Execution and Control
- Project Closing

Defining Project Management

- Application of knowledge, skills, tools, and techniques to project activities in order to meet or exceed stakeholder and expectations from a project
- It is not just scheduling !
  - A lot has to be done before and after your schedule or timeline has been drafted
  - ***Gantt charts*** driving on-time and on-budget can distract from the important element of people.

Defining Project Management

- A project is different from operations, since it is:
  - One-time only
  - With a defined starting and end point
  - With a defined budget, objectives and scope
  - Unique !

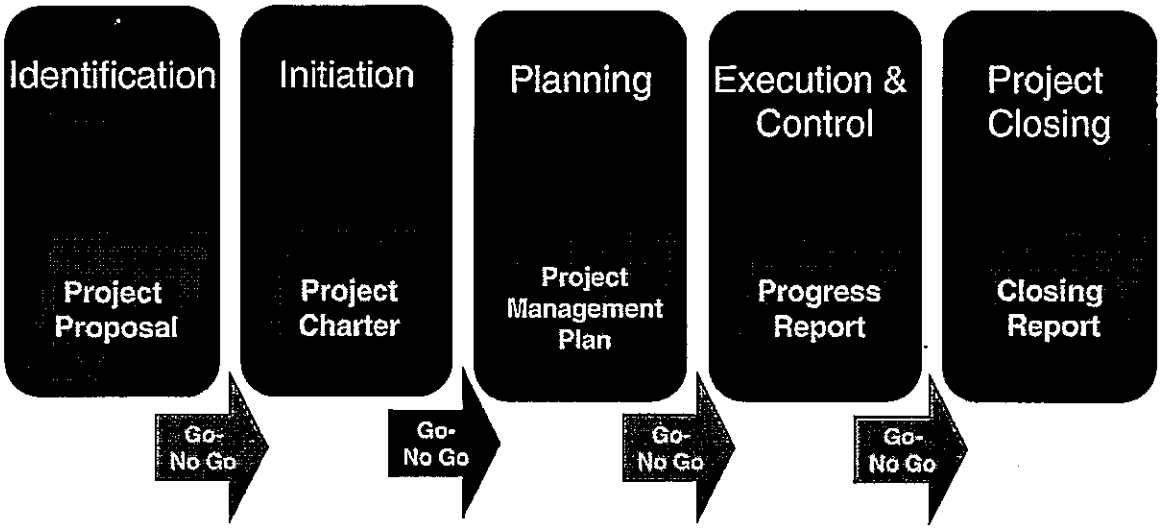
Defining Project Management

Project Manager responsibilities:

- Meets project objectives within constraints
- Integrates everything and everybody
- Makes decision
- Resolves conflict
- Communication hub
- Prime negotiator with stakeholders

Defining Project Management

Project life cycle phases



Project Identification

- Conceptual Phase
- **Someone identifies a need that must be met**
  - Cost savings
  - Improved productivity
- Project scope is broadly defined
- Deliverable: **Project Proposal**

Project Identification

- **Project Proposal content:**
  - Project ID
  - Broad descriptions of project scope
  - Main actors
  - Broad estimates for time, costs, resources
  - Project justification
  - Main impacts of project
  - Assumptions, dependencies & constraints considered
  - Recommendations made
  - Submitted to senior management

Project Identification

- **Project Proposal Purpose**
  - Raise awareness of project viability
  - Provide rationale for project

Project Initiation

Project Team

- Clarify the mandate of the endorsed project
- Select implementation strategy
- Perform stakeholder analysis
- Perform impact assessment
- Perform risk analysis
- List project deliverables
- Budget estimates
- **Get authority to go ahead**
  - Deliverable: **Project Charter Report**

Project Initiation

Project Charter Report content:

- Context
- Project Description
- Project goals
- Project objectives
- Justification
- Implementation Strategy
- Risks and roadblocks (internal, external)
- Recommendations
- **Approval from CEO/B. of D./AM**

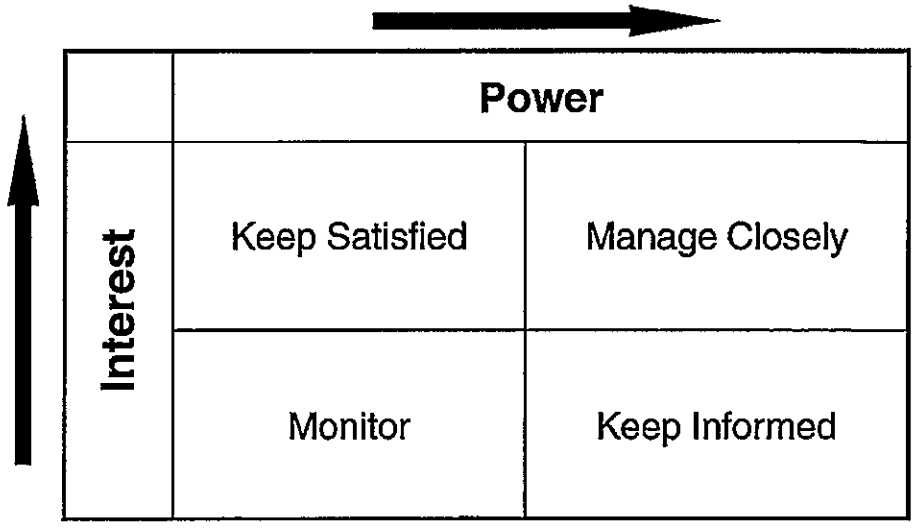
Project Initiation

Stakeholder Management

- **Identify**
  - Organizations or individuals
  - Participants in the project
  - Anyone affected by the project
  - Anyone having an impact on the project
- **Analyze**
- **Prioritize**
- **Understand motivating factors**
  - Use as base for communication plan
  - Use as base for risk identification

Project Initiation

Stakeholder Analysis



** Do it early and do it often*

Project Initiation

Project Risk Analysis

- Create a realistic project baseline
- **Identify Risk***
  - Classify by cause, not impact!
  - Project owner is responsible for risk management decisions
  - Person performing the task is best placed to identify the risk
  - Risk identification is a team effort
- **Build contingency plans by:**
  - Identifying alternative options

Project Planning

Process

- Project team is created
- Work Breakdown Structure (WBS) is created
- Roles and responsibilities are assigned
- Feasibility studies are determined
- Schedules is created and optimized
- Project baseline is created
  - Deliverable: **Project Management Plan,** Formal and approved document that defines how the project is executed.

Project Planning

Project Management Plan content:

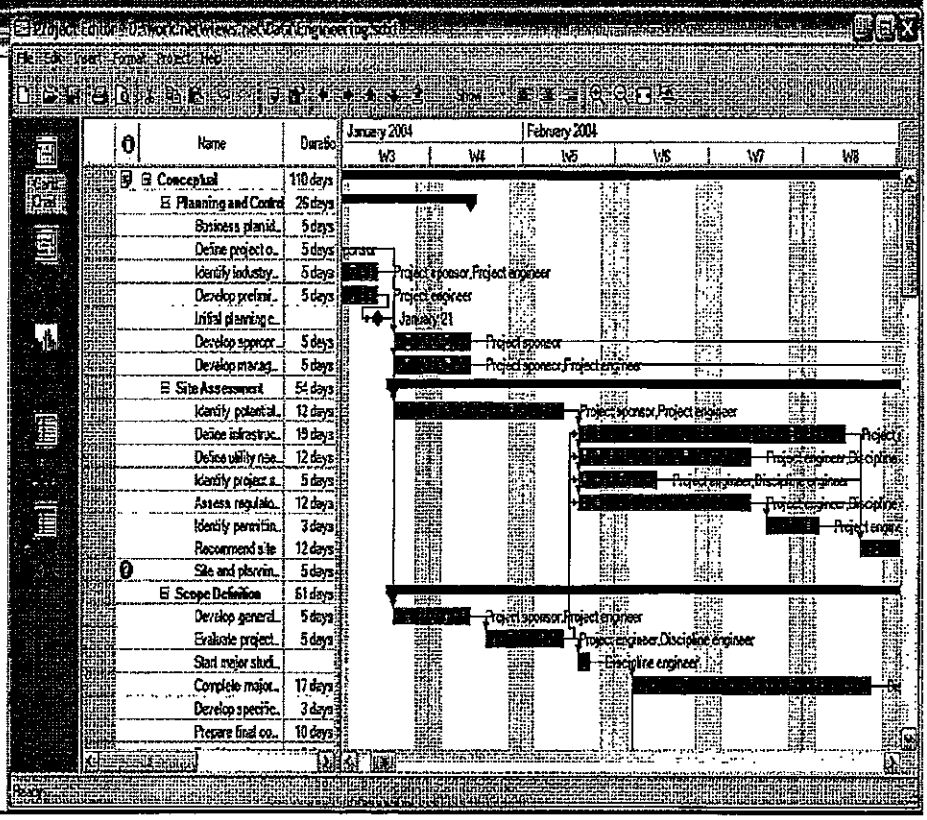
- Baselines
  - Scope, schedule, budget, quality
- Management processes
- Tools techniques and procedures
- Change management and control
- Configuration
- Risk register
- Key management reviews

Project Planning

Work Breakdown Structure (WBS)

- Deliverable-oriented hierarchical decomposition of the work to be done.
- Organizes and defines total scope of the project
- Roles/Critical elements
  - Activity duration estimation
  - Resource requirements
  - Cost estimation
  - Risk identification
  - Responsibility assignment
  - Performance tracking
  - Communication

Gantt Chart



Project Execution

During the course of the project:

- Conduct regular meeting with core team
- Assess Progress
- Identify potential delays
  - Develop Mitigation plan
  - Divert or assign additional resources
  - Evaluate impact on other dependent tasks
- Create an environment where everyone feels comfortable giving an accurate assessment

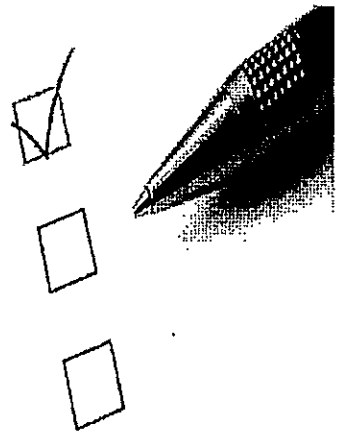
Security Management Systems
Session 15

Change Management

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives



At the end of this module you will be able to understand and describe:

- why there is a need to consider change management when implementing SeMS
- how to apply Prosci's ADKAR Model
- the skills a change agent requires to be successful
- the different change management strategies

Topics covered

- Why Change Management
- Change Management Process
- Change Management Skills
- Change Management Strategies

Why Change Management?

- Oppose change is a natural tendency:
  - Anthropologically and psychologically based
- Convince your staff that changing set processes
  - Improves the organizational productivity
  - Facilitates individual daily duties in the long term
  - Will be problem solving not problem causing
- Get buy-in from everyone to ensure success of your project

Why Change Management?

- Being organized contributes in gaining support
  - Project Management Plan
- Proactive management of change produces:
  - Increased credibility (with everybody)
  - Better informed decisions and judgments, and more effective activity
  - Savings in time and money
  - Better resource allocation and measurable results
- Application when developing the SeMS

Why Change Management?

Gleicher's Formula* :

change is possible

if...

D x V x F > R

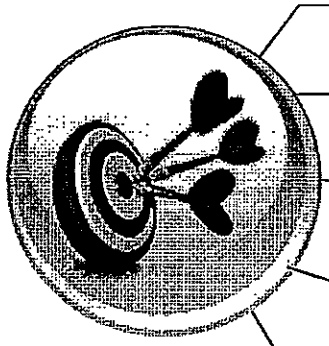
Where:

- **D** Dissatisfaction with how things are now
- **V** Vision of what is possible
- **F** First, concrete steps that taken towards the vision
- **R** Resistance

Change Management Process

Prosci's ADKAR® Model (1998)

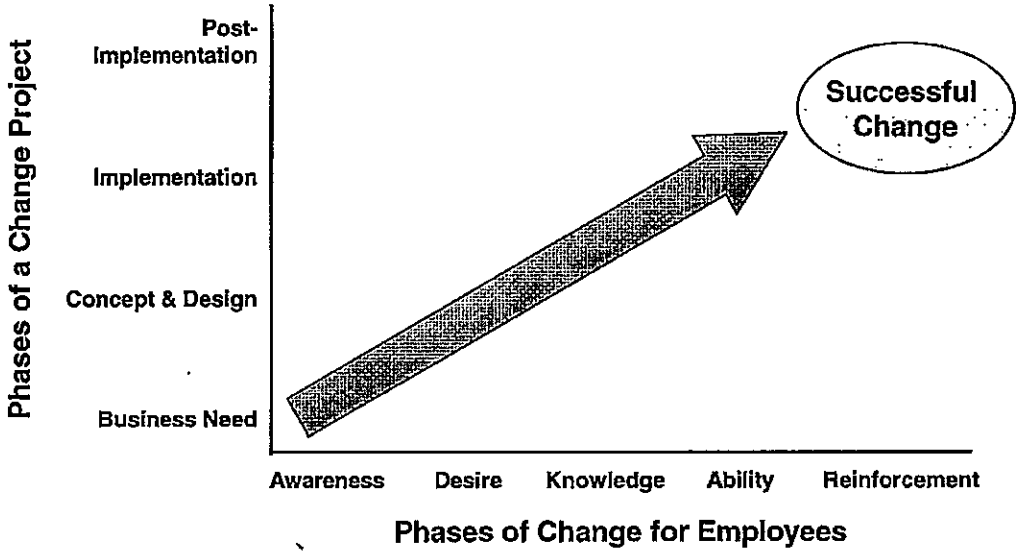
Management's 5 key goals:



- **Awareness** of the need to change
- **Desire** to participate & support the change
- **Knowledge** of how to change (and what the change looks like)
- **Ability** to implement the change on a day-to-day basis
- **Reinforcement** to keep the change in place

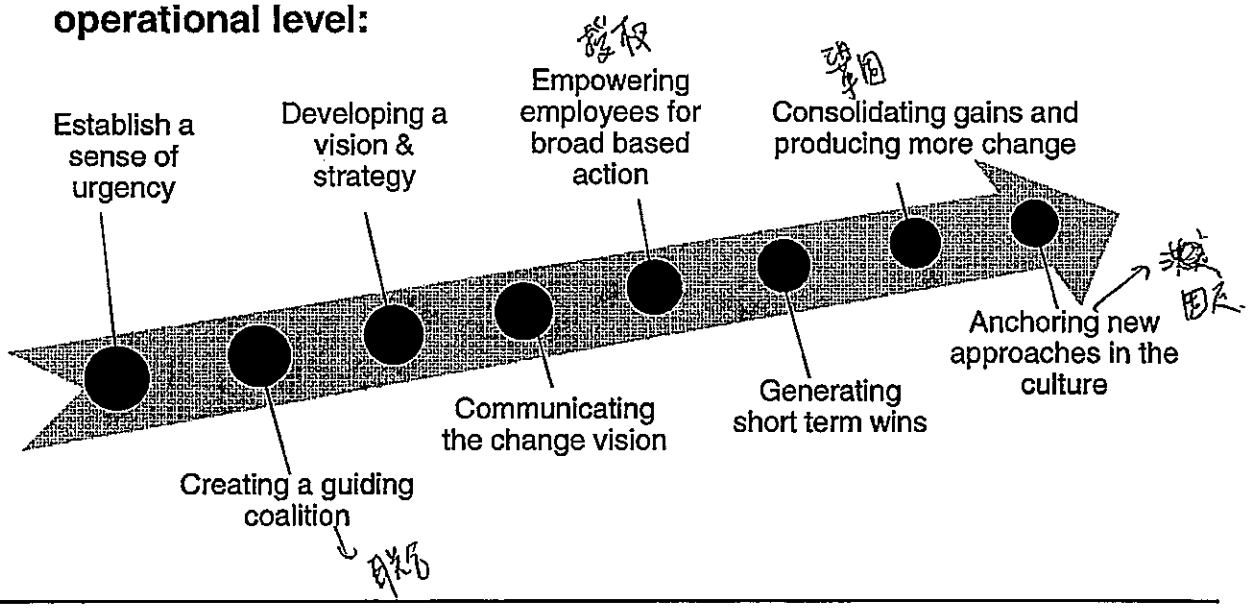
Change Management Process

Prosci's ADKAR® Model (1998)



Change Management Process

Kotter's 8 stage process linking strategy to execution at operational level:



Change Management Process

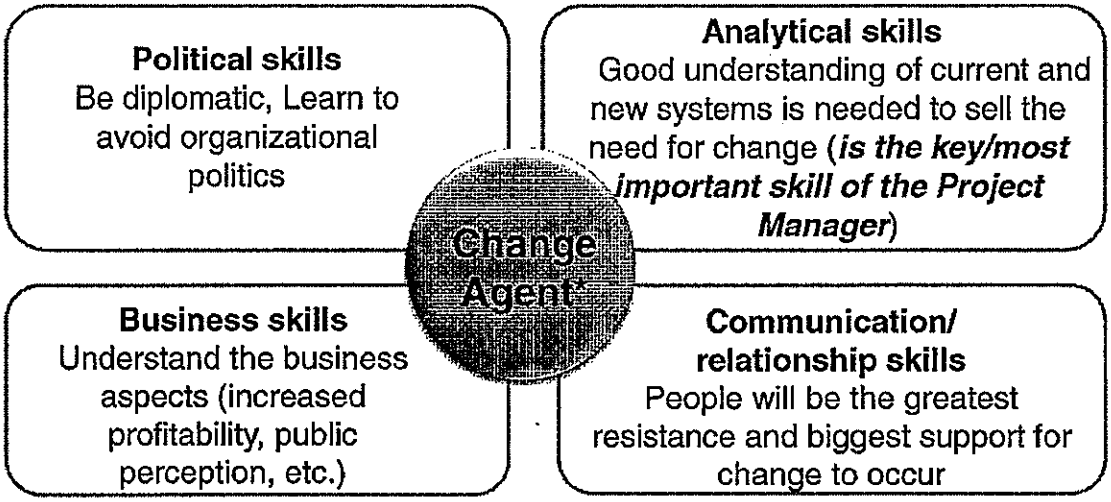
Teamwork

Person's role in the organization will define what questions they will ask*:

- Systems and Operations: — How? (How to operate.)
- Performance units: — What? (what is the result)
- Perimeter units: — How ? (How to measure the result)
- People with no direct role in day-to-day operations (i.e. Senior Mgmt): — Why? (Different Job.)

Change Management Skills

Skills required for change agents



Change Management Strategy

- **Empirical-Rational** 經驗管理法
  - People are rational and will follow their self-interest — once it is revealed to them.
  - Change is based on the communication of information and the proffering of incentives. 動機
- **Normative-Re-educative** → 規範
  - People are social beings and will adhere to cultural norms and values.
  - Change is based on redefining and reinterpreting existing norms and values, and developing commitments to new ones

Change Management Strategy

- **Power-Coercive**
  - People are basically compliant and will generally do what they are told or can be made to do.
  - Change is based on the exercise of authority and the imposition of sanctions
- **Environmental-Adaptive**
  - People oppose loss and disruption but they adapt readily to new circumstances.
  - Change is based on building a new organization and gradually transferring people from the old one to the new one.

Change Management Strategy

- **Factors in Selecting a "Change" Strategy:**
  - Degree of Resistance
  - Target Population
  - The Stakes
  - The Time Frame
  - Expertise
  - Dependency

Module summary exercise

- Understand why there is a need to consider change management when implementing SeMS
- Understand how to apply Prosci's ADKAR Model
- Know the skills a change agent requires to be successful
- Know the different change management strategies.

Questions?

Security Management Systems

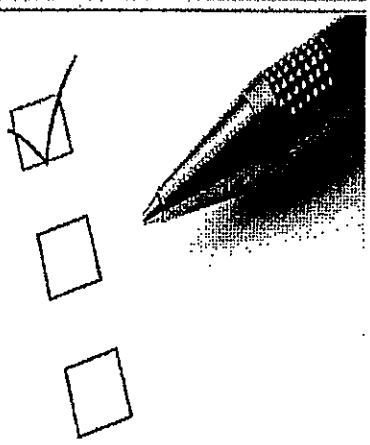
Module 16

Performance-Based Regulations

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS

Module objectives

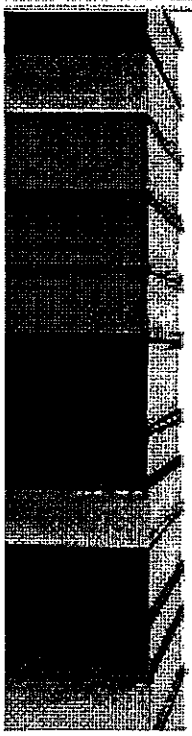


At the end of this module you will be able to understand and describe:

- the difference between prescriptive and performance-based regulations
- the advantages of performance-based regulations
- the potential challenges of implementing performance regulations

Topics covered

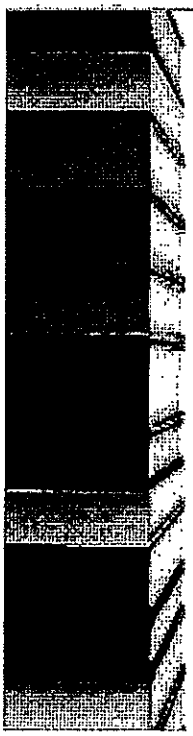
- Prescriptive Regulations
- Performance-Based Regulations
- Prescriptive or Performance-Based (exercise) ?



Prescriptive Regulations

Features Instructions direction, low or rule

- Traditional model for AVSEC regulations
- Regulator told stakeholders how to ensure security
- Becomes difficult when
  - Multitude of security layers interacting together
  - Multiple threats exist
  - Threat varies from location to location
- One size fits all measure is becoming harder to implement



Prescriptive Regulations

Features

- Regulators must invest more time and energy to implement appropriate regulations
- Regulations are always trying to prevent the last incidents (little causal analysis)
- Stakeholders are forced to focus on meeting the last requirements
  - Time-consuming and costly
  - Difficult to exceed baseline measures
- Generally very little consultation takes place
  - Too many stakeholders

Performance-Based Regulations

Also known as "Risk-based" regulations

- Legislates **what** is required rather than **how**
- Developed in consultation with stakeholders
- Considers the potential impact on operations
- Focus on policies & procedures to ensure on-going delivery
  - Multiple risk and threat level
- Role of Regulator - oversight with effective sampling rather than on-going & detailed inspection
- Promotion & maintenance of responsibilities

Performance-Based Regulations

Advantages of performance-based approach

- Provides stakeholders the ability to implement the best security measures based on
  - Operational environment
  - Specific risk and threat realities e.g. airport zones with different threat levels – tailor the security response
- Promotes communication and co-operation
- Reduces the burden on the Regulator*

Performance-Based Regulations

Advantages of performance-based approach

- **Pro-active**
  - Stakeholders are able to try to prevent the present threat while meeting the regulatory objective
- Facilitates mutual acceptance of security measures (outcomes)
  - A better option than harmonization – less effort
- Rather than developing new "reactive" technical rules on a particular issue, performance levels can be specified.

Performance-Based Regulations

Challenges

Can stakeholders self-implement security measures?

- Regulators needs a thorough oversight program

Especially for higher risk situation, how do you ensure the right threat is addressed with effectiveness?

- Constant communication between stakeholders and regulator
- Intelligence sharing
- More hands-on approach may be required

Example:
Transport Canada 100% HBS Regulation Model

Compliant with International Standards

- Annex 17 Standards and Recommended Practices on Hold Baggage Screening

Performance Based

- The regulator Transport Canada (TC) sets the Objectives and Standards
- The screening authority (Canadian Air Transport Security Authority identified how best to meet the objectives and standards
- Multiple approved HBS configurations to accommodate airports' characteristics

Example:
Transport Canada 100% HBS Regulation Model

Stakeholder Input

- 3 Stakeholder meetings
- Continuous dialogue with all stakeholders
- Amendments made on basis of stakeholder input
  - To reduce negative impact on airport and air carrier operations
  - To improve screening effectiveness and efficiency

Example:
Transport Canada 100% HBS Regulation Model

- SeMS type approach
- Complement to regulations
- Used as a Quality Assurance tool
- Used to ensure best practices are implemented
- Provides operational flexibility to regulate entity
- SeMS is a requirement for all Canadian registered Air Carriers under Bill C-7 Public Safety Act 2002 – Aviation Security

Prescriptive or Performance-Based?

Access to airside shall be restricted in order to deter unauthorised persons and vehicles from entering these areas.

Prescriptive or Performance-Based?

- If unable to monitor catering from preparation to delivery, conduct searches on a minimum of 50% of the trays in each catering cart.

Prescriptive or Performance-Based?

- Each Contracting State shall establish measures to ensure that originating hold baggage is screened prior to being loaded onto an aircraft engaged in commercial air transport operations departing from a security restricted area.

Prescriptive or Performance-Based?

- All passenger-carrying aeroplanes of a maximum certificated take-off mass in excess of 45 500 kg or with a passenger seating capacity greater than 60 shall be equipped with an approved flight crew compartment door that is designed to resist penetration by small arms fire and grenade shrapnel, and to resist forcible intrusions by unauthorized persons. This door shall be capable of being locked and unlocked from either pilot's station.

Prescriptive or Performance-Based?

- The Operator shall ensure procedures are in place that prevent disembarking passengers from leaving items on board an aircraft during a transit stop at an airport, that is deemed by the Operator or the appropriate authority to be under an increased security threat.

Module summary exercise

- Understand the difference between prescriptive and performance-based regulations
- Understand the advantages of performance-based regulations
- Understand the potential challenges of implementing performance regulations within an Operator.

Questions?

IATA Training & Development Institute

KNOWLEDGE • EXPERIENCE • NETWORKING • SKILLS • RESULTS