EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

ESARR ADVISORY MATERIAL/GUIDANCE MATERIAL
(EAM/GUI)

EAM 1 / GUI 3

GUIDELINES FOR SAFETY REGULATORY AUDITING

Edition	:	1.0
Edition Date	:	17 October 2005
Status	:	Released Issue
Distribution	:	General Public
Category	:	ESARR Advisory Material

SAFETY REGULATION COMMISSION

F.2 DOCUMENT CHARACTERISTICS

TITLE		
EAM 1 / GUI 3 **Guidelines for Safety Regulatory Auditing**		
Document Identifier	**Reference**	EAM 1 / GUI 3
eam1gui3_e10_ri_web	**Edition Number**	1.0
	Edition Date	17-10-2005

Abstract

This deliverable has been prepared by the Safety Regulation Commission (SRC) to provide National Supervisory Authorities (NSAs) with guidance and recommendations on the implementation of a safety regulatory audit process in accordance with ESARR 1.

The document sets out all stages of the audit process and, in particular, describes details specific to safety regulatory auditing which are required to be followed by NSAs in order to meet ESARR 1. In addition to guidance on the practice of conducting audits, the document contains guidance to NSA senior and middle managers on activities which are necessary to support safety auditing and associated activities.

Keywords

Safety Oversight	National Supervisory Authorities	Monitoring of Safety
Safety Regulatory Audit	Safety Oversight of Changes	Verification of Compliance
Supervision	Single European Sky	ESARRs

Contact Person(s)	Tel	Unit
Juan VÁZQUEZ SANZ	+32 2 729 46 81	DGOF/SRU

DOCUMENT INFORMATION

Status		Distribution		Category	
Working Draft	□	General Public	☑	Safety Regulatory Requirement	□
Draft Issue	□	Restricted EUROCONTROL	□	Requirement Application Document	□
Proposed Issue	□	Restricted SRC	□	ESARR Advisory Material	☑
Released Issue	☑	Restricted SRC Commissioners	□	SRC Policy Document	□
		Restricted SPG	□	SRC Document	□
		Restricted SRU	□	Comment / Response Document	□

COPIES OF SRC DELIVERABLES CAN BE OBTAINED FROM

Safety Regulation Unit	Tel: +32 2 729 51 38
EUROCONTROL	Fax: +32 2 729 47 87
Rue de la Fusée, 96	E-mail: sru@eurocontrol.int
B-1130 Bruxelles	Website: www.eurocontrol.int/src

F.3 DOCUMENT APPROVAL

The following table identifies all management authorities who have approved this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Quality Control (SRU)	***signed by Daniel Hartin*** (Daniel HARTIN)	17.10.2005
Head Safety Regulation Unit (SRU)	***signed by Peter Stastny*** (Peter STASTNY)	17.10.2005
Chairman Safety Regulation Commission (SRC)	***signed by Ron Elder*** (Ron ELDER)	17.10.2005

Note: For security reasons and to reduce the size of files placed on our website, this document does not contain signatures. However, all management authorities have signed the master copy of this document which is held by the SRU. Requests for copies of this document should be e-mailed to: sru@eurocontrol.int.

(Space Left Intentionally Blank)

F.4 DOCUMENT CHANGE RECORD

The following table records the complete history of this document.

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
0.01	10-Mar-05	Creation. Outcome of drafting conducted with the support of national experts.	All
0.02	10-Jun-05	SRU review. Modification of terminology used, alignment of the document with ESARR 1 and SES and restructuring of contents.	All
0.1	01-Aug-05	Minor editorial changes followinng RTF consultation (RFC No. 0515). Document sent to SRC for formal consultation and approval.	Sections 6.5.5, 8.5.5, 10
1.0	17-Oct-05	Document formally released following final review in the light of SRC consultation (RFC No. 0521).	All

(Space Left Intentionally Blank)

F.5 CONTENTS

Section Title **Page**

FOREWORD

CONTENTS

PART 1 – GUIDANCE FOR NSA SENIOR AND MIDDLE MANAGERS

F.5 CONTENTS

PART 2 – GUIDANCE FOR AUDITORS AND AUDIT TEAM LEADERS

F.5 CONTENTS

APPENDICIES

(Space Left Intentionally Blank)

F.6 EXECUTIVE SUMMARY

This deliverable has been prepared by the Safety Regulation Commission (SRC) to provide National Supervisory Authorities (NSAs) with guidance and recommendations on the implementation of a safety regulatory audit process in accordance with ESARR 1.

The guidance contained within this document is primarily concerned with safety regulatory auditing of ATM service providers by NSAs, or by those recognised organisations commissioned by them to undertake safety auditing activities on their behalf. The document is designed to support ESARR 1 by providing guidance on what is considered to be current best audit practices linked to the various stages of the overall safety oversight process, in order to make clear how auditing should be used as an integral part of ATM safety oversight.

The international standard ISO 19011 has been considered in the development of this document. Consequently, whilst primarily intended for the verification of compliance with safety regulatory requirements, this guidance may also be applicable in relation to compliance with other regulatory requirements applicable to ATM service providers.

The document sets out all stages of the audit process and, in particular, describes details specific to safety regulatory auditing which are required to be followed by NSAs in order to meet ESARR 1. In addition to guidance on the practice of conducting audits, the document contains guidance to NSA senior and middle managers on activities which are necessary to support safety auditing and associated activities.

More specifically:

- ❑ Part 1 is intended to assist NSA senior and middle management in both the understanding and application of auditing techniques in relation to the safety oversight of ATM service providers, and covers the higher level processes relating to the management of auditing activities to ensure that the audit process itself effectively serves the needs of the NSA.
- ❑ Part 2 is intended to provide auditors with an understanding of good audit practice and protocol as adopted by auditors working in a variety of industries and organisations, but specifically adapted to suit the needs of auditors working for, or on behalf of a NSA in a range of ATM environments.
- ❑ Appendices A to I include examples to illustrate the practical application of auditing in various situations. These examples have been developed with support from national safety oversight experts.
- ❑ Appendix J includes criteria recommended for training in relation to safety regulatory auditing. These criteria are considered by SRC as a recommended means to meet the ESARR 1 requirements on qualification of auditors.

Service provider organisations may also find some of the general guidance contained within this document helpful in relation to the conduct of internal auditing and supplier/contractor evaluation and auditing activities.

1. INTRODUCTION

1.1 Purpose

These guidelines are provided for National Supervisory Authorities (NSAs) within States whose responsibilities include the safety oversight of ATM service provider/s in accordance with ESARR 1.

The guidance contained within this document is primarily concerned with safety regulatory auditing of ATM service providers by National Supervisory Authorities, or by recognised organisations commissioned by NSAs to undertake safety auditing activities on their behalf. The document is designed to support the implementation of ESARR 1 by providing guidance on what are considered to be current best audit practices linked to the various stages of the overall safety oversight process, in order to make clearer how auditing should be used as an integral part of ATM safety oversight.

The international standard ISO 19011 has been considered in the development of this document. Consequently, whilst primarily intended for the verification of compliance with safety regulatory requirements, the guidance may also be applicable in relation to compliance with other regulatory requirements applicable to ATM service providers.

The document sets out all stages of the audit process and, in particular, describes details specific to safety regulatory auditing that are required to be followed by NSAs in order to satisfy ESARR 1. In addition to guidance on the relatively well understood practice of conducting audits, the document contains guidance to NSA managers on activities that are necessary to support safety auditing and associated activities.

Service provider organisations may also find some of the general guidance contained within this document helpful in relation to the conduct of internal auditing and supplier/contractor evaluation and auditing activities.

1.2 Scope

In these guidelines the term 'audit' is normally used in relation to its specific application to ATM safety oversight in the form of 'safety regulatory audits'. Throughout the text, both terms can be considered **synonyms** unless a different meaning is explicitly indicated.

In the context of ESARR 1, the safety regulatory audits constitute the basic means by which NSAs obtain objective evidences as regards the compliance by service providers with applicable safety regulatory requirements.

It should be noted that the audit process required in ESARR 1 will be implemented within the existing regulatory framework.[1]

[1] *Within EU Member States, the existing regulatory framework and requirements applicable to the provision of ATM services is based on the SES legislation which came into force in April 2004. This legislation, adopted by the European Parliament and Council consists of four Regulations (EC); 549/2004 (the Framework Regulation), 550/2004 (the Service Provision Regulation), 551/2004 (the Airspace Regulation) and 552/2004 (the Interoperability Regulation). In non-EU countries who are Members of EUROCONTROL, the existing regulatory framework and requirements applicable to the provision of ATM services will primarily be of a national nature and developed consistently with the various international obligations binding on those States, such as those contained in the Chicago Convention and the EUROCONTROL Convention.*

Within the Single European Sky (SES) framework, Regulation (EC) 550/2004 establishes that National Supervisory Authorities shall organise *"proper inspections and surveys"* to verify compliance with the requirements of the Regulation. These requirements cover a wide range of areas apart from safety and the methods applied for their verification may consequently vary. Nevertheless, safety regulatory auditing is the **means identified within ESARR 1 to implement** the *"proper inspections and surveys"* required in the Single European Sky regulations wherever safety is the aspect subject to verification.

Safety regulatory audits are therefore recognised as an essential process for the supervision of safety in the provision of ATM services throughout European airspace. However for such auditing to be fully effective it is necessary not only for those conducting safety regulatory audits to understand the process, related techniques and good practices but also it is necessary for those managing the auditors and the overall audit process to be aware of current best practice in auditing and the importance of providing adequate resources to meet the obligations established in ESARR 1 consistently with the existing regulatory framework.

These guidelines provide an indication of the minimum structural arrangements and resources that are likely to be necessary in order to plan, manage and conduct the audits necessary as part of the safety oversight of ATM services. The methodology and full process to be followed for each stage in the process is described together with appendices providing examples that illustrate the practical application of the processes described in the text.

Part 1 of this document has been provided with the aim of promoting harmonised and professional management of auditing practices for safety oversight throughout the ECAC states in support of harmonisation and acceptability of audit results. It has been developed taking into consideration what is generally considered to be 'best audit practice' and is regarded as the minimum standard for auditing that should be adopted by professional auditing organisations. It draws on the experience gained from the application of such practices within a range of National Supervisory Authorities.

Part 2 provides a methodology and full process for auditors to follow in the conduct of initial or ongoing safety oversight audits, which is clearly mapped to, and comprehends the requirements of ESARR 1. The template in this document is a useable tool irrespective of the size or complexity of the provider to be audited.

TO NOTE THAT: The guidance in this document is provided as follows:

- ❑ ***Part 1 is provided for NSA senior management whose responsibilities include the initial and ongoing oversight of service provider/s in accordance with applicable safety regulatory requirements and who need to ensure the effectiveness of audits.***
- ❑ ***Part 2 is provided for those involved in the day to day management and conduct of safety regulatory audits.***

2. APPLICATION

2.1 Application by NSA Management

The guidance provided in Part 1 of this document is intended to assist NSA senior and middle management in both the understanding and application of auditing techniques in relation to the performance of safety oversight of ATM service providers, and covers the higher level processes relating to the management of auditing activities to ensure that the audit process itself effectively serves the needs of the NSA.

These higher level processes relate to the concept of provision of adequate and competent resources, planning oversight visits and the utilisation of audit results in reaching decisions relating to initial oversight of ATM service providers.

It is recommended therefore that, as a minimum, senior managers should read Part 1 of this guidance document. However, senior and middle managers should also have a full understanding of the general process of auditing in order to appreciate the problems and difficulties associated with auditing and the concept of audit sampling with its associated limitations.

There are significant implications for the effectiveness of safety oversight if the NSA does not have sufficient audit resource to perform the necessary level of auditing activity. A full understanding of the audit process and associated resource implications is also necessary to ensure adequate resource provision. NSA management should be aware of the resource requirements necessary to enable sufficient planning to be undertaken by auditors and by senior and middle management responsible for managing the audit process.

TO NOTE THAT: the audit processes will fail to deliver the required results if the audit process and the auditors are not managed effectively.

2.2 Application by Auditors

The guidance contained in Part 2 of this document is intended to provide auditors with an understanding of good audit practice and protocol as adopted by auditors working in a variety of industries and organisations but specifically adapted to suit the needs of auditors working for, or on behalf of a NSA in a range of ATM environments.

The audit process exists to provide NSA management with information to enable them to make judgements relating to the initial oversight or continued operation of an ATM service provider. The auditor must recognise and understand that their responsibility is to carry out the audit as required by NSA management and to provide factual, objective and unbiased information relating to the effective implementation of the applicable safety regulatory requirements and associated practices together with views / opinions that will act to alert the NSA to possible weaknesses observed and areas for future investigation.

The guidance contained in Part 2 of this document may also be of use for service providers in the development and implementation of their internal audit processes.

3. TERMS AND DEFINITIONS

The following terms and definitions are used within this document:

Term — ***Definition***

Applicable safety regulatory requirements

The requirements for the provision of ATM services, applicable to the specific situation under consideration, and established through the existing rulemaking framework, concerning, inter alia:

i) Technical and operational competence and suitability to provide ATM services;

ii) Systems and processes for safety management;

iii) Technical systems, their constituents and associated procedures.

Air Traffic Management (ATM)

The aggregation of airborne and ground-based functions (air traffic services, air space management and air traffic flow management) required to ensure the safe and efficient movement of aircraft during all phases of flight.

ATM service provider

Any public or private entity providing ATM services for the purpose of ATM.

Audit

Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.

(NOTE 1: definition from ISO 9000:2000)

(NOTE 2: as pointed out in Section 1.2 of this document, this guidance normally uses the term 'audit' in relation to its specific application to ATM safety oversight in the form of 'safety regulatory audits'. Throughout the text, both terms can be considered synonyms unless a different meaning is explicitly indicated)

Audit base

The specified requirements against which an auditor performs an audit verification

(NOTE: the audit base may be a regulation or a combination of regulations, together with other related requirements or arrangements to be fulfilled by an organisation, such as manuals and procedures).

Term ***Definition***

Audit management

The function responsible in an NSA for determining, implementing and following up the annual programme of safety regulatory audits required in ESARR 1. This includes the management of the audit process and the auditors.

Audit scope

Those parts of an organisation that are the subject of an audit.

Certificate

A document issued by a Member State in any form complying with national law, which confirms that an ATM service provider meets the requirements for providing a specific service.

Corrective action

Action to eliminate the cause of a detected nonconformity or other undesirable situation.

(NOTE: Corrective action does not mean the action taken to restore a nonconforming situation to a conforming situation. This is known as remedial action. If the root cause of a non-conformity is not addressed then it is very likely that similar nonconformities will recur).

'Designated point of responsibility'

A point nominated within the NSA to receive the audit report and undertake appropriate actions in accordance with ESARR 1 with regard to the findings of the audit.

(NOTE: see ESARR 1 Section 6.6 b and c

Initial oversight

The process undertaken by a designated authority to gain objective information to enable a decision to be made to permit an organisation to operate in a particular field.

(NOTE: in the context of ESARR 1, and depending on the existing regulatory framework, that decision could be related to:

- *The issuance or renewal of a certificate, or*
- *The designation or renewal of a designation of an organisation holding a certificate to provide services within specific airspace blocks, or*
- *The proposed operation of new systems and changes to the ATM system)*

National Supervisory Authority (NSA)

A body nominated or established by States which is independent of service providers at least at a functional level and according to the existing regulatory framework supervises the implementation of requirements applicable to the provision of ATM services to general air traffic.

Term ***Definition***

On-going oversight
The process undertaken by a designated authority to verify that regulatory objectives and requirements are continuing to be effectively met.

Safety regulatory audit
A systematic and independent examination conducted by, or on behalf of, a National Supervisory Authority to determine whether complete safety-related arrangements or elements thereof, to processes and their results, to products or to services, comply with required safety-related arrangements and whether they are implemented effectively and are suitable to achieve expected results.

Safety oversight
The function undertaken by a designated authority to verify that safety regulatory objectives and requirements are effectively met.

Verification
Confirmation through the provision of objective evidence that specified requirements have been fulfilled.

See ESARR 1 for other terms and definitions relevant to auditing in the context of the safety oversight process in ATM.

(Space Left Intentionally Blank)

PART 1 – GUIDANCE FOR NSA SENIOR AND MIDDLE MANAGERS

4. INTRODUCTION TO AUDITING AND ITS MANAGEMENT

4.1 What is an Audit ?

Auditing[2] is a process used to obtain **independent evidence** that will provide confidence in the effective operation of a management system that has been designed to enable an organisation to meet defined objectives.

"Management System" is the International Organisation for Standardisation defined term used to describe a set of organisational policies, objectives, responsibilities and processes used to achieve organisation's overall functional objectives. The management system, together with the human and physical resources function, provides the organisation's product or service.

Sometimes a management system needs to be designed to incorporate system elements that focus on very specific objectives that must be met by the organisation, such as safety, quality or environmental performance and including also the need to comply with regulations which may relate to one or more of these, such as the applicable safety regulatory requirements. In many modern enterprises there is one system designed to cater for a diverse range of objectives, including those that must comply with regulatory requirements.

When there is a need to verify that a management system satisfies specific regulatory requirements for the purpose of granting some form of approval[3], then the audit is often termed "Initial Oversight" or an "Assessment". In these cases the audit is undertaken in two stages, with stage one involving a full review of the documentary evidence of the organisation's management system against the requirements that must be met and undertaken by the audit team off site, followed by stage two which requires the audit team to conduct on-site audit activities to verify that the declared and documented management system is being used and is effective in satisfying the requirements.

Auditing needs to be undertaken by those who are sufficiently independent of the actual processes being audited in order to be able to provide impartial, objective and unbiased information to those who need to make decisions concerning the adequacy of the processes to meet defined objectives and the need for any corrective action.

In the ATM context, safety regulatory auditing is auditing organised by an NSA in order to obtain confidence in the ability of the service provider to operate an effective management of safety which meets the applicable safety regulatory requirements and provide a safe service.

[2] *As pointed out in Section 1.2 above, the guidance in this document normally uses the term 'audit' in relation to its specific application to ATM safety oversight in the form of 'safety regulatory audits'. Throughout the text, both terms can be considered synonyms unless a different meaning is explicitly indicated.*

[3] *EAM 1 / GUI 5 is being developed by the SRC to provide specific guidance on the implementation of ESARR 1 in the context of a certification scheme, such as the one established by Regulation (EC) 550/2004 in EU Member States.*

ATM service providers achieve that effective management of safety through the implementation, consistently with the existing regulatory framework, of various organisational policies, objectives, responsibilities and processes. They will constitute the equivalent to the ISO notion of "management system" and are normally developed, but not necessarily limited to, around the implementation of a Safety Management System[4].

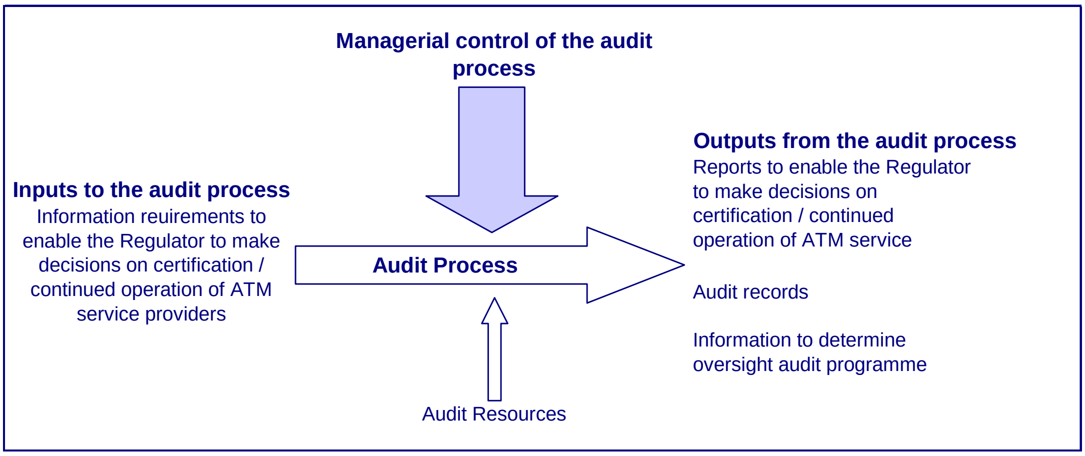
4.2 The Need to Manage the Audit Process and the Auditors

The management of an organisation performing audits should always be in full control of the audit process and of the auditors. This has significant implications where auditing is used as an integral part of a safety oversight process.

In the case of NSAs, they should ensure that their safety regulatory audits are organised in a manner which provides the NSA with sufficient information upon which judgments in relation to the initial oversight and continued operation of ATM service providers can be made, or further regulatory actions justified if necessary.

NSA management should therefore be in full control of their safety regulatory audit process and also in control of the NSA staff involved in audit activities.

If it has been chosen to delegate the auditing activity to a "recognised organisation" the NSA should be satisfied about the adequacy of the recognised organisation's management and also the adequacy of the audit process implemented by that organisation, recognising that the NSA cannot delegate their ultimate responsibility for the overall adequacy and effectiveness of the safety oversight process.


Managerial control of the audit process
Inputs to the audit process
Information reuirements to enable the Regulator to make decisions on certification / continued operation of ATM service providers
Audit Process
Outputs from the audit process
Reports to enable the Regulator to make decisions on certification / continued operation of ATM service
Audit records
Information to determine oversight audit programme
Audit Resources

[4] *In this document various expressions are used to describe the 'management system' used by a service provider to meet the 'applicable safety regulatory requirements'. This includes the terms 'management of safety', 'safety-related arrangements' and 'provider's arrangements'. None of these terms are necessarily confined to the arrangements specifically intended to implement a safety management system in accordance with ESARR 3.*

ESARR 3 requires the implementation of a Safety Management System (SMS) for the provision of ATM services. In EU Member States, this requirement will be consistent with the SES Common Requirements incorporating that ESARR 3 obligation into Community law. However, it should be noted the term "applicable safety regulatory requirements" as defined in ESARR 1 can include provisions not specified in the text of ESARR 3 and/or the SES Common Requirements specifically intended to regulate SMS. In the context of SES, this is the case of:

a) Other common requirements on technical and operational competence and suitability to provide ATM services, and

b) The interoperability implementing rules.

4.2.1 The Audit Management Function[5]

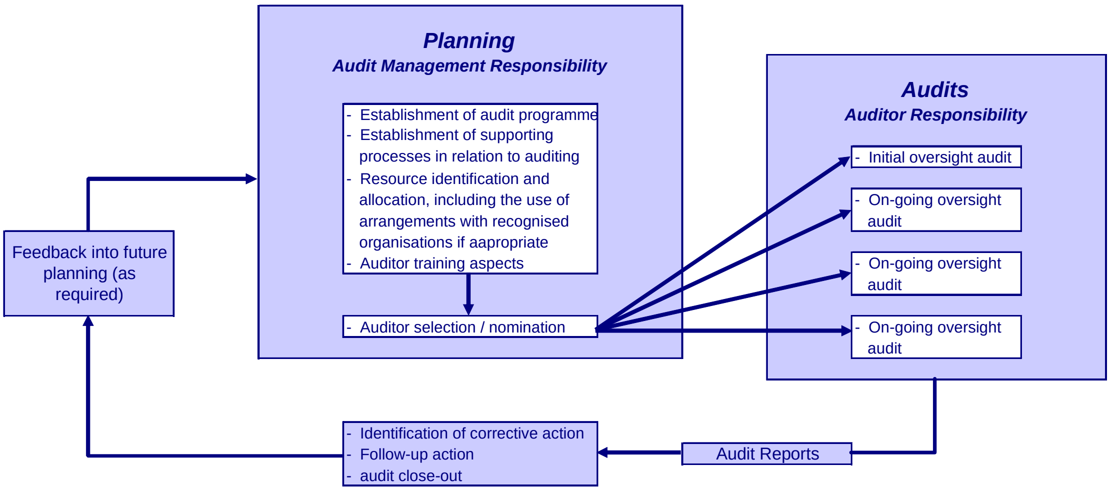
Although not explicitly required in ESARR 1, the need for this function stems from the ESARR 1 provisions related to the determination and implementation of an annual programme of safety regulatory audits.

It is necessary for an NSA to ensure that safety regulatory audits are effectively managed. In particular, audits need to be organised[6] in a planned and systematic manner to provide the NSA management with appropriate information to support the initial oversight and the on-going oversight of ATM service providers.

Consequently, an audit management function should be established in the NSA. Various internal organisational arrangements could be suggested to set up this role. However, such a function should always be able to plan and schedule the audit activities utilising the available audit resources in the most effective manner to ensure that the implementation of applicable safety regulatory requirements is verified.

The audit management function should normally determine, implement and follow up the **annual programme of safety regulatory audits** required in ESARR 1. The rationale is that this programme constitutes a major tool for the management of the audit process.

The detailed tasks of the audit management function will stem from its role as regards the annual programme and will cover a wide range of activities related to it. These are discussed further in Section 5 of this document.


Planning
Audit Management Responsibility
- Establishment of audit programme
- Establishment of supporting processes in relation to auditing
- Resource identification and allocation, including the use of arrangements with recognised organisations if aapropriate
- Auditor training aspects
- Auditor selection / nomination
Audits
Auditor Responsibility
- Initial oversight audit
- On-going oversight audit
- On-going oversight audit
- On-going oversight audit
Feedback into future planning (as required)
- Identification of corrective action
- Follow-up action
- audit close-out
Audit Reports

(Figure 2 - Management aspects in the audit process)

In line with other professional organisations, the NSA management should also consider the advisability of monitoring the effective implementation of their safety regulatory audit process to ensure that it meets their needs and discharges their international regulatory obligations in a manner demonstrable to third parties if so required. Some regulatory authorities use an internal audit process as a means of monitoring their continued compliance with their own safety regulatory audit process. NSAs will also be subject to external auditing from ICAO (IUSOAP) and EUROCONTROL SRC (ESIMS). In addition, within the Single European Sky framework the NSAs will also participate in "peer reviews" to be organised by the European Commission.

[5] *Sometimes simply referred to as "Audit Management" in some of the sections of this document.*

[6] *It should also be noted that, in the context of SES framework, the NSAs are explicitly required to "organise" the activities implemented to supervise compliance with requirements.*

TO NOTE THAT: NSAs and recognised organisations commissioned to undertake audits on behalf of an NSA should develop documented procedures to be followed by their auditors. Such procedures should as a minimum reflect the requirements of ESARR 1 and the guidance in this document.

4.3 Approach to Auditing in ATM Safety Oversight

Auditing is now accepted and recognised as a very valuable component of the overall approach to safety oversight.

Whilst there are other activities undertaken as part of safety oversight (not the subject of this guidance document), auditing provides valuable information to an NSA upon which to base judgments[7] relating to the initial or continued operation of the ATM service provider.

A basic principle of auditing is that it is a systematic, impartial and objective approach to obtaining information that will provide for a level of confidence in an organisation's ability to manage key processes. If correctly undertaken audits will avoid subjective judgments that could lead to incorrect conclusions. It is a requirement of the auditor to provide factual evidence of noncompliance, and not to rely on the auditor's own opinion or statements made by those being audited.

The overall process of safety regulatory auditing may be broken down into two separately identifiable sub-processes, each needing to be managed effectively to ensure that the full benefits of auditing are obtained.

- ❑ The first sub-process is the physical act of auditing to verify that the management of safety is in place and is functioning effectively.
- ❑ The second sub-process is concerned with making decisions on the need for correcting any system weaknesses that have been revealed by the audit.

4.3.1 The Audit Process

Auditing may be considered to involve two separate activities. The first is the **investigation and the gathering of factual information.** This is the audit process itself. The second is the process of correcting identified weaknesses.

Auditing is a process requiring an independent auditor to search for evidence in order to verify that a system is functioning in the way that the organisation has declared that it should function in order to meet higher level objectives such as applicable safety regulations. The regulations together with the declared system (as defined for example in the form of a Safety Management System - SMS) will be the auditor's baseline against which the verification is performed. The audit will always be a sampling activity, never a 100% check, and is designed to provide confidence in an organisation's ability to meet applicable regulatory requirements and to operate a safe system.

Auditors are required to undertake a very difficult and complex task. This task can be made even more difficult when those being audited do not understand the process and the approaches that the auditors need to take to obtain their information.

[7] *For example, wherever the need is identified for some form of restrictions on operational activities or wherever further regulatory action is needed due to continued non-compliance with regulations in situations where the continuation of operations is necessary or highly desirable.*

The basic task of an auditor to is to obtain factual evidence that an organisation is complying with a set of requirements. This requires the auditor to search for this evidence with the cooperation of those that they are auditing but in a way which will ensure that the evidence is not artificial or biased as a result of those being audited making the decisions as to what the auditors actually see and hear. Auditors need to have free access to staff at all levels in an organisation, and to be in total control of where they go, who they speak with and what they look at and examine. The factual evidence will be collected by conducting interviews with key staff and those involved in undertaking work tasks, examination of documents and observation of work activities and general conditions in the areas being audited.

Unless the auditors remain in control of this process of information gathering the results will always be of limited value.

For example, it is usually very easy for a manager to explain how a process works and then showing the auditors some examples of documents or records that will demonstrate effective process performance. The auditor needs to see not just an example of how the process works but must test the process to see that it has been, and continues to work in the way that the organisation wishes it to work (as described in procedures or stated by managers). The auditor is searching for evidence and may only judge that a situation is incorrect if the facts prove this. It is a fundamental principle of auditing that those audited must always be judged to have followed the process unless the auditor can prove otherwise. Audits therefore involve the collection of evidence in order to verify that what should be happening is actually happening. This requires the auditor to work with information obtained from interviews and questioning of staff and undertaking the necessary investigations to find the evidence that proves conformity or nonconformity as the case may be.

Auditors will need to consider in advance of the audit what evidence that they require and a general plan or strategy that will be adopted to obtain this evidence in a systematic and unbiased way. They will need to undertake sufficient audit planning in advance of the audit. Throughout the audit process auditors should always try to identify the extent of any problems found as this could significantly effect the corrective action that may be required of the ATM service provider.

TO NOTE THAT: NSA management should be aware of the resource requirements necessary to enable sufficient planning to be undertaken by auditors.

4.3.2 The Corrective Action Process

Once the audit findings have been communicated to the audited organisation we then enter what is called the **“Corrective Action”** process.

The term “Corrective Action” has a specific meaning that relates to the action taken to eliminate the cause of a problem or system weakness. It is not the term that should be used to refer to the action taken to eliminate the symptom. For example a medication such as aspirin is often used to alleviate an undesirable headache, however the aspirin does not deal with what has caused the headache, such as stress or dehydration, it only acts to minimise the effect. Corrective action in response to a headache requires the identification of what has or is causing the headache and then implementing the necessary action to remove the cause, such as taking appropriate rehydration therapy in response to a headache caused by dehydration.

For audits that have been undertaken there will often be a requirement for the audited organisation to respond to the audit findings within a reasonable timeframe with appropriate corrective actions.

The purpose of the corrective action process is to identify the **“root cause”** of the problem that has resulted in the nonconformity found by the auditor, and then to determine a suitable corrective action that will address the root cause and so prevent future similar nonconformities. The root cause is usually a system weakness which is the responsibility of the management of the audited organisation to correct. (Sometimes a staff member may be identified as being a root cause, however most staff failings can be traced back to a system weakness that has resulted in staff poor performance, for example lack of effective training, communication of requirements, etc.).

In order to respond to an audit nonconformity and determine a suitable corrective action that addresses a root cause it is necessary for the management of the audited organisation to initiate the necessary investigation to establish if the audit finding was an isolated incident or an endemic situation, and also to fully identify what has given rise to the audit finding, i.e. the weakness in the system. There is often a tendency for such investigations not to be undertaken and instead to simply guess at what might have caused the problem. Working without factual data is not a good approach to solving problems.

Having undertaken an appropriate investigation and determined a likely root cause the proposal for corrective action will need to be sent to the NSA for formal review and agreement. Following the auditing organisation’s agreement the corrective action will be implemented and at a later time some form of re-audit should be undertaken to verify that the implemented corrective action has indeed resulted in the elimination of further similar nonconformities.

Such re-audit activity results in the original audit finding being **“closed out”** if it is verified that the corrective action has effectively eliminated the root cause and ‘symptoms’ as found on the original audit are no longer evident. It may not always be necessary to undertake corrective action in relation to simple and straightforward audit findings. Some findings may be simple isolated documentation errors and omissions that the auditor has identified as being non systemic, that are easily corrected and require no ‘root cause’ determination.

4.3.3 Considering the Processes and their Results

Audit verification activities will need to be undertaken in relation to specific processes forming an integral part of the management of safety, together with outputs provided by processes in the form of information, tangible product and ultimately service provision. Approaches to audit need to recognise that compliance with procedures will **not necessarily in themselves ensure adequacy of process outputs** (and ultimate ATM service provision outcomes) unless the procedures are appropriate, well engineered and developed in relation to the level of competence of those required to use the procedures.

Accordingly, the audits address the processes and/or the products/services[8] depending upon the case. In fact, ESARR 1, Section 5.1 requires the verification of compliance with applicable safety regulatory requirements and any arrangements needed to implement them. Two complementary levels of verification and their related references are defined in ESARR 1 Section 6.2, bullet (e):

[8] *Irrespective of their nature, the “products” are the final outputs of a process. Within the ATM environment, and for the purpose of ESARR 1, the “ATM services” are normally the “products” under consideration.*

i. Established arrangements against required arrangements;

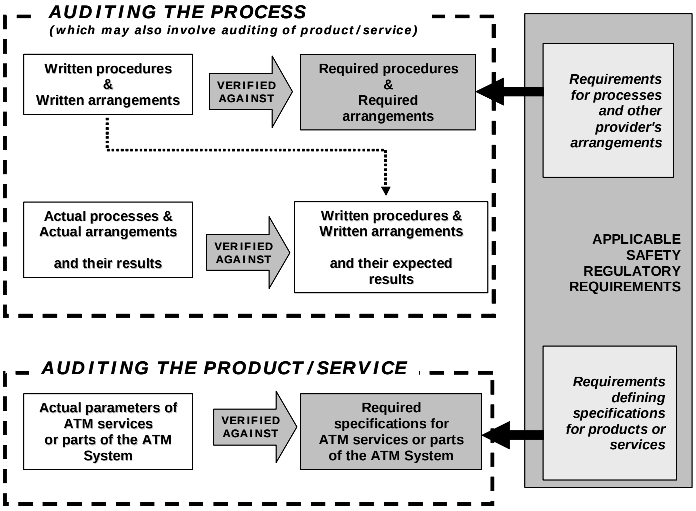
ii. Implemented arrangements and their results against established arrangements and their expected results

A case in point is the implementation of Safety Management Systems (SMS) in accordance with ESARR 3, where those points may correspond with:

i. The SMS Manual against ESARR 3

ii. What actually happens against the SMS Manual

The following figure illustrates these notions:


AUDITING THE PROCESS
(which may also involve auditing of product/service)
Written procedures & Written arrangements
VERIFIED AGAINST
Required procedures & Required arrangements
Actual processes & Actual arrangements and their results
VERIFIED AGAINST
Written procedures & Written arrangements and their expected results
AUDITING THE PRODUCT/SERVICE
Actual parameters of ATM services or parts of the ATM System
VERIFIED AGAINST
Required specifications for ATM services or parts of the ATM System
Requirements for processes and other provider's arrangements
APPLICABLE SAFETY REGULATORY REQUIREMENTS
Requirements defining specifications for products or services

(Figure 3 – auditing in relation to processes and products)

These principles imply that NSAs will need to arrange for safety regulatory audits to focus on verification of the **effective implementation** of the organisational policies, objectives, responsibilities and processes used to achieve the organisation’s overall functional objectives in accordance with the applicable safety regulatory requirements.

This implementation can only be judged to be effective if all components of the ATM service are performing satisfactorily. Consequently, an audit will almost certainly have to sample, for example, the effective functioning of equipment that contributes to the safety of the ATM system. This might therefore require examination of the process used by the ATM service provider to identify the performance criteria to provide assurance that the equipment is suitable to support the ATM service and audit that such performance criteria have been met in the past (through audit of maintenance records) and continue to be achieved (through audit of current performance, either by the audit team or by suitably competent independent third party).

4.3.4 Auditing versus Inspection

In carrying out their responsibilities, NSAs will commonly refer to those who are involved in the verification of compliance with applicable safety regulations as *‘auditors’* or *‘inspectors’* (or some other term). Irrespective of the term that may be used to describe these individuals, **auditing is the safety oversight tool** used to verify compliance with the applicable safety regulatory requirements.

The use of the term *'inspector'* by an NSA can sometimes cause misunderstandings and confusion and it is important to recognise that for safety oversight purposes, auditing will always be used. In particular, it should be noted that service providers will normally employ a variety of techniques, including, for example, internal audits, inspection and monitoring of the service or components of the service, in order to meet specific requirements or for other business reasons.

Within a management systems context consistent with the ISO approach, the term *"inspection"* is normally reserved for the internal verification activities that are necessary to maintain the required standard of product or service outputs. As such this activity will form an integral part of the 'implemented arrangements' of an ATM service provider to achieve organisational safety objectives. Such verifications being performed as an integral part of the day to day activities (i.e. an integral part of the process) and undertaken by those with the responsibility for product or service provision. Auditing however is a completely independent activity, performed by staff not directly involved in product or service provision and is designed to provide confidence that the overall management system and product and/or service provision processes, including the necessary inspection activities are being undertaken and effective in the achievement of the organisations objectives.

TO NOTE THAT: NSA managers and auditors will need to clearly understand the difference in the use of such terminology in order to fully comprehend the process management and control techniques that may be used by ATM service providers as part of their management of safety. A lack of such understanding could lead to serious weaknesses in the management of safety implemented by ATM service providers

(Space Left Intentionally Blank)

5. BASIC ARRANGEMENTS FOR AUDITING

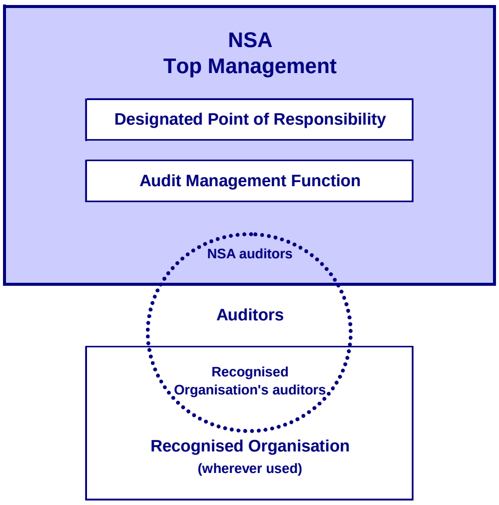
5.1 Responsibilities and Accountabilities

The implementation of a safety regulatory process by a NSA requires the establishment of clear responsibilities as regards programming, resourcing, conduct and follow up of safety regulatory audits.

Within the NSA, responsibilities with regard to auditing can be identified in relation to:

- ❑ The NSA top management
- ❑ The audit management function
- ❑ The designated “point of responsibility” required in ESARR 1
- ❑ The auditors[9]

There are many possible ways to establish effective organisational arrangements within an NSA to provide for the necessary functions required in regard to safety regulatory auditing. However, any possible combination of roles should specifically ensure the existence of a “designated point of responsibility” with responsibilities consistent with ESARR 1 and the establishment of an audit management function.


NSA
Top Management
Designated Point of Responsibility
Audit Management Function
NSA auditors
Auditors
Recognised Organisation's auditors
Recognised Organisation
(wherever used)

(Figure 4 - Identification of key roles with regard to auditing)

5.1.1 Top Management Responsibilities

The NSA top management:

- ❑ Has an overall responsibility for the safety oversight activity, including the safety regulatory audit process;
- ❑ Is responsible for resourcing the various functions.
- ❑ Is responsible for meeting the requirements established in ESARR 1 and the rest of the existing regulatory framework.
- ❑ Subject to the existing legal framework, is (normally) responsible for decisions to impose the sanctions foreseen in the applicable regulatory framework. In the context of the ongoing oversight of ATM service providers these decisions should be normally based on objective evidence obtained from safety regulatory auditing.

[9] *Responsibilities for auditors are addressed in Section 7 of this document.*

- ❑ In the SES context, is responsible for issuing / renewing the service provider's certificate[10] after, amongst other things, compliance with applicable safety regulatory requirements is demonstrated and verified by means of appropriate safety regulatory audits

In many cases the NSA senior management may be far from the practical day to day oversight mechanisms and may therefore delegate and rely on the organisational structure to discharge its responsibilities in relation to safety regulatory auditing activities.

However the NSA top management cannot delegate its ultimate accountability for the effective operation of the safety regulatory auditing processes and should therefore be fully involved in the establishment of the appropriate organisational arrangements and the **effective resourcing** of the various functions involved.

The role of the NSA top management may be particularly important when an NSA elects to commission a "recognised organisation" or where one NSA is cooperating with other NSAs in the conduct of joint audits or auditing in relation to Functional Blocks of Airspace. In some of these situations, high level agreements decided at top management level may normally be needed between various organisations.

As these specific cases imply the need to interface with other organisations, proper terms of reference should be defined to ensure the effectiveness, clarity and transparency of the audit process. Consequently, the NSA top management should pay particular attention to the establishment of these types of arrangements wherever they are needed and make sure their effectiveness.

> ***TO NOTE THAT: the NSA top management has an overall responsibility for the safety regulatory audit activities and should resource the functions to conduct them. More specifically, there should be adequate and competent audit resources available to the NSA to conduct audits in accordance with the audit programme. These may be the audit resources of the NSA itself or may be the resources of a "recognised organisation" commissioned by the NSA to undertake safety regulatory audits on its behalf.***

5.1.2 The Designated Point of Responsibility

ESARR 1 Section 6.6 requires the identification of a designated "point of responsibility". This point of responsibility must be kept within the NSA and should:

- ❑ Receive the audit report produced by the auditors.
- ❑ Ensure that the audit findings are communicated to the senior management of the organisation audited;
- ❑ Request corrective action to address the non-conformities identified
- ❑ Assess the corrective actions determined by the auditee, and accept them or not.
- ❑ Undertake additional actions if required, such as providing inputs to:
  - a) Support the decisions related to the initial oversight (e.g issuance/renewal of certificates in the context of SES).

[10] *EAM 1 / GUI 5 is being developed by the SRC to provide specific guidance on the implementation of ESARR 1 in the context of a certification scheme such as the one established by Regulation (EC) 550/2004 in EU Member States.*

[12] *ESARR 1, Section 6.3, requires a NSA to establish an annual programme of safety audits. As explained in EAM 1 / GUI 1 (Explanatory Material on ESARR 1 Requirements) the term 'annual' means that the programme should be subject to review and update on an annual basis.*

b) Allow the Audit Management Function to maintain and refine the Annual Programme of Audits (e.g. as regards follow up audits).

c) Inform the NSA Top Management as regards the need for sanctions in accordance with the existing regulatory framework.

ESARR 1 does not use the term ‘client’ from the ISO-related bibliography. However, the concept of an audit ‘client’ is important and should be understood by the auditors and those who are managing audit processes, to ensure that relative responsibilities of auditors and NSA management are clearly understood.

In the context of ESARR 1, **auditors have a “client”** in the form of a designated “point of responsibility” in the NSA. Audit reports, including details of non-conformities, will be forwarded by the auditors to this “point of responsibility”. Once the audit has been completed and the information provided to the “point of responsibility” it is his/her role to take the necessary action(s) resulting from the audit.

The designated “point of responsibility” manages the corrective action process and collects all the information related to the audit in order to channel the appropriate information to the various NSA functions which make decisions on aspects such as the issuance and renewal of certificates, the safety oversight aspects related to the designation of providers, the sanctions, etc.

In practical terms, **the designated “point of responsibility” is the “client”** of the audit, and therefore, the designated point of responsibility plays the role of the third vertex of the classical triangle ‘auditor-auditee-client’ as presented in the ISO related bibliography. However, it should also be noted that the designated “point of responsibility” **will normally act on behalf of an “ultimate client”** (e.g. the NSA top management, the NSA certification management, etc) who makes decisions related to the initial oversight or continued operation of service providers in the light of the information obtained.

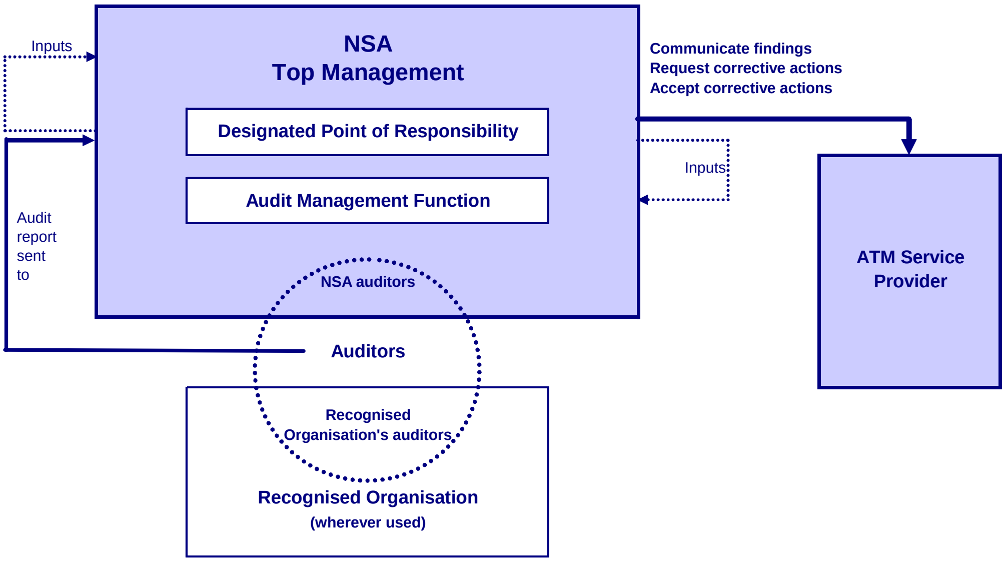
The role of the “point of responsibility” also involves triggering other actions needed in the NSA in the light of the audit findings. More specifically the “point of responsibility” shall provide appropriate information to support the NSA decisions related to the initial oversight of service providers or the initiation of procedures to sanction them.

It should be noted that the initial and ongoing oversight of service providers, as well as the procedures related to sanctions, are all processes which require information from the audit process. In the context of ESARR 1, the designated “point of responsibility” **is not necessarily involved** in producing the outcomes from these NSA processes beyond providing the information obtained from auditing. In fact such involvement is neither required nor prevented by ESARR 1. Therefore it will ultimately depend on the organisational arrangements internally established within the NSA.

Different organisational arrangements could be proposed to meet the ESARR 1 requirements as regards the designated “point of responsibility” in a manner consistent with the guidance of this document. The solution adopted will probably depend on the organisational size of the NSA and its level of activity. In any case, it should be noted that, in the light of ESARR 1, **nothing prevents an NSA from**:

❑ Combining the role of the designated “point of responsibility” with other functions such as the audit management function, the function responsible for issuing a service provider’s certificate in the context of SES, or other roles.

- ❑ Appointing different designated “points of responsibilities” for different audits or different types of audits.



(Figure 5 - the role of the 'designated point of responsibility')

Once the audits have been undertaken and the information provided to the designated “point of responsibility”, it is then the responsibility of the “point of responsibility” to **decide if any corrective action is necessary** and by when, although this does not preclude the audited organisation from taking any corrective action in advance of action requested by the “client”. He/she will either need to liaise directly with the audited ATM service provider or request the audit management function to undertake this task on their behalf. By this means NSA senior management may remain fully in control of the audit mechanism, the auditors merely providing information as necessary.

The designated “point of responsibility” should receive and analyse audit results, and determine the need for, and timescales of, corrective actions. However whilst retaining the full responsibility and accountability in relation to the effective operation of these activities it may nevertheless delegate some or all of these to the audit management function.

It is important to recognise that for any type of audit there is a reason for the audit needing to be performed, and that reason is to provide impartial and unbiased information that provides the assurance of operational effectiveness to a higher authority and enables that higher authority to make decisions relating to allowing the continued provision of services.

The audit process therefore always has a ‘client’ who requires the audit information, and the audit process must be managed effectively to ensure that the client is provided with the requisite information upon which decisions and judgments may be based. This “client” is referred to in ESARR 1 as the designated “point of responsibility”. **<u>It should not normally</u>** be the task of the auditors to decide what is important to be corrected and how quickly it should be actioned. Many auditors feel that it is their right to demand corrective action, forgetting that they are there only to serve the needs of the 'client' and it is for the client to decide if corrective action is necessary together with associated timescales. These complex relationships should be first understood before an NSA puts in place structures and resources to undertake safety oversight audits.

***TO NOTE THAT:** in some NSAs where the auditors have a good deal of practical ATM regulatory experience the corrective action process may be delegated directly to the auditors. However this practice:*

- ❑ ***Should be exceptional and could only be justifiable in situations where immediate action is needed to address a significant safety issue;***
- ❑ ***Is not possible wherever recognised organisations are used to conduct the audit on behalf of the NSA***
- ❑ ***Does not remove the ultimate responsibility for demanding corrective action from the NSA management through its designated "point of responsibility", as established in ESARR 1.***

5.1.3 Audit Management Function

The auditors and the audit process need to be managed effectively in order to provide the NSA, through its designated "point of responsibility", with sufficient and adequate information upon which to base judgments concerning the initial oversight and the continuous operation of ATM service providers.

Such a need provides the rationale for the identification of an audit management function in the NSA, which should normally be associated with the management of the annual programme[12] of safety regulatory audits.

Accordingly, an audit management function established within the NSA should:

- ❑ Develop and maintain the **annual programme of safety regulatory audits**, and be responsible for its implementation in relation to all ATM service providers operating under the responsibility of the NSA;
- ❑ As part of the **management of the annual programme**, ensure that audits are pre-planned and systematically sample the service providers processes and related outputs to ensure that over a period of two years[13] sufficient confidence is obtained in relation to all applicable safety regulatory requirements in all the functional areas of relevance to allow for continued operation of the service provider;

  More specifically, the annual programme of safety regulatory audits should:

  a) Cover all the areas of potential safety concern and focus, but not exclusively, on those areas where problems have been identified as a result of monitoring safety performance,

  b) Include audits to address all the ATM service providers and the different ATM services operating under their responsibility,

  c) Conduct sufficient audits, over a period of at least once every two years, to check the compliance of all ATM service providers under their responsibility with applicable safety regulatory requirements in all the functional areas of relevance,

  d) Include sufficient audits to follow up the implementation of corrective actions intended to address non-conformities found in previous audits,

[13] *ESARR 1 requires an NSA to conduct sufficient audits, over a period of two years, to check compliance of all ATM providers in all areas of relevance.*

e) Allow for the modification of the objectives of pre-planned audits, and the inclusion of additional audits to those originally programmed, wherever that need is identified in the safety oversight activities of the National Supervisory Authority.

f) Be based on sound considerations including identified safety risk, confidence in the service provider and previous audit results and **not** on the limitations of audit resources available to the NSA.

□ Ensure that audits performed as part of the safety oversight process are properly planned, undertaken and reported, in accordance with **appropriate procedures**.

□ Ensure that audits are conducted by appropriately qualified and competent auditors of the NSA or recognised organisations commissioned by the NSA. This should normally include:

a) Selecting the auditing staff (or accept it wherever recognised organisations are involved).

b) Identifiying **qualification criteria for auditors** consistently with the requirements of ESARR 1 (see Section 5.7 and Appendix J of these guidelines) and supplying the required levels of training for the auditors of the NSA and the recognised organisations working on its behalf.

□ Ease the **uniformity of the auditor's performance** from audit to audit. Amongst various measures this may, for example, include:

a) Providing harmonised tools (e.g. forms) and guidance material for its use by auditors,

b) Monitoring the auditor's individual performance,

c) Ensuring the interchange of auditing personnel between groups,

□ Monitor **audit effectiveness**, by means of specific actions which may include:

a) Direct consultation with the clients of the audits including the point of responsibility designated in accordance with ESARR 1 and other NSA management functions involved in decision-making based on the findings from audits.

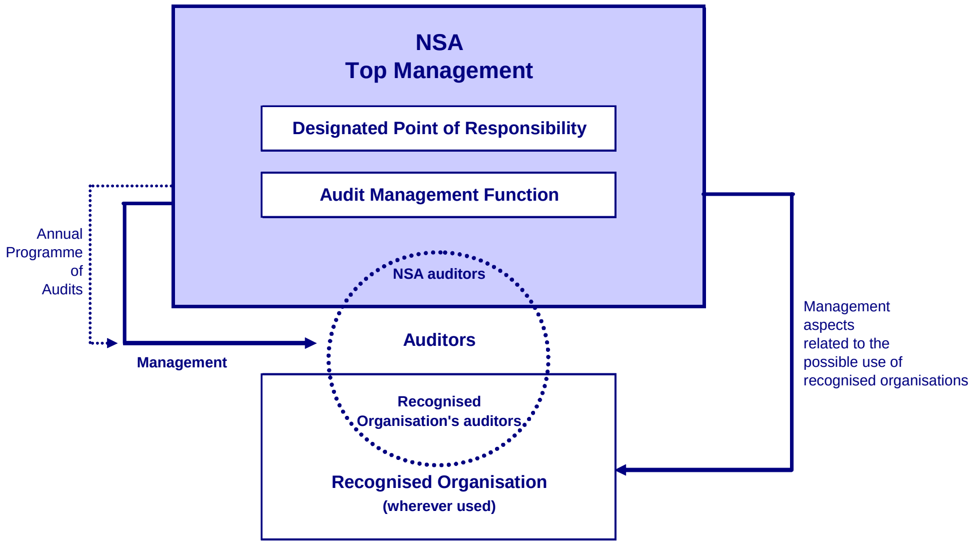
b) Obtaining feedback from the auditees in a systematic manner, for example by means of questionnaires or regular surveys.

c) Obtaining feedback from the auditors themselves on the adequacy of the time / resource allowed for the conduct of audits which in turn impacts on the ability to achieve audit objectives.

□ Evaluating the **resources necessary** to implement the annual programme of safety regulatory audits and bringing any additional resource requirements to the attention of NSA top management.

□ Wherever applicable, manage[14] the **possible use of recognised organisations** by the NSA, including those aspects related to the rationale for the NSA decisions on the possible use of a recognised organisation in accordance with ESARR 1, Section 8.

[14] *Subject to the conditions in the regulatory framework for the delegation of supervisory tasks, a NSA may decide to commission recognised organisations to conduct safety regulatory audits on their behalf. ESARR 1 establishes that such a decision shall be based upon a specific demonstration provided by the recognised organisation to satisfy the NSA that the recognised organisation meets the criteria identified in ESARR 1, Section 8.2. For further details on these aspects, refer to EAM 1 / GUI 1 (Explanatory Requirements of ESARR 1 Requirements).*


NSA
Top Management
Designated Point of Responsibility
Audit Management Function
NSA auditors
Auditors
Recognised Organisation's auditors
Recognised Organisation
(wherever used)
Annual Programme of Audits
Management
Management aspects related to the possible use of recognised organisations

(Figure 6 - the role of the audit management function)

Different organisational arrangements could be proposed to establish the audit management function and cover the various responsibilities referred to above. The arrangements adopted will normally depend on the organisational size of the NSA and its level of activity. For example, in larger NSAs the audit management function may be a large division with regional offices. In any case, it should be noted that, **nothing prevents an NSA from**:

- ❑ Allocating the audit management function to the NSA personnel responsible for conducting the audits, notably in the case of small NSAs;
- ❑ Combining the audit management function with the role of the designated "point of responsibilities" or other safety oversight functions;

Wherever the designated "point of responsibility" and the audit management function are not combined, the audit management function is responsible for liaising with the designated "point of responsibility" to determine the audit information needs and then plan the annual programme of audits and arrange for suitable resources to provide this information. It should be recognised that for certain information auditors with very specialist knowledge and experience may be required.

5.1.4 Specific Roles with regard to Certification

Section 7 of this document addresses the roles and responsibilities of audit team leaders and team members. This material is applicable to all audit activities, irrespective of whether it is part of an initial or on-going oversight process.

In the context of an initial oversight conducted as part of a certification scheme, such as the one established in the EU Member States by Regulation (EC) 550/2004, it is common to use the expression "certification team". The roles and responsibilities of the certification team members will normally be equivalent to those described for the audit team leader and team members in Section 7 of this document, on the basis that auditing constitutes the core activity of the certification exercise. However, some additional responsibilities could exist due to the specific procedures intended to implement the certification scheme established in the applicable regulatory framework.

In addition, certification will normally need the identification of a focal point or function in the NSA for the receipt and management of applications for certification. This function will depend on the size and organisational arrangements of the NSA and the number of potential applicants. It may therefore be combined with other roles in the NSA. The function could be assumed by the Audit Management Function or the Certification Team depending upon the case.

EAM 1 / GUI 5 is being developed by the SRC to provide further guidance on these aspects.

5.2 Resource Planning

NSA senior management will need to ensure that there is sufficient audit resource to undertake safety regulatory audits, including those undertaken as part of initial and on-going oversight, together with unscheduled audits or any additional necessary audits in response to noted problems or specific corrective action verification activities. They will need to identify both short and long-term audit resource requirements to meet their obligations for providing effective oversight of all ATM service providers operating under their responsibility.

Whilst there is not a simple formula by which an NSA may easily determine this level of resource, there are considerations which enable an estimation to made for the amount of resource that may be required to perform Initial and On-going Oversight of an ATM service provider.

5.2.1 Major Considerations in Determining Oversight Resources and Strategy

- ❑ Stage of development of the management of safety in the service provider organisation,
- ❑ Observed strengths and weaknesses in the documented management of safety,
- ❑ Level of service provider management maturity to safety management,
- ❑ Level of service provider staff maturity to safety management processes and techniques,
- ❑ Level of maturity of the management of safety itself,
- ❑ Level of NSA maturity to safety management processes and techniques,
- ❑ Level of NSA maturity / experience in respect of auditing,
- ❑ Overall safety performance of the service provider.

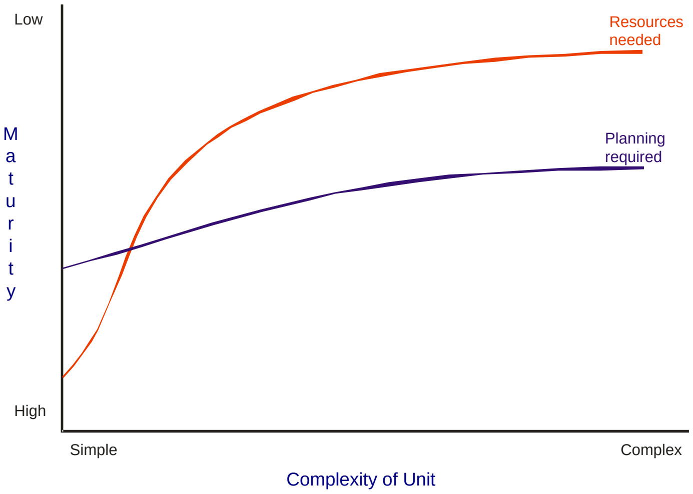
These considerations will also have an impact on the oversight strategy that will need to be adopted. Such strategy decisions relate to the determination of specific operations or activities of the ATM service provider together with those parts of the applicable safety regulatory requirements that will be the main focus of audit attention.

Potential weaknesses identified during the document review of the ATM service provider’s management of safety will also be used to determine the level of auditing activities to be undertaken throughout the ATM service provider organisation and in relation to specific regulatory requirements.

5.2.2 Implications of a Lack of Resources

TO NOTE THAT: A lack of resource provision by an NSA could lead to weak or totally unsatisfactory safety management systems development and implementation within ATM service providers with the consequence of potentially safety risk activities not being under effective control and hence increased safety risk to the air transport system.

From a general perspective the total resources (time, personnel, funding etc.) that will be required for an audit will vary from one audit to another. It is the responsibility of an Audit Team Leader to ensure that the resource requirement for a requested audit is adequately assessed and communicated to the audit management function.



The diagram opposite gives an indication of how the level of resource typically needed for an audit will vary due to the nature and complexity of an ATM service provider. Clearly, a relatively simple ATM unit with a mature management system - perhaps one that has been audited on many occasions in the past and found to be operating well - will demand less audit resources than a newly established unit undergoing initial oversight. However, as can be seen from the diagram, whilst the resource requirement for an audit reaches a plateau (limited by the amount of detail that can be efficiently covered within a single audit), the level of resource required quickly reaches this level.

Similarly, the amount of planning and preparation required for a ‘simple’ audit is little different to that required for a far more complex assessment and, again, quickly reaches a plateau.

It is difficult to translate the curves in the diagram into numbers of personnel or planning time required due to various factors and consideration, however audit team leaders can be expected to develop a better understanding of the resource needs for a specific audit as they develop greater experience. It is important, however, not to underestimate the level of resources that are require to successfully plan undertake and report an audit in a fully satisfactory manner.

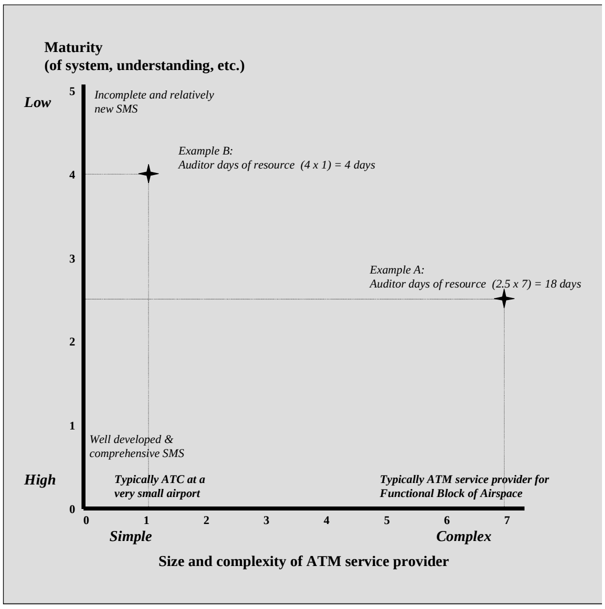
(Space Left Intentionally Blank)

An indication of the personnel resources required to conduct an Initial Oversight is as follows. Application of this approach is also indicated in Appendix A.

“Example A” might be one of the larger European ATC centres where the SMS has been developed over a period of some two years and the document review has revealed very few significant concerns.

“Example B” might relate to a small regional airport with very few movements per day and where the SMS has been recently developed and the document review has revealed several areas of concern.

*In addition, audit resource is also required to plan and report an audit, and **generally it can be estimated that a similar amount of audit resource will be required as that necessary to conduct the audit.***



*Therefore for the above examples the total resource that should be provisioned by an NSA should be **36 days for Example A and 8 days for Example B** respectively.*

5.3 Audit Reporting Requirements

The NSA should develop an **audit reporting process and report formats** (to support the NSA needs as regards Initial and On-going Oversight) that auditors are required to use as a means of communicating to the NSA the results of audits. These reports should be confidential to the NSA.

The following should be considered for inclusion in oversight visit reports:

- date of oversight visit,
- auditor(s),
- observers / specialists accompanying the auditors,
- objectives and scope of the audit,
- summary statement / audit conclusions,
- audit schedule *(areas of the service provider visited together with times spent in each area)*,
- overall status of this oversight visit in relation to the NSA annual programme of audits in relation to the organisation being audited,
- details of the specific management system elements / paragraphs sampled
- status of previously agreed corrective actions *(if forming part of this audit)*,
- reference documentation used to plan the audit,
- specific documentation/records reviewed during the audit,
- key staff interviewed,
- specific activities observed,
- details of identified non-compliances *(the NSA may have methods for determining significance)*,

- supporting details in relation to identified non-compliances,
- general audit observations,
- recommendations to the NSA by the auditor(s).

The following may also be considered for inclusion as attachments to the report:

- Auditor(s) check lists and associated notes,
- Copies of evidence (permission to use these should be obtained from the service provider),
- Auditor's notes relating to audit samples, responses to questions, requests for information etc.

If the above are not attachments to the report, the **retention of all these audit records** should be ensured.

Reporting methods should ensure that the identified non-compliances are accurately reported to the NSA, and remain **exactly** as communicated to the service provider before the audit team completed the oversight visit. The report may also express any opinions of the auditor or comments that the auditor wishes to make to the NSA regarding the noted situation in the service provider. However, it should be recognised that in some states data protection legislation could require reports to be accessible to the service provider if so requested.

TO NOTE THAT: Such opinions should not be used by auditors as a means of attempting to communicate non-compliances which they believe to exist but for which the auditor has failed to undertake the necessary investigations to reveal factual evidence of non-compliance.

The NSA should communicate as a minimum the following information to a service provider within a reasonable timeframe of the audit visit ***(good practice would suggest no more than 14 days)*****:**

- Date of oversight visit,
- Auditor(s),
- Observers / specialists accompanying the auditors,
- Objectives and scope of the oversight audit,
- Audit schedule *(areas of the service provider visited),*
- Details of non-compliances identified by the audit team *(including perceived significance)*,
- Response of the ATM service provider to identified non-compliances,
- Requirements for corrective actions,
- *(including timeframes - determined by perceived significance/impact on safety),*
- Considerations for investigations *(relating to auditor(s) general observations),*
- Intended NSA audit follow up action(s),
- NSA conclusions - *(relating to continued operation, limited operations, sanctions etc. - The NSA may use covering letters to communicate any conclusions reached).*

5.4 Audit Records Requirements

ESARR 1 Section 11.1 explicitly requires the NSA to keep, or maintain access to, the **appropriate records related to their safety oversight processes**.

The NSA will need to be able to demonstrate to third parties[15] that it is in full control of its safety oversight process and that judgments made relating to continued service provider operation are based on factual data. The NSA should also be able to demonstrate that corrective actions in relation to reported non-compliances are being monitored and effectively verified for adequacy, and that there is full justification for extensions to timescales for corrective action implementation.

Consequently, the NSA will need to set up a safety regulatory audit records system which will not only serve as a repository for all audit records, but will also provide a valuable source of data to be used for future safety oversight planning, and provide evidence of an effective audit process to third parties.

The NSA should ensure the retention and access to **the records of all audit activities and related results** including those listed in Section 5.3 above. ESARR 1 does not specify a minimum retention period. An appropriate policy for the retention of audit records should therefore be defined by the NSA.

Different records are likely to need different retention periods. If not for other consideration, all records should be kept, or maintained access to, **for at least** the maximum possible cycle between two visits from an international programme with responsibilities for auditing the implementation of ATM safety oversight frameworks established by States[16].

These policies and their associated procedures should also concern the reports and related records of audits conducted by recognised organisations on behalf of the NSA. In this case the NSA **may prefer to maintain access** to some audit records through specific arrangements with the recognised organisation.

TO NOTE THAT: audit records should comprise all documentation produced by the NSA in relation to the determination of audit programmes, and by the NSA and auditors throughout individual oversight visit audit planning, conduct, reporting, follow up and close out phases. Any retained audit evidence should also be entered into the audit record system.

It is important that the NSA has an adequate record and archiving system in place and that individual auditors understand that audit records are not their personal property but the property of the NSA. It may also be necessary in some States for NSAs to satisfy data protection requirements in relation to the retention of audit records, particularly where retained audit evidence is traceable to individuals.

(Space Left Intentionally Blank)

[15] *Including the audits from IUSOAP, ESIMS and the peer reviews to be organised by the European Commission.*

[16] *Such as IUSOAP, ESIMS and the peer reviews to be organised by the European Commission.*

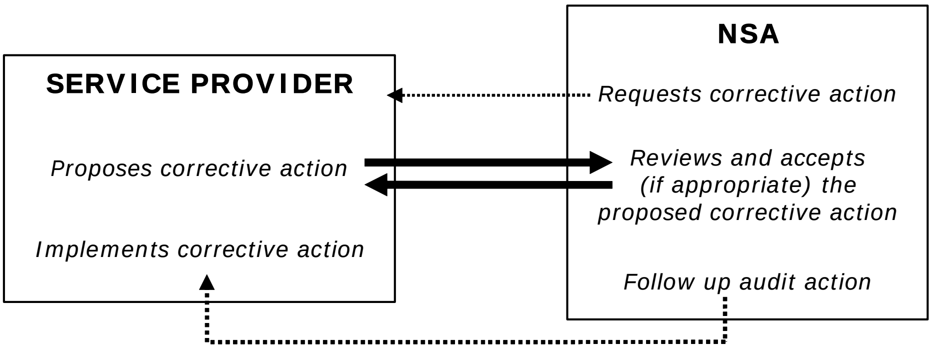
5.5 Corrective Action and Audit Close-Out

Once an audit is completed it is the responsibility of the management of the audited organisation to determine and propose corrective action. They are responsible for investigating the circumstances surrounding the reported nonconformities and determining likely root causes.

In far too many audit situations the proposed corrective action is a 'quick fix' addressing the symptom of the problem only and not dealing with a likely root cause. The NSA should be satisfied that corrective action proposed will deal with the root cause of the problem and when implemented is fully effective in eliminating the noncompliance found in a timely manner to ensure that system weaknesses are rectified as soon as practicable.

The proposed corrective actions are therefore **subject to acceptance by the NSA**. This implies that, once the corrective action is proposed, there will be a need for the NSA to review the corrective action proposals for acceptability.

Consequently the NSA should provide the necessary **process** to be followed in relation to all **associated communications** with the service provider together with the formal review, acceptance, follow up and close out of corrective actions and the auditing activities necessary to verify the effectiveness of corrective actions taken in dealing with the root causes of reported non-compliances. NSAs should also provide a formal documented process that they require auditors to follow in relation to the follow up of corrective actions.


NSA
SERVICE PROVIDER
Requests corrective action
Proposes corrective action
Reviews and accepts (if appropriate) the proposed corrective action
Implements corrective action
Follow up audit action

(Figure 7 – Usual steps as regards corrective actions)

In order to ease the corrective action process, it is important that upon completion of the on-site audit and before departing from the service provider’s facility the audit team leader should inform the service provider’s management of the audit findings (verbally and in writing). Such findings will in practice be the factual details of nonconformities found during the audit, however the team leader may also indicate areas of ‘concern’ which whilst no direct evidence of nonconformity could be found give the audit team cause for concern that there may be a process / system weakness which should be investigated by the service provider. If such findings are not adequately communicated before leaving the service provider’s facility dispute over conclusions and / or findings detailed by the NSA in subsequent reports could arise.

TO NOTE THAT: as a general rule auditors should confined themselves to raise non-conformities and document them. Auditors should not be involved in the corrective action process. However, NSA auditors are sometimes delegated the authority to request corrective action on behalf of the NSA. This practice can be acceptable and does not complicate the audit process providing that:

- ❑ ***Its use is confined to auditing conducted by NSA auditors, not by recognised organisations;***
- ❑ ***Its use is preferably limited to cases where an unsafe situation needing urgent action is detected***
- ❑ ***The auditor understands that first they act as an auditor and then armed with the facts they then require corrective action to be taken on behalf of the NSA;***
- ❑ ***In accordance with ESARR 1, the responsibilities for requesting corrective action and accepting proposed corrective action rest with the designated point of responsibility in the NSA. Consequently, appropriate communication arrangements are established between the designated point of responsibility and the auditors to allow them to act on his behalf. More specifically, this should include an a posteriori endorsement by the designated point of responsibility of the actions taken by the auditor on his behalf.***
- ❑ ***The NSA makes clear the authority of its auditors to operate in this way.***

In many situations audit follow up activity will be necessary in order to verify not only that the corrective action has been taken, but that it has also been **effective in dealing with the root cause of the problem**, and that repeats of the originally observed symptoms (non-compliances) are no longer evident. If the situation is found to be satisfactory then the original audit finding(s) may be 'closed out'. The NSA has a responsibility to ensure the adequacy of the audit follow up and close out process and to keep good record relating to its activities at this important stage.

Follow up audits should be planned such that **similar samples** are taken to those that revealed the original nonconformities. This means not only similar samples but also samples designed to see that related areas and activities are also free from the originally observed symptoms.

There are many stages throughout the corrective action process where the process could go wrong. In particular it is the need to identify likely root causes which gives rise to the biggest problem, as often there is a tendency to just deal with the nonconformity found by the auditor and not investigate fully to identify a likely root cause, however there are other general weaknesses observed in audit corrective action processes such as badly written non-compliances, inadequate review of corrective action proposals and insufficient audit follow up sampling to verify that the root cause has been addressed and symptoms as originally identified by the audit are no longer evident.

In the event of unsatisfactory resolution of significant nonconformities an NSA will need to escalate and take appropriate measures such as the imposition of sanctions or restrictions in conformance with the **applicable legal framework**. NSAs should have documented procedures to control such decision making and associated actions.

More specifically, it is a common regulatory practice to consider the use of enforcement measures if the auditee fails to implement the corrective actions agreed by the NSA within the timescale granted by the NSA. This approach will be adopted in the certification of service providers established in EU Member States by Regulation (EC) 550/2004[17].

5.6 Additional Measures by the NSA

ESARR 1 establishes that, through its designated point of responsibility, the NSA should undertake additional actions if necessary. As discussed in Section 5.1.2 above, this means that the designated point of responsibility provides the information needed, based upon objective evidence obtained during the audits, to initiate a number of NSA processes established to address various situations.

A case in point is the need for NSA action **if an audit reveals an unsafe situation**.

In that context, measures may include the imposition of sanctions, operational restrictions or any other enforcement measure applicable within the existing regulatory framework, such as the revocation or suspension of relevant approvals.

The audit management function should establish **procedures to react immediately** to a major safety issue. In order to define these mechanisms it is particularly important for the NSA to identify some form of categorisation where safety is an issue.

> ***TO NOTE THAT: in practical terms, the use of these procedures should be exceptional and exclusively justified on the need to react in serious situations to ensure aviation safety in the public interest. An abusive use of these procedures would jeopardise the safety regulatory process implemented by the NSA.***

In defining these procedures, it is recommended to adopt the following criteria:

- ❑ Classify the non-conformities in two basic categories associated with levels of safety significance as follows:
  - a) Category ‘level 1’ should include any non-compliance with the applicable safety regulatory requirements which lowers the safety standard and **significantly** hazards the safety of aircraft.[18]
  - b) Category ‘level 2’ should include any non-compliance with the applicable safety regulatory requirements which lowers the safety standard and **may possibly** hazard the safety of aircraft.
- ❑ If appropriate, further sub-categories may be defined by the NSA within these two basic levels[19]. This may help the NSA to define specific actions in relation to a more refined categorisation.

[17] *Article 5 of the draft Commission Regulation being considered at the time of this writing to lay down common requirements for ANSP certification, establishes that “where corrective action has not been properly implemented within the agreed timetable, the NSA shall take appropriate measures in accordance with Article 7(7) of Regulation 550/2004 and Article 9 of Regulation 549/2004 while taking into account the need to ensure the continuity of services”. The provisions referred to state that “measures may include the revocation of certificates”.*

[18] *EXAMPLE OF A POSSIBLE LEVEL 1 NONCONFORMITY: In a safety regulatory audit conducted in an ATM operational unit to verify compliance with ESARR 5, objective evidence is found showing that an air traffic controller is providing an ATC service without holding a valid rating for that specific service (noncompliance against ESARR 5 Section 5.2.2.1 a)*

[19] *To note that it is a common regulatory practice to consider a “third level” of findings (apart from the non-conformities) intended to address issues that contain potential problems that could lead to a noncompliance. If used, this type of finding should not include information suggesting noncompliance. Moreover, no corrective action can be required by the NSA with regard to these findings.*

- ❑ Guidance material for auditors should be produced by the NSA to illustrate, preferably with examples, the type of non-compliances which fall under the ‘level 1’ and ‘level 2’ categories.
- ❑ As discussed in various sections of this document, any non-conformity raised in an audit **must be based on objective evidence**. This aspect becomes **critical** in the case of a ‘level 1’ non-compliance. Objective evidence must be found before the NSA considers the possibility of taking action.
- ❑ If an audit reveals ‘level 1’ non-conformities, **immediate action should be taken** by the NSA to correct the unsafe situation. Depending upon the case, the measures may include the determination of corrective actions to be implemented by the auditee in a specific period of time, the imposition of sanctions, operational restrictions and any other enforcement measure such as the revocation or suspension of relevant approvals.
- ❑ Practical arrangements should exist to allow immediate action by the NSA without waiting for the audit report where a ‘level 1’ non-conformity is revealed. In particular, auditors may need to immediately report the situation to the designated point of responsibility within the NSA.
- ❑ Any decision on enforcement measures will normally be decided upon by the NSA management in the light of the evidence obtained in the audit process. Exceptionally, and where a robust safety justification exists, the NSA auditors could also play a role in determining measures on-site to be immediately implemented by the auditee. However, this will not be possible in the case of audits conducted by recognised organisations.
- ❑ For ‘level 2’ non-conformities, the normal corrective action process should always be followed and, therefore, the NSA should not interfere with the determination of corrective actions by the auditee.

It should be noted that the **issue of a safety directive**[20] is not necessarily confined to situations where ‘level 1’ non-conformities are revealed. Following the results from an audit, a safety directive may require all or some service providers to take action to eliminate a practice or implement a process improvement. However, a safety directive should not interfere with the normal corrective action process where only level 2 findings have been revealed. Accordingly, the issue of a safety directive should normally wait until corrective actions are proposed by the auditee and agreed by the NSA, unless level 1 non-conformities were revealed. In addition, the contents of the safety directive should normally be consistent with the corrective actions agreed by the NSA.

(Space Left Intentionally Blank)

[20] *ESARR 1 Section 10 requires NSAs to issue safety directives when an unsafe condition has been determined by the NSA to exist in a system.*

TO NOTE THAT:

- ***The imposition of sanctions, operational restrictions or any other enforcement measure applicable within the existing legal framework will normally be decided by the NSA top management in the light of evidence obtained in the audit process. The evidence supporting these decisions will be provided by the designated 'point of responsibility' to the NSA top management.***
- ***However, there should exist a mechanism in place that will enable an auditor to react immediately to a major safety-related issue revealed by an audit such that the auditor, acting under delegated authority of NSA senior management, may require immediate action to be taken by the ATM service provider in advance of the normal audit reporting mechanism.***
- ***Only an NSA auditor can exceptionally act as a representative of the Authority beyond his/her audit responsibilities if a serious safety issue is revealed in an audit. This should not be possible if the audit is conducted by recognised organisations.***
- ***NSAs will need to develop suitable defined processes to enable fast tracking of serious safety critical audit findings. Without such fast tracking mechanisms the NSA could become partly responsible for safety failings / incidents due to known significant problems remaining unattended to by the ATM service provider.***
- ***There may be instances where a non-compliance found at a service provider will result in an NSA issuing a "Safety Directive" requiring all service providers under its responsibility to take action to eliminate a practice or implement a process improvement with the ultimate aim of improving overall safety levels.***

5.7 Auditor Selection and Competency Issues

It is important to select the right type of person to undertake safety regulatory audits. Auditor competency may be summarised under the following main categories:

- Knowledge and skills relating to ATM,
- Knowledge and skills relating to auditing,
- Knowledge and skills relating to safety oversight and other regulatory processes.
- Interpersonal Skills,

It is not only important to ensure the adequacy of initial training of auditors but also to ensure maintenance of competency together with commonality and consistency of approach across audit teams. To this end monitoring of auditor performance and periodic recurrent training for auditors is considered to be essential.

TO NOTE THAT: ESARR 1 includes specific provisions as regards the qualification of personnel designated to conduct safety regulatory audits in the NSA or the recognised organisations acting on its behalf.

5.7.1 Interpersonal Skills

Interpersonal skills are often not considered by auditing organisations but in practice extremely important. They may be grouped and include:

- ❑ *General human qualities*
  - Friendly, personable and able to relate to staff at all levels in an organisation.
  - Polite, diplomatic, non confrontational and not arrogant.
- ❑ *Specific positive attributes*
  - Self reliant, strength of character, able to deal with stressful situations.
  - Worldly wise, adaptable to changing situations.
  - Observant and perceptive, logical and analytical, objective,
  - Open minded, impartial, firm yet fair,
  - Decisive,
  - Ethical and professional.

Negatives traits to be avoided include: arrogance, domineering, argumentative, self opinionated.

Audit team leaders should also possess general organisational and leadership skills.

TO NOTE THAT: although it may be possible to select staff exhibiting some of the above, this will need to be supplemented by awareness training and specific skills development programmes.

5.7.2 Qualification Criteria for Auditors

In accordance with ESARR 1 Section 9.4, **NSAs must define qualification criteria** to be met by audit personnel, including personnel from recognised organisation conducting audits on behalf of the NSA.

Those qualification criteria must at least cover the following aspects:

a) The knowledge and understanding of the ATM environment and the requirements against which safety regulatory audits are performed. In that regard it should be noted that:

- The need for understanding of the ATM environment implies that being an expert in auditing techniques is not enough to deal with ATM safety.
- The requirements against which safety regulatory audits are to be performed may depend on the existing regulatory framework applicable to the situation.

b) The use of assessment techniques of examining, questioning, evaluating and reporting;

c) Additional skills required for managing an audit such as planning, organising, communicating and directing;

d) The demonstration of competence of auditors. **Examination** should be the normal and usual means to demonstrate competence of auditors. Any other acceptable means[21] should ensure that the qualification criteria defined by the NSA in accordance with ESARR 1 are effectively covered.

[21] *An example of other acceptable means could be a demonstration of competence accepted by another NSA which uses equivalent qualification criteria.*

5.7.3 Recommendations as Regards the Criteria to be Developed by the NSA

The following recommendations are consistent with good audit practices from other industries and provide a harmonised basis for the development of qualification criteria by NSAs in order to meet the ESARR 1-related requirements.

> ***TO NOTE THAT: it is recognised that implementing fully some of the following recommendations may raise practical difficulties during the initial implementation of ESARR 1. NSAs should therefore adopt a flexible approach which should eventually lead to the fulfilment of criteria equivalent to those recommended here.***

Accordingly, the full implementation of these recommendations constitutes a medium-term objective to be achieved in a phased approach by the NSAs. The recommendations on suitable audit training (bullet b, point iv, below) should apply in any case.

a) Knowledge and skills relating to ATM:

i) It is recommended that a minimum of three years practical working experience in an ATM environment is necessary for auditors, with the experience being gained either directly as an air traffic controller, engineering personnel, or in an appropriate management, regulatory or supporting function related to ATM.

ii) For team leaders such experience is highly desirable but not regarded as essential, providing there is a reasonable level of understanding of ATM related processes, at a technical and/or operational level as appropriate to the nature of the audit activity.

b) Knowledge and skills relating to auditing:

iii) It is recommended that this should comprise a combination of suitable training and practical audit experience.

iv) It is recommended that suitable auditor training is considered to be an auditor training programme that meets the **minimum criteria set by SRC** in Appendix J of this document for training on safety regulatory auditing.

v) It is recommended that at least twenty days of experience in undertaking audits is necessary in order to develop sufficient competence. This experience should have been gained under the guidance of an experienced auditor (operating at team leader level) and should involve a minimum of 8 separate audits of at least one full day on-site undertaking practical audit activities.

vi) For team leaders the above experience should be supplemented by acting as the team leader under the guidance of a practising team leader for at least three audits of no less than three days each (each audit includes one day off site document review and planning), plus report writing and with a team of at least two auditors in addition to the trainee team leader.

c) Knowledge and skills relating to regulatory processes:

vii) It is recommended that as a minimum three years of experience working in safety oversight activities in an aviation regulatory environment is required for auditors, with experience gained at a senior level grade for an additional two years for audit team leaders.

viii) Alternatively, full familiarity with regulatory processes can be considered enough if it was gained either in a regulatory support function or by virtue of work experience where there has been a period of at least two years acting as a direct interface with regulatory processes.

5.7.4 Provision of Suitable Auditor Training

To fulfil the qualification criteria established by the NSA, safety auditors should have undergone **specific training** to the extent necessary to ensure their competence in the skills required for carrying audits, and for managing audits. Such competence should have been demonstrated through written or oral examinations, or other acceptable means.

NSA may therefore decide to **recognise the training provided by particular organisations as an acceptable means** to demonstrate the competence to conduct and manage safety audits, provided that the training given:

a) Meets specific criteria established by the NSA for suitable auditor training to achieve the qualification criteria established in ESARR 1, Section 9.4, and

b) Includes an evaluation which must be successfully passed by the candidate auditor and whose result must be documented by the organisation.

TO NOTE THAT: minimum criteria recommended for training in relation to safety regulatory auditing are included in Appendix J of this document.

Those minimum criteria are considered by SRC as a recommended means to meet the ESARR 1 requirements and, therefore, provide for a harmonised basis to support the recognition of specific training courses by NSAs in the EUROCONTROL Member States.

5.7.5 Maintenance of Auditor Competence

It is recommended that the competency of auditors is maintained by means of a combination of routine performance monitoring and periodic recurrent training, together with providing for variation in the auditors undertaking audits of particular ATM service providers and the composition of audit teams.

The purpose of auditor performance monitoring is to verify that an auditor is adopting good audit practice and undertaking sufficiently thorough and searching investigations. There is a tendency over time for auditors to adopt less effective practices and also to develop a familiarity with ATM service providers, with the result that the oversight process may not be effective. Monitoring of performance together with regular review can provide for maintenance of auditor performance.

Routine monitoring of an auditor’s performance in the field should be undertaken by other experienced auditors and may be achieved by an experienced auditor accompanying the auditor on an oversight visit and reviewing his/her performance against the NSAs internal oversight procedures and good audit practice. In particular the performance review should verify that the auditor is undertaking a sufficiently in depth investigation and obtaining sufficient objective evidence. This may be difficult for smaller NSAs to achieve, however it may be realised by using auditors from other NSAs who are working in cooperation or by the use of contracted auditing agencies. For larger NSAs there should be a ‘core’ team of auditors who have the responsibility for maintenance of audit standards. Ideally this team should be a part of an NSAs internal audit staff with the overall responsibility for verification of effective implementation of the NSAs own internal management systems.

It is recommended that auditors should receive recurrent training in auditing techniques at suitable intervals designed to mitigate against the institutionalising of bad audit practices. Such training opportunities may also be used as an auditor developmental process aimed at the development of knowledge and skills relating to auditing practice, oversight methodology and awareness of latest safety management systems techniques.

It is considered to be beneficial for auditors to work from time to time with different colleagues in order to facilitate best practice. This is relatively easy to achieve in larger NSAs where there is a large 'pool' of auditors from which audit teams may be formed.

5.8 Monitoring Audit Effectiveness

NSA management should consider using an internal audit process as a means of monitoring the NSA's continued compliance with its own safety regulatory audit process, recognising that they will also be subject to external auditing from ICAO (IUSOAP) and EUROCONTROL SRC (ESIMS) and possibly participate in "Peer Reviews" with other NSAs.

The effectiveness of the safety regulatory audit process should be verified by independent auditors undertaking audits of all stages of the safety regulatory audit process and the audit management function. This should be undertaken at least on an annual basis with the report provided to NSA senior management.

It is also considered beneficial for on-going oversight not to be performed continuously by the same auditor(s) due to the possible problem of over familiarity with the situation and personnel at a service provider, however by constantly changing the auditor there is also a problem of the new auditor needing to gain an understanding of the organisation before the auditing may be fully effective. A balance needs to be struck.

5.8.1 Sharing Audit Experience and Feedback on the Audit Process

An NSA should develop processes to gather experience from the audited organisations. A possible approach is to organise regularly (for example annual) meetings where the NSA meets some or all of the audited organisations to get informally their feed-back about the audits.

This informal approach is not intended to discuss the audit contents, but to gather experience and contribute to good relationship with the service providers. The NSA should make sure that such meetings are not used by the audited organisation to discuss audit results.

This kind of meeting can bring information on the way the audits are seen from the audited organisation and on the common problems encountered during audits such as auditor behaviour, misunderstandings regarding audit reporting methods, etc.

(Space Left Intentionally Blank)

6. USE OF AUDITING IN SAFETY OVERSIGHT

6.1 Initial and On-going Oversight

Safety regulatory auditing will be used to obtain information to assist NSAs in making decisions relating to the initiation of operations by an ATM service provider. This is termed “Initial Oversight”.

Following initial oversight, a NSA will need to implement an audit programme designed to verify the continued effective operation of the service provider’s management and hence allow for continued operation of the ATM service provider. This is termed “On-going Oversight”.

The generic notions of initial and on-going oversight may concern compliance with non-safety related requirements beyond the scope of ESARR 1. It should be noted that the guidance in this document makes use of the terms “initial oversight” and “on-going oversight” in relation to the actions needed to verify compliance with applicable safety regulatory requirements[22] unless a different meaning is explicitly indicated.

6.1.1 Initial Oversight in Single European Sky

Depending upon the existing regulatory framework, the operation of ATM services may be subject to different regulatory mechanisms to address the initiation of operations by a service provider.

A case in point is the certification of service providers in the EU Member States against a set of Common Requirements and the subsequent designation of certified organisations to provide services in specified airspace blocks. Similar schemes may exist in non-EU countries if they are established through their applicable regulatory framework.

In the case of the EU Member States, “initial oversight” will be applied to verify compliance with applicable safety regulatory requirements in the context of the overall initial oversight processes articulated for the certification and designation of ATM service providers. Safety regulatory audits will be used for that specific purpose.

TO NOTE THAT: further guidance is being developed by SRC as regards the implementation of ESARR 1 in the context of the certification and designation processes established by the SES regulations in the EU Member States.

A specific deliverable (EAM 1 / GUI 5) is being developed to address this subject. Nevertheless, the following sections already provide basic guidance to articulate the safety oversight actions as part of the certification of service-providers and the subsequent designation of certified organisations to provide services in the EU Member States.

6.2 Initial Oversight

The purpose of conducting an Initial Oversight of an ATM service provider is to verify that the service provider has put in place the necessary processes and disciplines to meet the applicable safety regulatory requirements in an effective manner and that the service provider may therefore be permitted to provide ATM services. Initial Oversight may also be required following significant changes to the organisation or infrastructure of the service provider in order to verify that the significant changes have not negatively impacted on the service provider’s ability to continue to provide services with the necessary level of safety.

[22] *The term “applicable safety regulatory requirements” is defined in ESARR 1.*

TO NOTE THAT: initial oversight <u>should not be performed</u> on an ATM service provider until its arrangements intended to meet the applicable safety regulatory requirements, or parts thereof that are being audited, have been formally implemented for at least six months. This is to allow for sufficient evidence to be available to demonstrate the effective operation of the provider's arrangements.

Initial Oversight of a service provider might not be undertaken on one visit alone, but may involve **a series of visits with each visit focusing on a specific aspect** of the operation and/or specific elements of the applicable safety regulatory requirements. This approach may be most appropriate when there is a need for the NSA to pro-actively work with the service provider to encourage the continual development of safety management to increased levels of maturity; that is to say, where the baseline maturity level of the management of safety requires further enhancements until a fully satisfactory minimum is achieved.

The audit approach will need to relate to this incremental process within an overall audit oversight programme aimed at full compliance whilst each individual oversight visit will focus only on sampling against specific elements. Thus use of the audit sampling approach where each audit will sample against a predetermined set of safety regulatory criteria.

For many NSAs with a significant limitation on resources and a relatively large number of ATM service providers for which safety oversight needs to be implemented it may only be possible to undertake **one visit** for the conduct of an initial oversight for the **smaller ATM service providers**, in this case the visit will need to be sufficiently comprehensive to provide the necessary assurance.

In this situation it is important to verify the effective implementation of **all** applicable safety regulatory requirements. However if the state of maturity in the ATM service provider with regard to the management of safety is at a relatively low level, the NSA must be prepared to undertake an initial oversight which will result in significant non-compliances for which a further visit(s) will be required after a suitable period of time during which time the ATM service provider will need to further develop its management of safety. However, this approach may only be possible if the NSA still has confidence that the service is safe is spite of those non-compliances.

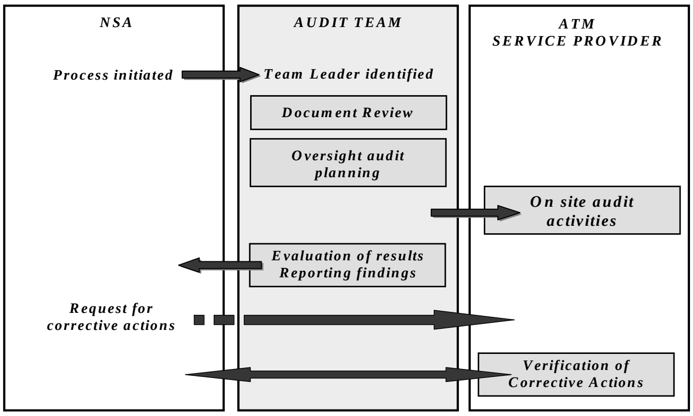
The approach to initial oversight will vary from case to case dependent upon the level of maturity of both the service provider and the NSA in relation to the management of safety and its practical application to fulfil the applicable safety regulatory requirements. The audit process will consequently need to be adapted to fit in with the overall oversight approach. However there are some recognised good practices relating to auditing as applied to an initial oversight activity that should be adopted.

(Space Left Intentionally Blank)

6.2.1 An Overview of the Initial Oversight Audit Process

The NSA initiates the Initial Oversight audit process. A Team Leader[23] should be identified who will have the responsibility for managing the initial oversight process through to completion.

The team leader will liaise with the ATM service provider, and will conduct the **"Document Review"** in relation to the management of safety implemented by the provider.



The team leader should determine a suitable audit team, plan the oversight visit and allocate specific audit tasks to the audit team members. The audit team members will plan their parts of the audit.

The audit team will visit the ATM service provider, conduct the audit, inform of their findings to the service provider at the end of the audit, and provide a detailed **audit report** to the designated "point of responsibility" in the NSA. Following internal arrangements, the designated "point of responsibility" will transmit appropriate information based on the audit findings to the NSA management function responsible for making decisions in relation to the initiation of operations by service providers (e.g. decisions related to the certification of providers in the context of SES).

The designated "point of responsibility" will, if necessary, request "corrective actions" of the service provider. In that situation, the service provider will determine suitable corrective actions and propose these to the designated "point of responsibility" who will decide whether they are acceptable.

The designated "point of responsibility" will arrange for verification of agreed corrective actions and final audit "close out".

6.2.2 Key Features of the Initial Oversight Audit Process

A person should be nominated to act as the **audit team leader** for the initial oversight activity. This person could be appointed amongst the NSA's staff or be part of a recognised organisation commissioned to conduct the process on behalf of the NSA.

In any case the audit team leader should meet the qualification criteria[24] identified by the NSA in accordance with ESARR 1 Section 9.4.

The team leader may need to undertake some form of pre-oversight visit in order to discuss the process with the service provider and to obtain some understanding of the organisation and facilities. After that, the initial oversight audit process breaks down into the following two key stages:

- ❑ Stage 1 - often called a "Document Review",
- ❑ Stage 2 - Initial Oversight audit visit.

[23] *To note that in the context of a certification scheme like the one established in Regulation (EC) 550/249, the Team Leader may normally receive the name of Certification Team Leader (CTL). For further clarification see Sections 5.4.1 and 7.4.1 of this document, as well as EAM 1 / GUI 5.*

[24] *See Section 5.7 and Appendix J of this document*

6.2.3 Stage 1 – “Document Review”

There is a need to see evidence that the service provider has understood the applicable safety regulatory requirements and has put in place what appear to be adequate processes and disciplines designed to meet these requirements and appropriate to the scale and scope of service provider operations.

Hence Stage 1 requires the audit team leader to undertake a review of the documentation that the service provider has put in place to describe and communicate its **arrangements to manage safety**. Such a review should not be used as an opportunity by the audit team leader to impose its own views on what the provider’s arrangements should look like or how they are developed. He/she should be confined to looking for evidence that the applicable safety regulatory requirements have been understood and there are clear indications that processes and disciplines have been put in place to meet the requirements that are applicable to the type of service provider organisation.

If a hierarchical approach to developing the documentation has been adopted then it would be normal practice to confine this review to the high level manual or manuals related to the requirements under consideration, with possibly only a sample of some of the lower level documents that convey working details.

Where no high level manuals have been produced, or where they contain very little information describing the management and safety-related practices adopted by the service provider, particular attention should be paid to the lower level documentation.

TO NOTE THAT: the scope of the documentation review is defined by the scope of the “applicable safety regulatory requirements”. Therefore this scope is not necessarily confined to the Safety Management System’s Documentation specifically intended to implement ESARR 3.

The purpose of this document review is not to challenge the organisation’s working procedures but simply to satisfy the two questions, does it look as though there is understanding of the requirements and is there evidence that processes have been developed to meet the requirements.

Comments on the arrangements established for the management of safety will need to be communicated to the service provider making it clear where additional clarification or detail is required, and again this must not be used by the audit team leader as an opportunity to dictate what they would like to see in the documentation other than what is necessary and practical to provide a level of confidence in the understanding and intentions of the service provider.

In the event that the document review reveals serious concerns about the level of understanding that the service provider may have of the applicable safety regulatory requirements or the processes that have been put in place to meet these, then the audit team leader should not proceed to Stage 2, but instead refer this matter to the NSA “point of responsibility” for decision on further action to be taken.

The document review should also be used to assist the audit team leader to develop an understanding of the ATM service provider, its organisation, associated responsibilities and basically what physically exists and work processes undertaken. Without this knowledge it will be difficult to identify the audit resource needed and adequately plan an oversight visit. Although this understanding may also be facilitated by pre-oversight visits it is not until close reading of documentation that a full understanding is developed.

The amount of time spent on undertaking the document review should be sufficient to enable the audit team leader to fully assess the provider's arrangements against the applicable safety regulatory requirements, to identify areas of perceived weakness or concern and to enable sufficient understanding of the organisation and its management of safety.

TO NOTE THAT: Inadequate resource applied at this stage is likely to result in an inadequate oversight visit.

If the document review indicates possible areas of weakness or concern about the service provider's arrangements to manage safety, then such areas should certainly be the **subject of on-site audit activity** to obtain the necessary regulatory confidence, in addition to the routine sampling to verify the effective implementation of the service provider's arrangements.

6.2.4 Stage 2 – Initial Oversight Audit Visit

Once the document review has been performed it will then be necessary to verify that the arrangements described in the documentation are indeed being used and are **effectively implemented** within the service provider. This will require a visit (or visits) to perform this verification.

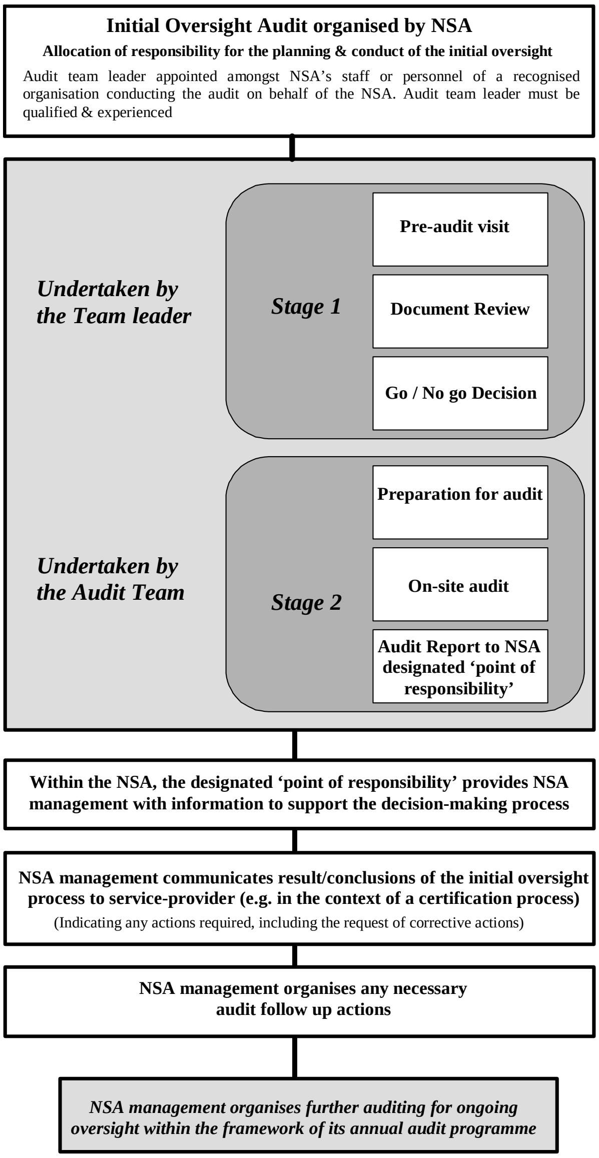
The audit team leader will, based on the information obtained at a pre-oversight visit and / or the document review, identify those parts of the service provider organisation and specific processes that need to be audited in order to verify selected requirements of the applicable safety regulatory requirements together with the implementation of the service providers arrangements in line with the previously identified intentions set out in the documentation reviewed.

The team leader will also need to **identify the audit resource needs** (number of auditors, experts in particular disciplines) and over how many days the audit is to be conducted. There is a need to arrive at a sensible balance and not to undertake audits of unrealistically long or short durations or to use teams unnecessarily large or too small to perform an effective audit.

The team leader should also develop an **oversight visit schedule** and determine where in the organisation the various requirements are to be verified, recognising that it is only necessary to verify a sample of the total requirements in each area of the organisation, but ensuring that all requirements are ultimately verified somewhere within the organisation.

Sampling of requirements in each area of the organisation will depend upon processes being verified and also the level of confidence that has been obtained by the team leader after having performed the document review. The document review may have identified aspects of the provider's arrangements for which the team leader has some concerns and so wishes to ensure that these are investigated more fully during the on-site auditing activity. However, the audit should not cover exclusively those areas that the document review highlights. It is good practice to check that some of the bits that look good on paper are also good in practice.

It may be appropriate, depending upon the level of maturity of the provider's management of safety or indeed if the regulator wishes to pro-actively encourage the gradual development of fully comprehensive arrangements in a service provider which is itself still developing its understanding of safety management, for the Initial Oversight to be performed over several separate visits, with each visit focusing on the verification of certain elements of the SMS. Over a defined period of time all elements and hence all applicable safety regulatory requirements would be verified.


Initial Oversight Audit organised by NSA
Allocation of responsibility for the planning & conduct of the initial oversight
Audit team leader appointed amongst NSA's staff or personnel of a recognised organisation conducting the audit on behalf of the NSA. Audit team leader must be qualified & experienced
Undertaken by the Team leader
Stage 1
Pre-audit visit
Document Review
Go / No go Decision
Undertaken by the Audit Team
Stage 2
Preparation for audit
On-site audit
Audit Report to NSA designated 'point of responsibility'
Within the NSA, the designated 'point of responsibility' provides NSA management with information to support the decision-making process
NSA management communicates result/conclusions of the initial oversight process to service-provider (e.g. in the context of a certification process)
(Indicating any actions required, including the request of corrective actions)
NSA management organises any necessary audit follow up actions
NSA management organises further auditing for ongoing oversight within the framework of its annual audit programme

(Figure 8 - Stages in the Initial Safety Oversight audit process)

6.3 On-going Oversight

6.3.1 Planning On-going Oversight

On-going oversight needs to be planned taking into consideration the results of Initial Oversight together with the results gained from the on-going oversight activities. This is likely to lead to **updates of the annual programme of audits** as more audit results are obtained.

The guidance of EAM 1 / GUI 1[25] has already pointed out that the term 'annual' used in ESARR 1 implies that the programme of audits is established on an annual basis and, therefore, needs **to be reviewed and updated at least annually**.

These updates should be both pro-active in relation to the confidence gained in certain areas / activities, as well as reactive to findings and changes taking place.

[25] *EAM 1 / GUI 1 'Explanatory Material on ESARR 1 Requirements'.*

Collectively the ESARR 1 requirements require an NSA to develop suitable audit programmes that are developed in full consideration of the data that the NSA has concerning the safety performance of ATM service providers and in a pro-active manner that responds to the “assurance” of conformance to requirements as revealed by the safety oversight process together with the findings of previous safety regulatory audits and the need for verification of corrective actions implemented to address such findings.

More specifically, ESARR 1 requires NSAs to organise sufficient audits to check the compliance of all service providers with the applicable safety regulatory requirements in all areas of functional relevance **over a period of two years**. It is therefore necessary to ensure that all applicable safety regulatory requirements are adequately investigated and verified over the two years time period.

The planning should also take into consideration the following aspects:

- Risks identified from previous audit results,
- Safety performance of the service provider,
- Confidence in the safety-related arrangements operated by the service provider,
- Size and complexity of the service provider operation,
- Maturity of the service provider’s organisation
- Organisational changes taking place in the service provider,
- Introduction of new/changed systems or technology.

Initial Oversight will have provided the NSA with a level of confidence in the application of safety related disciplines meeting applicable regulatory requirements throughout the organisation. On-going Oversight is designed to verify that there is continued application of these disciplines, and improvement action taken where system weaknesses are identified or safety performance falls below the required level. Audits undertaken in support of ongoing oversight will need to look closely at process effectiveness.

Process effectiveness is indeed of great importance in relation to safety management. An organisation may have a process in place that has been designed to meet a safety objective, such as the competence of personnel. In this case auditing must establish that not only is the competency process being followed, but that the competency process is effective in ensuring that those required to have a particular competence do in practice have the required competence. This means that the auditor must also look at the results being achieved (the output of the process).

On-going audits should therefore **look very closely at process effectiveness** and may consequently require more audit time and experienced auditors as well as ad-hoc support from experts with knowledge in specific fields.

(Space Left Intentionally Blank)

EXAMPLES:

- ***In an engineering support environment there may appear to be a very good process for analysing system fault data and improving the reliability of system elements where reliability is poor. But is the total system reliability meeting the specified reliability target?***
- ***The on-going audits may need to look at the effectiveness of engineering and calibration actions in relation to important equipment such Navigational Aids, ILS, etc. This may require independent tests of equipment performance to verify that the calibration process is effective, and examination of incidents / complaints etc. to see if there are trends indicating equipment performance deficiencies.***

6.4 Use of Recognised Organisations

Wherever allowed by the existing regulatory framework[26], NSAs may decide to commission "recognised organisations" to conduct, totally or partially, a safety regulatory audit.

TO NOTE THAT: in this case it is essential for NSA senior management to understand that they remain fully accountable for the safety oversight process and therefore must ensure that such delegation is managed and monitored to ensure full adequacy and effectiveness of the safety regulatory audit activities performed on their behalf.

Throughout the EU there may be several such "recognised organisations" with the competence to undertake supervisory tasks in accordance with the provisions of Regulation (EC) 550/2004. These will have been accredited by a NSA as competent to perform such activities, and may include certification companies also providing certification of products and management systems against international standards, and other organisations specifically constituted to provide such services.

It should be noted that those supervisory tasks may concern verification of compliance with non-safety related requirements[27]. ESARR 1 does not apply to these activities. However, wherever supervision concerns compliance with the "applicable safety regulatory requirements", ESARR 1 requires a NSA to establish certain mechanisms to support its decision-making in regard to the use of a specific recognised organisation.

In safety oversight, the use of "recognised organisations" is in principle confined[28] to the conduct of safety regulatory audits on behalf of the NSA.

[26] *Within the SES legislation applicable to EU Member States, Regulation (EC) 550/2004 establishes that a NSA may decide to delegate, in full or in part, the supervisory tasks to recognise organisations which fulfil a set of requirements included in a specific annex of the Regulation. ESARR 1, Section 8 elaborates further on this subject to address the case of the supervisory tasks specifically related to safety.*

[27] *Regulation (EC) 550/2004 identifies nine categories of Common Requirements against which certification takes place within EU Member States. Some of them cannot be considered as applicable safety regulatory requirements according to the ESARR 1 definition.*

[28] *This is consistent with Regulation (EC) 550/2004 which establishes the possible use of recognised organisations to conduct the "proper" inspections and surveys organised by the NSA. In the context of ESARR 1, safety regulatory auditing is the means to conduct such inspections and surveys wherever safety is subject under consideration.*

The use of “recognised organisations” requires appropriate arrangements between the NSA and the recognised organisation. **The audit management function**[29] will normally be responsible for managing these aspects within the NSA. This may include determining suitable processes and associated documented procedures. However, the decisions about the use of a specific recognised organisation should be made by the NSA top management.

More specifically, wherever a NSA decides to commission a recognised organisation to conduct work related to auditing, a **properly documented agreement** covering the applicable arrangements should be drawn up to make clear aspects such as:

- The roles and responsibilities of the NSA and the recognised organisation. These will ensure that the NSA remains fully responsible for the safety oversight activity,
- The interfacing arrangements between them and the service provider, including the communication of audit results through the designated ‘point of responsibility’ appointed at the NSA,
- The confidentiality and conflict of interest aspects.

Such practical arrangements should be established following, or as part of, a process to **decide on the possible use of a specific recognised organisation** to conduct safety regulatory audits on behalf of the NSA.

In that regard, ESARR 1 requires that **decisions made by a NSA** in relation to the delegation of safety oversight tasks to a recognised organisation **shall be based upon** a specific demonstration provided by the recognised organisation as to their suitability to perform the required safety oversight activities.

According with ESARR 1 such a demonstration has to satisfy the NSA that:

a) The recognised organisation is competent, to produce adequate auditing results **in relation to ATM safety aspects**

b) The recognised organisation is **not involved** in safety surveys or any other safety-related verification activities implemented internally by the audited ATM service-provider within its Safety Management System.

c) All personnel concerned with the conduct of safety regulatory audits are **adequately trained and qualified** for their job functions and meet the qualification criteria established by the National Supervisory Authority in accordance with Section 9.4 c) of ESARR 1.

d) The recognised organisation provides the National Supervisory Authority with full visibility of its planning, procedures and working methods to conduct safety regulatory audits and their results,

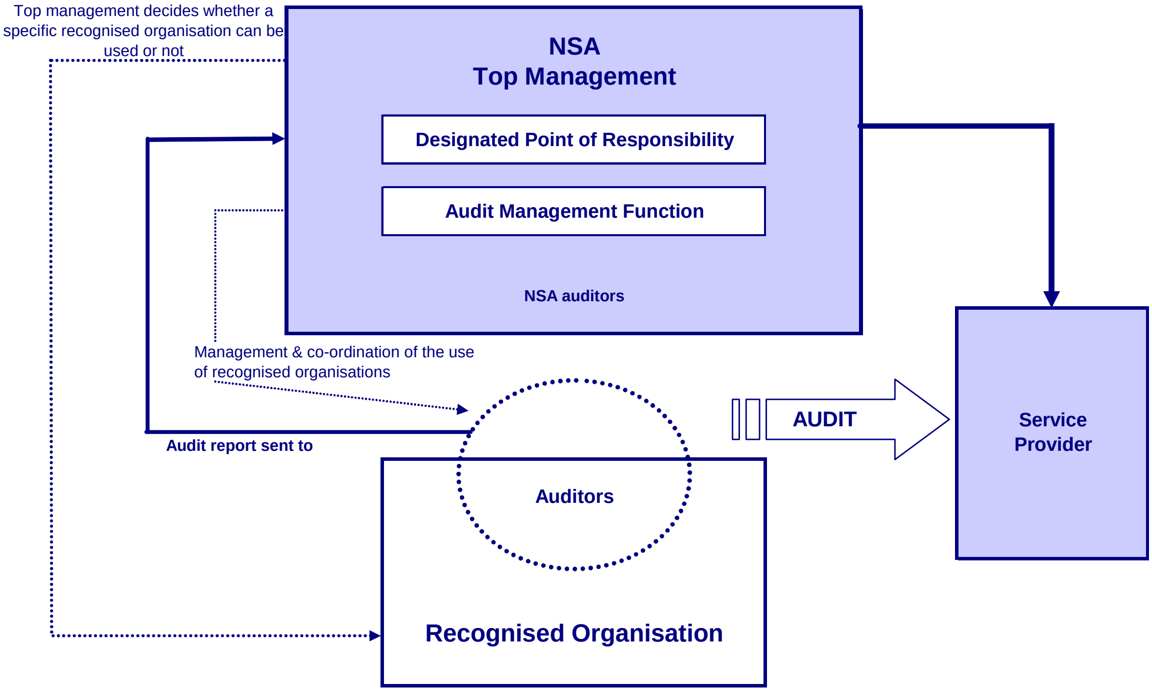
e) The recognised organisation accepts the possibility of being audited by the National Supervisory Authority or any organisation acting on its behalf.

In relation to bullet a) above, the NSA should normally assess, inter alia:

i) The experience in assessing safety in aviation entities, in particular ATM service-providers, and the

ii) Adequacy of processes and associated documented procedures relating to the safety auditing activities undertaken by the recognised organisation. As a minimum, the procedures should address the guidance provided in this document.

[29] *See Section 5.1.3 above on the responsibilities of an audit management function within the NSA.*


Top management decides whether a specific recognised organisation can be used or not
NSA
Top Management
Designated Point of Responsibility
Audit Management Function
NSA auditors
Management & co-ordination of the use of recognised organisations
Audit report sent to
AUDIT
Service Provider
Auditors
Recognised Organisation

(Figure 9 - Possible use of a recognised organisation by the NSA)

TO NOTE THAT: the NSA at all times remains responsible for:

- ❑ ***Ensuring the determination, adequacy and implementation of the annual programme of safety regulatory audits;***
- ❑ ***The auditing activities and its associated reporting mechanisms;***
- ❑ ***The establishment of qualification criteria for auditors;***
- ❑ ***The role of the designated 'point of responsibility' which must remain within the NSA.***

6.5 NSAs Undertaking Audits on Behalf of Other NSAs

Situations may exist where provisions are established, including relevant international agreements wherever appropriate, to allow for a delegation of the conduct of audits to a NSA different from the one responsible for the supervision of air navigation services provided in a specific airspace.

These situations may concern different States and, as a general principle, this sort of arrangements can only be implemented with the agreement of the States responsible for the airspaces considered. The agreements established between States with regard to the delegation of the provision of air navigation service to another State should address these aspects.

In that regard, it should be noted that the NSA function denotes an existing regulatory task which applies to the relevant authorities of any State who has accepted the responsibility for regulating and providing air navigation service functions over its territory and associated areas, and that, consequently, the term 'National Supervisory Authority' used in the context of ESARR 1 is not limited to EU Member States nor is it limited to the tasks of the NSA under the SES regulations.

From a purely practical perspective, a NSA may wish to establish arrangements with another NSA to delegate the conduct of safety regulatory audits in regard to some of the ATM services under its responsibility. This may take place in various situations, for example in the case of an airspace geographically isolated or surrounded by airspace where ATM services are subject to the supervision of a second NSA, or in any other situation in which for practical reasons it would be logical or convenient for the safety oversight of the ATM services to be performed by another NSA.

In any of those cases, the first NSA is responsible for the safety oversight of the services provided in a specific airspace. A second NSA conducts audits on behalf of the first NSA, although the first NSA is the one nominated or established by the State responsible for regulating an providing air navigation services in that airspace.

6.5.1 Possible Arrangements for Delegation to a Second NSA

In practical terms, three types of basic arrangements can be foreseen:

❑ In the first case, the first NSA remains fully responsible and accountable for the adequacy of the safety oversight auditing activities and makes arrangements with the second NSA in a similar way to those for using “recognised organisations”. In this approach:

  i) The **first NSA keeps its audit management function**, including the determination of an annual programme of audits, suitable audit processes and associated documented procedures for the implementation of the programme;

  ii) The second NSA would conducts audits for the first NSA, and

  iii) In general terms, the arrangements for auditing would be similar to those described in Section 6.4 of this document in relation to the use by NSAs of recognised organisations.

❑ This approach could also be adopted reciprocally to establish **cross-auditing** arrangements between the two NSAs with regard to all or some of the audits scheduled by their respective audit management functions. In this case the first NSA conducts audits for the second NSA, and the second NSA conducts audits for the first NSA.

❑ The third option would be for a first NSA to **delegate the audit management function to the second NSA** as well as the auditing activities themselves. In that regard it should be noted:

  i) That delegation is possible in the context of ESARR 1, on the basis that the ESARR 1 requirements related to the audit management function (e.g. the provisions on the annual programme of audits) are required to be met by “National Supervisory Authorities” (in plural);

  ii) However, such delegation **should not include** the role of the designated “point of responsibility” and the corrective action process on the basis that the ESARR 1 related provisions apply to “the National Supervisory Authority” (in singular).

TO NOTE THAT: the role of the designated ‘point of responsibility’ should not be delegated by a first NSA to a second NSA who audits the ATM services under the responsibility of the first NSA.

6.5.2 Joint Audits Conducted by NSAs

NSAs may additionally choose to undertake combined (joint) audits of service providers in which they both have a direct interest in relation to the adequacy and effectiveness of safe service provision within adjacent airspace or airspace jointly administered (such as Functional Airspace Blocks).

Such audits may involve teams of auditors with auditors from each of the participating NSAs, or auditors from one NSA acting only as observers. Whatever the role of each individual team member, they should be clearly defined and documented and there should always be an identified team leader with ultimate responsibility for the planning, conduct and reporting of the audit.

However for such joint auditing activities the NSA having the responsibility for provision of safety oversight in the airspace within which the ATM service provider is located should normally retain the full responsibility for the adequacy and effectiveness of the auditing activities undertaken by the joint parties.

In any case, the designated ‘point of responsibility’ and the corrective action process should remain within the NSA responsible for the supervision of the service provider.

6.5.3 Auditing in Regard to Providers Certified by Another NSA

Within the SES regulation applicable in the EU Member States, specific provisions exist as regards the cooperation between NSAs. More specifically, Regulation (EC) 550/2004 establishes that NSAs shall make appropriate arrangements for close cooperation with each other to ensure adequate supervision of service providers holding a valid certificate from one Member State that also provide services relating to the airspace falling under the responsibility of another Member State.

In the EU Member States, certificates are to be issued by the NSA of the State in which the service-provider organisation has its main place of operation. Once certified, the organisation may be designated to provide services in the airspace of any EU Member State, and subject to the safety oversight of the NSA nominated or established by that second State.

In terms of safety oversight, the arrangements already foreseen in the SES provisions should ensure **close co-ordination between:**

- ❑ The **audit management functions of the two NSAs**. The rationale is that the annual programme of audits of both NSAs need to be coordinated in order to properly check compliance with requirements, notably in terms of effective implementation irrespective of the jurisdiction in which the provider operates;
- ❑ The **designated ‘points of responsibility’ of the two NSAs**. There will be a need to coordinate the corrective action process resulting from the audits conducted by any of the NSAs, because non-conformities may affect the operation of services in the jurisdiction of the other NSA and also because in that case the effective implementation of corrective actions should take place irrespective of the jurisdiction in which the provider operates.

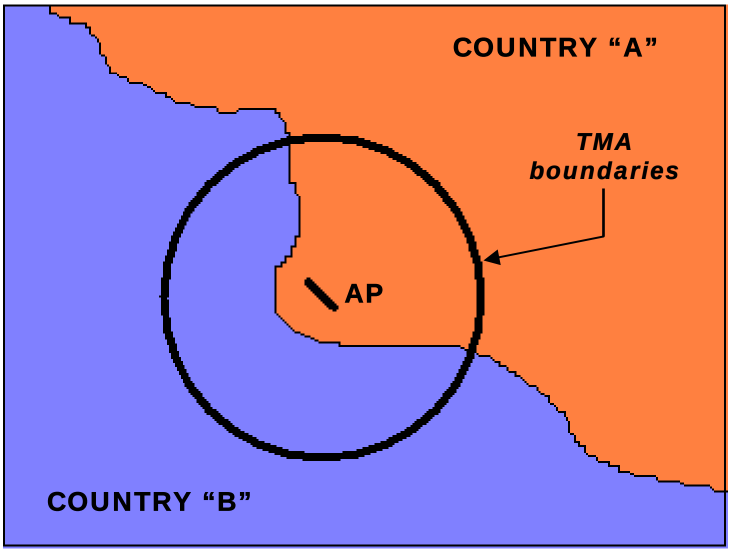
In particular the designated ‘point of responsibility’ of the NSA who issued the certificate should obtain all the information from the audits that could affect the validity of the certificate, irrespective of the NSA who conducts them.

Proper coordination mechanisms should be established between the two NSAs in the form of joint working structure to ensure an effective implementation of these aspects.

Wherever an organisation holding a valid certificate provides services in several states, all the NSAs involved in the safety oversight of that organisation should be involved in those coordination mechanisms.

6.5.4 Example of NSA Undertaking Oversight on Behalf of a Second NSA

For this example, an airport is located just next to the boundary of its country (Country “A”). For the safe use of procedures at this airport, Country “B” has delegated the provision of services in a part of its airspace (the part of the TMA that is in Country “B”) to Country “A”, where the airport is located. It should be noted that the NSA of Country “B” has the responsibility for the safety oversight of service providers that provide services in Country “B” airspace.



As a result of that delegation to Country “A”, the airport “AP”, which is an organisation certified to provide the ATM services needed at this aerodrome, has been designated as the service provider for all the TMA airspace.

The Country “B” also delegates the conduct of oversight of “AP” to Country “A”. Nevertheless, the NSA of Country “B” has the ultimate responsibility in its airspace, and therefore it has been decided that the safety oversight of airport “AP” will be conducted by the NSA of Country “A” with participation from the NSA of country “B”.

Countries “A” and “B” have written down an agreement as regards the audit of airport AP. The agreement is as follows:

The NSA of Country “A” (NSA “A”) and the NSA of Country “B” (NSA “B”) will follow the following arrangements:

- *The audit team leader always belongs to NSA “A”.*
- *The audit team is composed by auditors from NSA “A” and NSA “B”*
- *All information received during the audit, as well as the report are strictly confidential to the NSA “A”, the NSA “B” and “AP”.*
- *The audit report is sent to:*
    - *All members of audit team,*
    - *The manager of “AP”,*
    - *Both clients (the designated ‘point of responsibility’ of NSA “A” and the designated ‘point of responsibility’ of NSA “B”).*
- *The NSA “A” is responsible for the audit follow up (accepting, if appropriate, the corrective actions proposed by “AP” in case of non conformities). The NSA “B” is informed by NSA “A” of the corrective actions agreed. If NSA “A” does not approve the corrective actions, NSA “A” and “B” meet to find an agreement.”*

6.5.5 Example of Regional Co-operation for Safety Oversight Undertaken by NSAs

The Nordic region provides an example of such cooperation involving the conduct of common audits. A trial process was implemented in 2004-2005.

When common Nordic audits are conducted, the NSA of the state where the auditee is located is always identified as the **client** of the audit.

These audits are usually a part of the States ‘normal’ oversight audit plan. The auditors from the other Nordic states involved in the audit are considered to be external experts to help conduct the audit.

The scope of these audits relates to ESARR requirements and some other standards that are harmonised in the Nordic countries. In the planning phase, an area of responsibility (e.g. one of the ESARRs) is given to each auditor. Each auditor conducts his part of the audit (with help of the team), and produces a report of that area. The auditor from the client state acts as the team leader, and in the end collects the individual reports, and finally puts them together in a complete report. This report is then circulated to each auditor for acceptance. After this phase, the client ‘owns’ the report, and acts as it is suitable for their purposes.

The acceptance of corrective actions and follow up audits are to be decided by the state in question.

Such audits have been conducted in Sweden, Finland, Denmark, Norway and Iceland. In each case the client has been the NSA of the state where the audited unit was located. This principle was agreed at NORDREG (a meeting of Nordic regulators) along with the confidentiality policy. Naturally, the NSA of the audited unit has the ownership of the report and decides if the report should be available for others or not. The NSA of the state concerned is also responsible for the corrective action process and possible follow up audits.

The audit team leader has always been from the NSA of the state of the auditee. It was agreed that the team leader is responsible for the practical arrangements with the auditee; detailed visit schedules etc. Audit preparation is done mostly by correspondence and with a team meeting before the actual audit (usually the previous day). This meeting has been mostly for examining national regulations and to finalise the audit teams working program for the audit.

These audits have initially been used to verify compliance with ESARRs, as this was seen to be the easiest way to begin the trial because the implementation of the ESARRs has been harmonised in all Nordic states.

The participating auditors can be seen as external experts working for (or on behalf of) the NSA, however it was agreed that the ‘host’ NSA is not responsible for the costs of the auditors from the other states during the trial phase.

6.6 Safety Oversight in Relation to Functional Blocks of Airspace

In cases of functional airspace blocks across the airspace under the responsibility of more than one State, the agreements between States on the supervision of the ATM services relating to those blocks shall specifically ensure that responsibilities for ATM safety oversight are identified and allocated in a manner which ensures:

a) Clear points of responsibility to implement each one of the requirements that ESARR 1 imposes on an NSA,

b) Visibility of the safety oversight mechanisms operated as a result of the agreement,

c) Regular and visible review of the agreement and its practical implementation in the light of safety performance measurements.

In relation to safety auditing such agreements should therefore identify;

a) Responsibilities for the implementation of safety regulatory audits in relation to the FAB and its associated ATM service provider(s) together with responsibilities for decisions based on the results of such audits. This should include an identification of clear points of responsibilities within the agreements with regard to the **responsibilities that in a NSA relate to**:

   - ❑ The role of NSA top management, as described in Section 5.1.1 of this document;
   - ❑ The designated ‘point of responsibility’ to be appointed in a NSA in accordance with ESARR 1 Section 6.6 b, and described in Section 5.1.2 of this guidance;
   - ❑ The audit management function in accordance with the contents of Section 5.1.3 of this document.

b) The process to manage the safety regulatory audit process undertaken on behalf of the involved states who are parties to the agreement;

c) The periodic review of the agreement and the safety regulatory auditing activities in the light of practical auditing experience and the related audit results.

From a ‘good practice’ auditing perspective, whilst the planning of an annual programme of safety regulatory audits and the decision making based on the results of audits may be a joint responsibility between the co-operating NSAs, or involve points of responsibility from the different co-operating NSAs, the audit process itself should ideally be managed from **one single point of responsibility to ensure adequacy and effectiveness of the safety regulatory audit process**.

This point of responsibility for audit activities should be identified by the NSAs and provided with sufficient resource by the cooperating NSAs so as to enable the required level of auditing to be undertaken. Audit results should then be provided to the ESARR 1 designated “points of responsibility” within the participating NSAs to enable decision making in relation to the operation of the associated ATM service provider(s).

Audits may be conducted by auditor(s) drawn from the cooperating NSAs, and dependent upon the expertise and competence available. Where audit teams are formed, then there should always be a designated team leader who will ultimately be responsible for the planning, conduct and reporting of the audit to the NSAs “points of responsibility”.

There are many possible approaches that may be taken by cooperating NSAs, such as jointly planning, managing, conducting and reporting safety regulatory audits, one NSA delegating the audit planning, management, conduct and reporting to another NSA, or by all cooperating NSAs delegating the conduct of safety regulatory audits to a “recognised organisation”. However no single NSA can absolve its responsibilities and accountabilities in relation to safe service provision within its own airspace of responsibility and hence should ensure the adequacy of the audit process conducted by itself, in conjunction with, or on its behalf by other parties. Such mechanisms should be defined in written procedures and the properly documented arrangements subject to periodic audit and review of adequacy and effectiveness.

TO NOTE THAT: as already pointed out in EAM 1 / GUI 1, and although not required in ESARR 1, it appears advisable from a safety perspective to strongly recommend the establishment of a single point of responsibility for all ATM safety oversight functions related to a particular FAB, including the safety regulatory audit functions. Such an option would provide further safety barriers to prevent a dilution of responsibilities in complex situations.

(Space Left Intentionally Blank)

PART 2 - GUIDANCE FOR AUDITORS AND AUDIT TEAM LEADERS

7. INTRODUCTION TO THE CONDUCT OF AUDITS

In Part 1 of this guidance document, auditing is introduced by placing the focus on its management within the overall safety oversight process to be implemented by National Supervisory Authorities.

Part 2 of this document provides guidance to auditors and audit team leaders on the planning, conduct and reporting of audit. This includes:

- ❑ Generic guidance – intended to support a broad range of audit activities that may be undertaken as part of the overall safety oversight process, including all types of safety regulatory audits undertaken as part of Initial or On-going Oversight.
- ❑ Specific guidance – elaborating further in relation to activities undertaken in the Initial and On-going Oversight processes.

Auditing[30] is the process used to obtain independent evidence that will provide confidence in the effective operation of a management system that has been designed to enable an organisation to meet defined objectives. Auditing is now accepted and recognised as a very valuable component of the overall approach to safety oversight.

The notion of audit is discussed further in Part 1 of this guidance document[31].

7.1 Roles and Responsibilities

Part 1 of this document includes guidance for the identification of responsibilities with regard to auditing in relation to:

- ❑ The NSA top management
- ❑ The audit management function
- ❑ The “designated point of responsibility” required in ESARR 1

The following sections complement that information and address the roles and responsibilities of auditors and audit team leaders.

7.1.1 Audit Management Function

The overall audit process and the audit resources should be managed by an audit management function within the NSA.

Detailed responsibilities for the audit management function are described in Section 5.1.3 of this document. In the context of the conduct of audits, those responsibilities should be articulated to allow this function to:

- ❑ Provide the necessary procedures to manage the audit process and audit resources and organise the conduct of audits;

[30] *As mentioned in Section 1.2 above, the guidance in this document normally uses the term ‘audit’ in relation to its specific application to ATM safety oversight in the form of ‘safety regulatory audits’. Throughout the text, both terms can be considered synonyms unless a different meaning is explicitly indicated.*

[31] *In particular, see Section 4 of this document.*

- ❑ Request sufficient and competent audit resources to be provided by NSA top management;
- ❑ Be involved in the initiation of the audits;
- ❑ Identify the audit “scope” and “objectives” together with appropriate sampling against applicable safety regulatory requirements for each audit undertaken;
- ❑ Nominate audit team leaders amongst the personnel with appropriate qualification, available within the NSA or provided by recognised organisations
- ❑ Agree with audit team leaders the necessary audit team members for each audit, allocate audits to NSA auditors or accept the auditors proposed by recognised organisations wherever applicable;
- ❑ Identify the need for auditors to consider the results of previous audits when undertaking their audit planning.

TO NOTE THAT: inadequate management of the audit process and of the auditors may lead to totally ineffective safety regulatory audits.

It is the responsibility of NSA senior management to ensure a fully satisfactory approach to auditing and to provide for a fully effective audit management function to manage the process and the auditors. Only in this way can NSA senior management be provided with the necessary information upon which to base their decisions relating to initial and continued operation of services by ATM providers.

7.1.2 Audit Team Leaders

Audit team leaders have specific responsibilities in relation to an audit process. The term “team leader” is taken to mean the person delegated the task of performing an audit where the audit activity requires one or more auditors, including in some cases the use of technical resources used to assist or advise the auditors.

TO NOTE THAT: the audit team leader may be the only auditor conducting an audit activity.

The audit team leader should be appointed by the NSA audit management function, and is placed in overall charge of the audit.

The audit team leader can be appointed amongst the NSA personnel or, wherever applicable, be proposed by the recognised organisation involved in the conduct of the audit and accepted by the NSA audit management function.

Audit team leaders should meet specific qualification and experience criteria defined by the NSA, irrespective of being NSA staff or personnel provided by a recognised organisation.

These qualification criteria shall be developed by the NSA in accordance with ESARR 1 Section 9 and should meet the recommendations included in Section 5.7 of this document. The criteria should, in any case, encompass all the criteria established for auditors and expand them to ensure the management capabilities of the personnel nominated as audit team leaders.

The specific responsibilities of the audit team leader include:

- Co-ordinating with the audit management function in the NSA;
- Identifying the audit resources (auditor/days) needed after reviewing the documentation relevant for the audit;
- Ensuring the adequacy of audit planning and the following of plans by individual auditors;
- Liaising with the service provider throughout the audit process, ensuring the adequacy of communication with the main point of contact in the service-provider throughout the duration of the audit visit,
- Assisting with the selection of other audit team members to undertake specified audit tasks;
- Preparation of the audit team members;
- Allocating tasks to individual auditors;
- Finalising the audit report and submitting it to the "designated point of responsibility" in the NSA;

7.1.3 Auditors

The auditors, including the audit team leader, should be responsible for:

- Complying with applicable audit procedures and working practices, communicating and clarifying them appropriately;
- Planning and carrying out assigned responsibilities effectively and efficiently:
- Studying key documents to facilitate their understanding of the service provider and processes forming the subject of the audit:
- Verifying the requirements assigned by the audit team leader within the time allocated:
- Documenting the observations and reporting the findings:
- Retaining and safeguarding audit documentation in accordance with the procedures established for audits:
- Keeping confidentiality with regard to findings of the audit and the information gathered during the audit.

Auditors should be free from bias and influences which could affect objectivity. NSAs and recognised organisations should ensure by means of appropriate policies and procedures that all persons involved with an audit respect and support the independence and integrity of the auditors.

The auditors should meet specific qualification and experience criteria defined by the NSA, irrespective of being NSA staff or personnel provided by a recognised organisation. These criteria shall be developed by the NSA in accordance with ESARR 1 Section 9 and should meet the recommendations included in Section 5.7 of this document.

Depending upon circumstances, the audit team may include experts with specialised background, trainees or observers who are acceptable to the NSA audit management function and the audit team leader. The terms of reference for their participation in the audit should be established prior to the audit.

7.1.4 Specific Roles with Regard to Certification

In the context of an initial oversight conducted as part of a certification scheme, such as the one established in the EU Member States by Regulation (EC) 550/2004, it is common to use the terms:

❑ Certification Team Leader (CTL) and

❑ Certification Team Members (CTMs)

Their roles and responsibilities will normally be equivalent to those described above for the audit team leader and team members, on the basis that auditing constitutes the core activity of the certification exercise. However, some additional responsibilities could exist due to the specific procedures intended to implement the certification scheme established in the applicable regulatory framework.

In addition, certification will normally need the identification of a focal point or function in the NSA for the receipt and management of applications for certification. This function will depend on the size and organisational arrangements of the NSA and the number of potential applicants. It may therefore be combined with other roles in the NSA. The function could be assumed by the Audit Management Function or the Certification Team depending upon the case.

EAM 1 / GUI 5 is being developed by SRC to provide specific guidance on this matter.

7.2 The Need to Plan the Audit

To be effective, auditors must be focused on the task that they have been requested to carry out. In order to make best use of the time available the audit must be carefully planned. Such planning must ensure that specialist knowledge held by individual auditors is also put to best use and that neither the audit team's nor the staff members of the audited organisation's time is wasted.

The planning process must include all phases of the audit, including any document review and report preparation as well as the on-site visit.

An individual audit forms part of an overall safety oversight process. The management of that safety oversight process is the responsibility of the NSA but the audit team may need to take account of the findings of previous audits and other information provided by the audit management function when planning their work. Similarly, it is important for the audit team to make records of their findings for use in future audit planning and to assist the NSA to fulfil its safety oversight responsibilities. In some cases the audit team will also be requested to perform some post-audit visit actions on behalf of the NSA. The audit team leader should ensure that the audit plan takes account of such actions in order to ensure that sufficient resources are available.

The auditor must always remain in control of the process of information gathering otherwise the results will be of limited value. In order to remain in control auditors will need to consider in advance of the audit what evidence they require and a general plan or strategy that will be adopted to obtain this evidence in a systematic and unbiased way. They will therefore need to undertake sufficient audit planning in advance of the audit.

TO NOTE THAT: audit planning is therefore key to effective auditing, and lack of adequate planning is the biggest enemy of the audit process.

The audit planning will need to be undertaken at two levels:

a) Planning the visit to the service provider,

b) Planning the audit activities to be undertaken during the visit.

It is a primary responsibility of the audit team leader to ensure the adequacy of audit planning and the following of plans by individual auditors to ensure achievement of audit objectives.

TO NOTE THAT: the audit will always be planned as a sampling activity, never a 100% check. The sampling approach is used provide confidence in an organisation's ability to meet applicable regulatory requirements and to operate an appropriate management of safety.

The following sections discuss these topics in more detail.

(Space Left Intentionally Blank)

8. HOW TO PLAN, CONDUCT AND REPORT AUDITS

This section aims to provide guidance for the planning, conduct and reporting of safety regulatory audits that may be undertaken as part of safety oversight of ATM service providers. The guidance is generic and intended to provide basic principles and approaches that will facilitate effective auditing where such auditing is an integral part of an Initial Oversight of an ATM service provider, or individual audits forming part of On-going Oversight activities, together with unscheduled or follow up audit activities.

8.1 Audit Protocol

Over the years it has been found beneficial to adopt approaches to the general conduct of audits that are aimed at ensuring:

- ❑ Adequacy of communication between auditing organisations and those subject to audits,
- ❑ Acceptable conduct of auditors,
- ❑ Objective auditing,
- ❑ Factual reporting of audit findings.

These approaches are not required by means of mandatory rules. They are regarded as best practices to be adopted. Where they have not been adopted it has been found to lead to difficulties being experienced by auditors and in extreme cases serious disagreement and bad feelings between auditors and organisations audited. It is recommended therefore that the audit protocol detailed within this guidance is adopted by NSAs and implemented through the audit management function and by auditors and audit team leaders.

The audit management function of an NSA should ensure that documented procedures are provided in order that audits are undertaken using best practice audit protocol, and that auditors and audit team leaders fully understand their responsibilities in relation to such procedures and the need for such protocol to be adopted.

The following are regarded to be good practice to be followed by auditing organisations and will be amplified in the text of this guidance document:

- ❑ Appointment of an audit team leader,
- ❑ Mutually acceptable and pre-arranged dates for audits to be conducted,
- ❑ Clearly identified scope of audit (those areas / departments / processes to be audited),
- ❑ Effective communication before, during and after an audit,
- ❑ Audit entry meetings,
- ❑ Use of audit guides,
- ❑ Factual approach to recording and reporting audit findings,
- ❑ Audit exit meetings,
- ❑ Final report submitted in a reasonable timeframe.

8.2 Preliminary Preparation for an Audit

The audit management function (the Audit Management) is responsible for allocating audits to individual auditors in coordination with audit team leaders. Such audits will be part of an annual programme of safety regulatory audits. The programme will be regularly updated to include follow up audits to verify effectiveness of corrective actions resulting from previous audits or unscheduled audits in response to noted concerns with an ATM service provider.

The audit process is therefore initiated when an auditor is requested to undertake an audit by Audit Management. The audit purpose, scope and objectives should be clearly defined by Audit Management, and the auditor should ensure that these are clearly defined and understood before proceeding with the audit activity.

An auditor should be designated as the audit team leader although the audit may not involve any additional auditors or support staff to assist (dependent upon the magnitude / complexity / technical nature / etc. of the audit to be undertaken).

Preliminary preparation for the audit requires the auditor to:

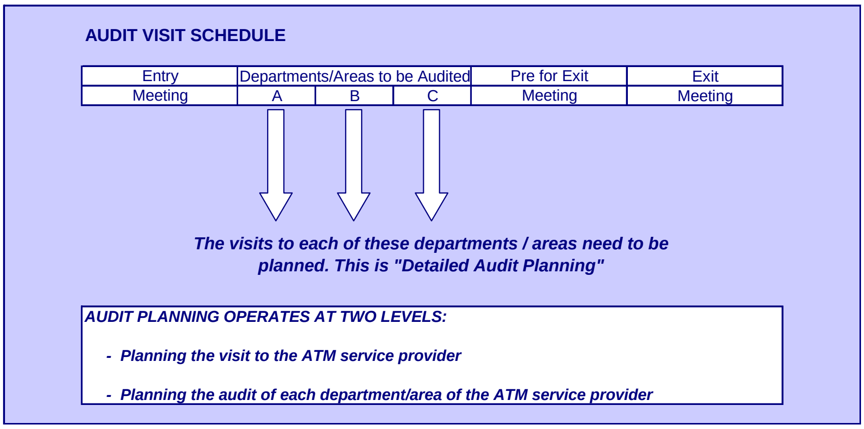
a) Develop an **understanding of the organisation** to be audited that is sufficient to enable the audit to be conducted.

b) Identify, or confirm with Audit Management, **which specific provisions** of the applicable safety regulatory requirements are to be verified and in which areas of the ATM service provider, or in relation to which regulatory processes.

c) Determine a **suitable audit visit schedule** and decide the composition of the audit team.

d) Communicate with the organisation to be audited to advise them of the audit intention, the objectives and scope of the audit, and where necessary the audit visit schedule to enable the organisation to ensure availability of appropriate personnel.

The audit visit schedule is an output from the preliminary audit preparation stage. It will identify those departments or areas of the service provider that are to be audited, giving sequence and times to be spent by auditors in each department / area. Although not part of the audit visit schedule, the specific paragraphs (or clauses) of the regulations to be verified will be determined and used to quantify the time that needs to be spent in each department / area of the service provider organisation. This may be undertaken by the team leader, as in the case of an Initial Oversight, or by Audit Management as in the case of On-going Oversight.



AUDIT VISIT SCHEDULE

Entry	Departments/Areas to be Audited			Pre for Exit	Exit
Meeting	A	B	C	Meeting	Meeting

The visits to each of these departments / areas need to be planned. This is "Detailed Audit Planning"

AUDIT PLANNING OPERATES AT TWO LEVELS:

- *Planning the visit to the ATM service provider*
- *Planning the audit of each department/area of the ATM service provider*

Once the preliminary preparation has been undertaken, an audit visit schedule provided and an audit team put in place, the audit team leader will need to meet with the proposed audit team and **allocate audit tasks to each auditor** indicating clearly the department / areas of the ATM service provider, or specific processes, that they are required to audit, together with details concerning the specific regulatory requirements, and associated paragraphs to be verified. This initiates the detailed audit planning process.

TO NOTE THAT: a regulation comprises many individual provisions or clauses communicating specific requirements. It must be made clear to individual auditors those provisions that they are required to verify. This is known as the 'sample' of the regulation (also called audit criteria) that are to be verified by the auditor.

8.2.1 Developing an Understanding

In order to develop an understanding of the organisation to be audited the auditor will need to obtain sufficient information about the organisation. This information may be available in formal documentation such as manuals and procedures, or in publicity or promotional material. It may also be desirable, or necessary, for the auditor to consult with colleagues, technical experts or previous auditors in order to assist with the development of this understanding. The auditor needs to have an understanding of the general work processes undertaken in the organisation to be audited. This relates to auditor competence to undertake the audit task.

TO NOTE THAT: lack of such understanding may seriously inhibit the ability of the auditor to conduct an effective audit.

In some cases it may be appropriate for the auditor(s) to undertake a "pre-audit visit" in order to obtain the necessary information to enable the auditor to begin planning the audit. Such visits may involve guided tours of the facility and explanations of how the organisation functions. The auditor may also request key documents that will be used assist this understanding and facilitate audit planning.

Such visits **should not be used** to begin the process of audit, and requests for documentation should be confined only to those considered necessary to understand the organisation and not specific procedures for formal review by the auditor. (For an Initial Oversight key management documentation will be requested formally by the NSA to undertake document review – see guidance on Initial Oversight).

Auditors may also use **process analysis techniques** in order to help them to understand the general sequence of activities undertaken in relation to specific processes. They may work with company documentation or rely on their own knowledge and/or experience with similar organisations and industries. Process analysis is made easy when an organisation has adopted process modelling as a means of understanding and managing internal processes. Organisations that have adopted the principles of ISO 9001 may have process diagrams and descriptions that can assist an auditor to better understand how the organisation undertakes its activities - descriptions of the sequence and interactions of processes.

When the auditor has developed an understanding of the organisation to be audited the auditor should then undertake **"detailed audit planning"** which will involve the development of various documents that the auditor will use to assist in the conduct and reporting of the audit findings.

SUMMARY OF METHODS TO DEVELOPING AN UNDERSTANDING:

- ❑ ***Undertaking a pre-audit visit,***
- ❑ ***Studying documentation relevant to the audit***
- ❑ ***Discussions with colleagues,***
- ❑ ***Undertaking Process Analysis.***

TO NOTE THAT: it is considered necessary for auditors to have experience in the industry environment that they are required to audit within. In depth specialist knowledge may be necessary for some environments; however such in depth specialist knowledge can sometimes lead to a lack of objectivity on the part of the [specialist] auditor and must, therefore, be carefully managed by the team leader.

8.2.2 Determination of the Requirements to be Verified

Regulations comprise many individual requirements. For any audit it will be necessary to decide which of these are to be verified in relation to the specified applicable safety regulatory requirements against which the audit is being conducted.

For an Initial Oversight it will be necessary to verify **ALL** such individual requirements of the appropriate regulation(s) within specific areas, units or departments of an ATM service provider, **without necessarily checking them in all the areas**, units or department where they must be implemented.

It will normally be the team leader who will decide on the **'sample'** of such individual requirements to be verified within each department or functional area of the service provider organisation. This in turn will enable an oversight schedule to be produced.

The team leader will need to consider the results of preceding activities, such as a document review, together with previous knowledge or safety performance of the service provider to assist in the sample determination.

***TO NOTE THAT**: for an on-going oversight audit it will be Audit Management that will have determined which applicable safety regulatory requirements will need to be verified on each oversight visit. This will have been decided by Audit Management as part of the annual programme of safety regulatory audits.*

8.2.3 Determination of the Audit Visit Schedule

The process is essentially the same for any type of audit, however there are some differences in the process when conducting an Initial Oversight.

For **on-going oversight audits**, Audit Management will need to communicate to the auditor those departments or areas and processes of a service provider to be verified together with appropriate samples of the regulatory requirements (Objectives, scope and sample of requirements to be verified).

The auditor is responsible for translating this into a suitable audit visit schedule and for **communicating this schedule to the ATM service provider**. It is recommended that the communication takes place at least one month in advance of the oversight visit (or earlier if it involves a significant level of auditing and a team of auditors). Although on-going oversight visits are likely to involve only one auditor, it may sometimes be necessary to use a team audit approach for larger ATM service provider organisations.

For **unscheduled audits, or follow up audits** undertaken as a means of verifying the effectiveness of corrective actions taken in response to previous audits, again it will be Audit Management that will identify the objectives, scope and sample of requirements to be verified, and again it is the responsibility of the auditor to develop and communicate a suitable visit schedule to the ATM service provider.

An **initial oversight audit** will require the team leader to fully understand the organisation of the service provider and what activities (processes) are undertaken within each department or functional area and how some processes are undertaken throughout the organisation (so called cross functional processes that flow through various departments). The team leader will need to determine the sample of regulatory requirements that need to be verified in each department or functional area and will need to make a judgment as to how much time will need to verify each requirement. The complexity of the organisation, the desired sample and associated time estimate will in turn enable the team leader to determine suitable resources to undertake the audit.

Such resources may include auditors with particular technical skills and / or technical specialists to support the audit team.

The team leader will need to produce an audit visit schedule that clearly identifies the audit resources, how long will be spent by each auditor in each department, the sequence of departments and over how many days the audit is to be conducted. The team leader may meet with the proposed audit team members to discuss, agree and finalise the schedule before it is sent to the service provider.

The proposed visit schedule **should be communicated to the ATM service provider**. It is recommended that the communication takes place at least three months in advance of the proposed date of audit to enable the service provider to make arrangements for the availability of necessary personnel. Until the service provider has confirmed acceptance of the proposed visit schedule it remains a proposal only.

Further information relevant for the determination of audit visit schedule can be found in the guidance for Initial Oversight in this document.

TO NOTE THAT: audit team leaders should agree audit visit schedules, team composition and the applicable safety regulatory requirements (or parts thereof) to be verified, with the Audit Management function.

(Space Left Intentionally Blank)

8.2.4 Communication

Adequacy of communication is important throughout the audit process in order to avoid misunderstandings and to facilitate the achievement of audit objectives.

Although a regulator always reserves the right to make unannounced visits to an ATM service provider, it is generally regarded as good practice to give reasonable notice of any audit visit in order to ensure that the necessary service provider staff and facilities are available to the auditor(s). Usually one to two months notice are recommended, however for an Initial Oversight visit involving a large team of auditors three to four months advanced notice is recommended.

***TO NOTE THAT**: an ATM service provider should always be made fully aware of the "objectives" and "scope" of any audit to be undertaken:*

- ❑ ***Objectives - The purpose of the audit.***

  (e.g. initial oversight leading to a certification possibility, part of the on-going oversight activities, corrective action follow up audit, or an unscheduled audit necessary as a result of concern or safety occurrence, etc.)

- ❑ ***Scope - Those departments, areas or specific processes of the ATM service provider to be subject to audit activity.***

The audit team leader should decide on the necessary support and assistance that may be required of the ATM service provider to facilitate the conduct of the audit, such as:

- ❑ Office space to conduct audit team meetings,
- ❑ Access to office facilities such as photocopiers etc.
- ❑ Guides to accompany the auditor(s) throughout the audit,
- ❑ Meeting rooms for Entry & Exit meetings,
- ❑ Access to company documentation and records (hard copy, data bases, intranet etc.),

The audit team leader should also clarify and confirm such matters as:

- ❑ Means of access to the facility, car parking, security arrangements, etc.
- ❑ Working times of various departments,
- ❑ Lunch and refreshment arrangements,
- ❑ Restrictions on the use of mobile phones, recording devices, cameras, etc. (Some auditors may wish to use recording devices, in which case they will need to ask permission. Cameras are not normally used / allowed when auditing except in certain working environments and only then after permission has been obtained from senior management).

***TO NOTE THAT**: all such support requests and clarifications should be communicated and/or confirmed in writing in advance of the audit, and preferably at the same time that the audit schedule is communicated and agreed with the ATM service provider.*

Although the audit visit schedule and general audit support requirements will have been communicated at the time of finalising the arrangements for the audit, the team leader should check a few days in advance of the intended audit date that the auditor(s) are expected and that the ATM service provider has put in place the necessary arrangements to support the audit team and facilitate the audit process. It is wise to check that key staff have been informed of the visit and that all staff have been made aware that they may become involved in the audit process, dependent upon the needs of the auditors.

The time of arrival of the audit team, together with the intention to hold a brief audit entry meeting, should be confirmed with the organisation. Communication at this stage is likely to be with the main point of contact in the organisation (e.g. Safety Manager or equivalent), however it is more appropriate for formal (written) communication to be with the overall director/most senior person heading the organisation in order to ensure that the audit process is afforded the necessary management attention.

It is the responsibility of the audit team leader to ensure adequacy of communication with the service provider main point of contact throughout the duration of the audit visit, and to ensure throughout all stages that the audit is conducted in a fully acceptable and open manner.

TO NOTE THAT: the main point of communication should be with the head of the service provider organisation for all high level and formal communications between the NSA and service provider, however for general practical arrangements relating to audits and follow up visits, the NSA may suggest that the Safety Manager (or equivalent) would be an acceptable contact point.

8.3 Detailed Audit Planning

As previously indicated audit planning operates on two levels.

- ***Planning the visit to the service provider***
  (undertaken by the team leader),
- ***Planning the audit activities to be undertaken during the visit***
  (undertaken by individual auditors).

The audit team leader is responsible for planning the audit visit, which will include the provision of an audit visit schedule, identifying date(s) of the visit, auditors in the team and areas / departments / processes to be audited during the visit.

Auditors are responsible for planning their individual audit tasks such that they are able to verify the necessary requirements (as allocated by Audit Management or an audit team leader). This is different to, and quite separate from, the audit visit schedule.

(Space Left Intentionally Blank)

8.3.1 Planning for the Individual Audit Activities

Once the visit schedule has been finalised, it will then be necessary to plan for the individual audit activities. This will require the audit team leader and any team members to ensure that they have sufficient understanding of the specific areas and processes of the ATM service provider that they are required to audit and the particular parts of the applicable safety regulatory requirements that they are required to verify[32]. They will need to work with the applicable safety regulatory requirements together with the service provider's declared safety-related documentation to plan their audit tasks and to produce the necessary auditor's working documents in the form of check lists and an audit strategy or plan of action.

To assist an auditor to understand the work processes that are undertaken within specific departments or areas of an organisation the auditor will first rely on their current level of industry specific knowledge coupled with their understanding of similar types of organisation. They may then read key documents, such as the provider's manuals, talk with colleagues who may already be familiar with the organisation, and if possible participate in a pre-audit visit when they may view operations and discuss with the organisation's managers to assist their understanding[33].

Undertaking a process analysis to identify how a process is likely to be implemented in an organisation can often be helpful, and in some cases may be simplified by the organisation itself describing some of its key processes in the form of process diagrams, flow charts etc. These can be very helpful to auditors, and also show clarity of thinking in relation to the management, control and improvement of processes by the service provider.

Without a reasonable understanding of work processes it is very difficult to undertake a meaningful audit. In extreme cases it may be necessary for the first part of an audit process to require the auditor to spend time with a manager who will explain relevant processes before the auditor is able to finalise planning and commence the audit (if this is necessary then there must be a sufficient time allowance in the audit visit schedule).

In many cases current NSA staff will already have a reasonable understanding of service provider operating under the jurisdiction of their organisation, however preliminary preparation of the nature described above will still be of value to assist the undertaking of effective audits.

Once such preliminary preparation has been completed by an auditor it is then necessary for the auditor to produce documents that will be used to control the audit investigation, assist the auditor to achieve the audit objectives and to allow he auditor to record important details and results of the audit investigations.

Auditor's working documents typically include:

- ❑ **High Level Check Lists** *(derived from requirements that the ATM service provider must meet),*
- ❑ **Plan of Action / Audit strategy** *(to guide the auditor to different locations or personnel)*

[32] *It is important that the 'sample' of the requirements is adequately specified to an auditor otherwise this will lead to an auditor only verifying those parts of a regulation that they understand or are familiar with, and will negate the systematic verification of all parts of a regulation arranged for by audit management.*

[33] *However such pre-audit visits are normally only undertaken by audit team leaders. They may be able to provide individual auditors with relevant information about the service provider organisation.*

- ❑ **Low Level Check Lists** *(to remind the auditor of specific evidences and questions),*
- ❑ Documentation used to maintain a record of what the auditor has actually examined during the audit,
- ❑ Documentation / forms to record the results of audit investigations and audit findings.

Auditors should be given clear guidance on the parts of the requirements to be verified, and although some form of check list may be provided that is aligned to the regulation(s) being verified, it will be necessary for the auditor to customise such check lists by working with the service provider's documented arrangements related to safety and other relevant documentation in order to arrive at an 'service provider specific' check list such that the auditor is then prepared with a list of requirements to be verified comprising a combination of regulation and service provider's declared means of meeting the regulation.

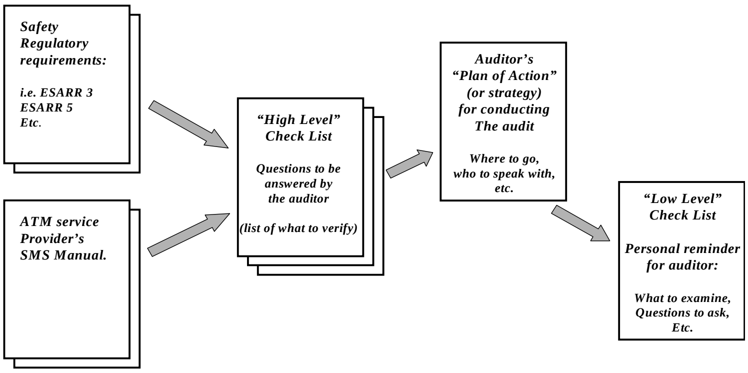
Such a check list is often termed a **"high level check list"** and effectively becomes the auditors **personal objectives** for the audit. These check lists provide the auditor with a constant reminder of what needs to be verified during the audit (the objectives of their part of the audit) and enables them to track their progress in achieving this verification within the time allocated.

> ***TO NOTE THAT**: an audit is always performed against a defined "audit base" that the auditor must interpret correctly and judge against in a fully objective manner. If the auditor misinterprets the audit base, or adds their own additional requirements then the audit is no longer objective and an incorrect verification has been performed.*

8.3.1.1 Audit Planning Methodology

Auditors should be competent in the development of high level check lists. Such check lists assist the auditor to understand the requirements, facilitate the planning, conduct and reporting of the audit, and help to ensure objective auditing. Auditors who judge an organisation against their own opinion of what the regulations mean and require, or who impose their own approaches to meeting requirements are not undertaking objective audits.

Detailed audit planning will require an auditor to develop high level check lists, a "Plan of Action" or "Strategy" for the conduct of the audit, and a reminder of the evidences needing to be seen together with questions that need to be asked in the form of a "low level" check list. This process will be explained on the following pages.


Safety Regulatory requirements:
i.e. ESARR 3
ESARR 5
Etc.
ATM service Provider's SMS Manual.
"High Level" Check List
Questions to be answered by the auditor
(list of what to verify)
Auditor's "Plan of Action" (or strategy) for conducting The audit
Where to go, who to speak with, etc.
"Low Level" Check List
Personal reminder for auditor:
What to examine, Questions to ask, Etc.

.

TO NOTE THAT: the whole purpose of producing the auditor's working documents in the form of check lists and strategy / plan is to put the auditor into a well planned situation such that they remain in full control of the audit process and undertake the audit investigations in a fully systematic and well thought out way rather than simply acting in a haphazard and random manner during the audit process, being led by the auditees and not being fully aware of what needs to be seen to verify compliance.

High level check lists are important documents. They record the original audit intentions (what was to be verified) and they provide a record of the eventual audit result. These together with details concerning the auditor's "Plan of Action", low level check lists and the auditor's notes (details of what was examined) provide evidence of effective auditing.

Development of such a check list will help an auditor to understand what the requirement is actually saying and therefore requires, and will help to maintain objectivity. Any question that appears on the high level check list that is not traceable to a regulation or requirement that an organisation must meet is allowing the auditor to make a personal and subjective opinion.

IT IS VERY IMPORTANT TO NOTE THAT:

- ❑ ***All questions appearing on the high level check list must be <u>traceable</u> to a requirement that the organisation <u>must meet</u>;***
- ❑ ***There must be no questions that are purely the auditor's opinion as to what the organisation should do or how it should do it; and***
- ❑ ***All questions must be answerable simply with YES or NOT. The organisation either does or does not something.***

The high level check list will be used during the audit to act as a constant reminder of what the auditor should be verifying, and will enable the auditor to maintain a record of progress. Use of this check list helps to maintain objectivity throughout the audit process.

Upon completion of the audit the high level check list together with the answers YES or NO will provide a formal record of what the auditor intended to verify and what the audit actually revealed. Additionally the auditors notes will provide a record of what was examined together with answers provided by the audited personnel.

TO NOTE THAT: the NSA audit management function should provide appropriate procedures and forms to be used by auditors as a means of ensuring that the results of the auditors investigations are retained as audit records. Such records should include details of evidence viewed, replies to questions etc.

It is **not good practice** to send copies of high level check lists **reflecting the sampling of requirements determined by the audit team** to organisations to be audited in advance of the audit, as this could lead to pre-preparation of responses and evidences relating to the specific parts of a regulation being verified in advance of an audit.

However, there is no reason why high level check lists **relating to the full text** of a regulation may not be used by an ATM service provider as a means of themselves checking that they have processes in place that are designed to satisfy the regulation. This is an approach often adopted by an organisation to check their state of system development in preparation for a forthcoming audit. NSAs may also consider the use of a similar approach by sending a full high level check list in advance of an Initial Oversight to request that the ATM service provider undertakes their own pre-audit check and also responds indicating key responsibilities in relation to particular requirements, the references to specific documents used to control certain activities and locations where specific records are held in relation to the safety management system. Such an approach is often combined with pre-audit questionnaires (often used by organisations auditing potential contractors or suppliers).

For an example of how to develop high level check lists, see Appendices.

Once the high level check list(s) has been finalised, the auditor should then give some thought as to how such items on the high level check list will in practice be verified. The auditor will need to think very carefully about the actual objective evidence that will need to be seen in order to verify regulations are being met in a consistent manner, and from where or whom such evidence will be obtained. It is now dependent upon the skill of an auditor to prepare for sufficiently in-depth and effective investigations to search for the necessary objective evidence in a systematic way that ultimately provides confidence that there are consistently and effectively applied approaches being adopted by the service provider to meet the regulatory requirements.

The auditor will need to arrive at a proposed plan of action or strategy to obtain objective evidence of compliance and should record in advance a low level check list of the actual evidence (documents / record / hardware etc.) that the auditor wishes to examine together with sample sizes and questions of key individuals that the auditor must remember to ask in order to obtain information or clarification of activities undertaken and associated responsibilities.

TO NOTE THAT: in some cases pre-prepared high level check lists will exist for a regulation (provided as part of guidance documentation etc.) or will have been developed for use within an NSA. This will assist auditors, however care must be taken by the auditor that they understand exactly what the regulation is asking for. Such check lists may then be further developed by auditors to produce check lists for application at a specific ATM service provider by developing additional questions that are derived from the ATM service providers documented arrangements (usually working with high level documentation such as an Safety Management System Manual).

8.3.1.2 The Auditor's Plan of Action / Strategy

The high level check list has identified what the auditor must verify, the auditor now needs to determine a suitable strategy or “Plan of Action” that will enable the auditor to obtain the necessary **objective evidence** to be able to answer these questions simply with a yes or no.

Auditors will need to think in advance of the audit **the approach** that they will take in order to obtain the evidence necessary for them to answer the questions on their High Level check list. This will require the auditor to think very carefully about specific locations that they need to visit and personnel that they wish to ask questions of / interview. This is a very important part of the audit planning process upon which the success or failure of the audit will depend.

An auditor needs to think very carefully **about the objective evidence** that they will need to be able to answer the questions on their High Level check list and how they will obtain this evidence. By examining each question on the High Level check list the auditor will be able to determine the best approach to take to obtain information / evidence that will enable them to answer the question. By taking each question in turn eventually a pattern will emerge which will enable the auditor to visit specific locations / personnel and in a particular sequence that will enable the necessary objective evidence to be obtained in a logical and time efficient way.

The plan of action may result in the identification of some specific staff that the auditor wishes to interview, this will enable the auditor to inform the company in advance that the presence of such staff would be necessary and so enable the company to provide for their availability. However, it is not normally necessary to be so specific in advance of an audit unless there are very real reasons why a key individual may need to be seen. The audit visit schedule will have alerted senior staff as to the need for the presence throughout the audit of key staff, for which provisions may easily be made if the visit schedule is supplied far enough in advance of the proposed audit date.

It is not possible to be totally accurate with this plan of action and a degree of flexibility will always need to be maintained as audit information is revealed. However by thinking in advance the auditor is far more likely to not only be able to quickly access the necessary objective evidence, but will also be able to retain control of the audit rather than being led by the auditees.

The plan of action will need to be supported with a Low Level check list of specific documents, records etc. that need to be examined by the auditor and some specific questions that will need to be asked of managers and staff to obtain information and access to evidence.

8.3.1.3 Low Level Check Lists

These are produced by auditors for use during the audit and to act as a reminder to the auditor of what is to be examined, sample sizes and specific questions to be asked of auditees to obtain information, clarification or confirmation of responsibilities, actions etc

Effectively, low level check lists are an extension of the auditor’s memory and are an important output from the detailed audit planning process. An auditor cannot commit to memory all of those things that they wish to examine and specific questions to be asked, particularly if the audit is conducted some days after planning is undertaken.

Throughout the on-site audit the low level check list will act in support of the audit process and will remind the auditor of all of the samples and questions that the auditor identified whilst planning the audit.

A plan of action and low level check list will need to be produced for each specific audit task allocated to an auditor. The plan of action should not be confused with an audit visit schedule. The audit visit schedule identifies individual audit tasks to be undertaken by auditors in different departments or areas of the service provider, each individual audit task requires a plan of action and associated low level check list (however, for short on-going oversight audits the audit may be so restricted in scope that in practice the schedule and plan of action are one and the same).

SUMMARY OF AUDIT PLANNING:

❑ ***High level check lists remind the auditor of the audit objectives and act as an important record of the intended audit sample and final overall audit result.***

❑ ***The plan of action and associated low level check list will greatly assist the auditor to plan an audit and to remain in control throughout the audit process. This in turn leads to confidence on the part of the auditor. The auditor knows what they are looking for and where they will go to find this evidence. It helps to avoid random, haphazard and non systematic auditing.***

The planning methodology previously described can assist auditors to undertake searching and in-depth audits in a fully systematic manner, making the best use of the available time and causing the minimum of disruption to those being audited.

Evidence of in depth detailed audit planning provides audit management (and hence NSA top management) with confidence in the audit process.

8.4 Audit Conduct

8.4.1 Audit Entry Meeting

Upon arrival at an ATM service provider and before commencing any audit activities the team leader should hold a brief audit “Entry” meeting in order to introduce the audit team, communicate the objectives and scope of the audit, and provide details concerning the basic audit process to ensure that both parties have a clear understanding of how the audit is to be undertaken. The entry meeting is an opportunity for the team leader to ensure that the ATM service provider management understands and feels comfortable with the process that is about to be undertaken. It is normal practice for entry meetings to involve all key members of the management team of the service provider together with all audit team members.

The audit team leader is responsible for ensuring that all arrangements are in place and satisfactory to support and facilitate the audit process. This will include ensuring that each auditor will be accompanied by a suitable person from the service provider organisation who will be senior enough and sufficiently knowledgeable to act as an audit guide, able to fulfill the practical function of guiding, introducing, facilitating access to areas, people and information, and maintaining a parallel record of audit findings, whilst at the same time not inhibiting the audit process in any way (by being too senior, distracting or disrupting the audit process by either asking audit questions of auditees or responding in place of the auditees). It is often the case that the Safety Manager or a senior director may wish to accompany the audit team leader - this would be likely to inhibit the audit process and is to be discouraged.

Throughout the audit process the **audit guides** will become an important communication link between the auditors and the company. They may also be requested to maintain a record of audit findings in order to be in a position to support the auditors' findings should they be disputed by the service provider management.

AUDIT GUIDES MAY BE USED TO:

- ❑ ***Assist the auditor to find specific locations and service provider staff,***
- ❑ ***Introduce auditors to auditees and resolve any difficulties,***
- ❑ ***Facilitate access to service provider documentation,***
- ❑ ***Translate the language of company terminology for the auditor,***
- ❑ ***Translate the language of requirements for auditees,***
- ❑ ***Maintain a record of findings.***

If the audit is being conducted over several days the audit team leader should consider offering a short meeting at the end of each day when results obtained so far may be indicated to a designated member of the management team (usually this could be the Safety Manager or equivalent). Detailed discussion concerning any findings should be avoided, however it may provide opportunities for clarification on either side.

All of the above should be adequately addressed at the entry meeting.

Audit Entry Meeting - Typical Agenda

Introductions
Team Leader and individual audit team members
Service provider representatives

Purpose / Objectives of the audit
(e.g. routine oversight / compliance with ESARRs, etc.)

Scope of the audit
(areas of service provider to be audited)

Oversight visit schedule
(times when each area / person will be visited and by whom)

Audit limitations
(audit conclusions based on limited sample / snapshot in time)

General administrative arrangements
Office facilities
Audit guides
Health & Safety considerations
Lunch arrangements
Etc.

How results will be formally communicated
(reporting mechanism / documentation)

Closing meeting arrangements

Confidentiality

Questions

Entry meetings should be confined to addressing the essential minimum agenda items as detailed above and should not be allowed to drift into other subjects consuming unnecessary time unless considered by the team leader to be important to discuss before commencing the audit.

It is normally more productive to keep the meeting moving briskly and transfer any problematic items or additional topics raised to a brief discussion immediately after the meeting with concerned persons only, rather than the full management team.

Although the audit team leader will chair and control the entry meeting, such control should be tactful, diplomatic and fully respect the authority of the ATM service provider management team.

The entry meeting is an opportunity to build a good working relationship with the ATM service provider senior management. This will help to diffuse any problems that might be encountered during the audit process.

8.4.2 The Audit Investigation

It is the responsibility of the audit team leader to ensure that audit investigations are conducted effectively and that the audit objectives are achieved. The team leader is responsible for managing the audit and the audit team, and for acting as the main communication channel with the ATM service provider throughout the audit process.

Each auditor is responsible for verifying the required requirements within the time allocated, and for ultimately ensuring that they satisfy their respective audit objectives.

The audit team leader will need to ensure adequacy of communication between the team members and make decisions regarding the necessity of following any audit trails. Regular **team meetings should be held throughout the audit**, at convenient times such as lunch and at the end of each working day, when findings may be discussed and progress towards objectives judged.

If the team leader is the only auditor, in place of team meetings the auditor should set aside periods of time throughout the audit to review results, check on progress and determine the necessity to follow audit trails.

If the auditor (or audit team leader) considers it to be necessary due to the difficulty of verifying certain requirements or the need to follow particular trails that are considered to be very relevant to evaluate the effectiveness of the provider's management of safety, the audit visit schedule may be modified, however as it has previously been agreed with the ATM service provider such modifications will also need to be agreed.

TO NOTE THAT**: **it is not normal however for an audit to be extended except in exceptional circumstances. However if the audit team leader feels that this is necessary it should first be discussed and agreed with Audit Management.

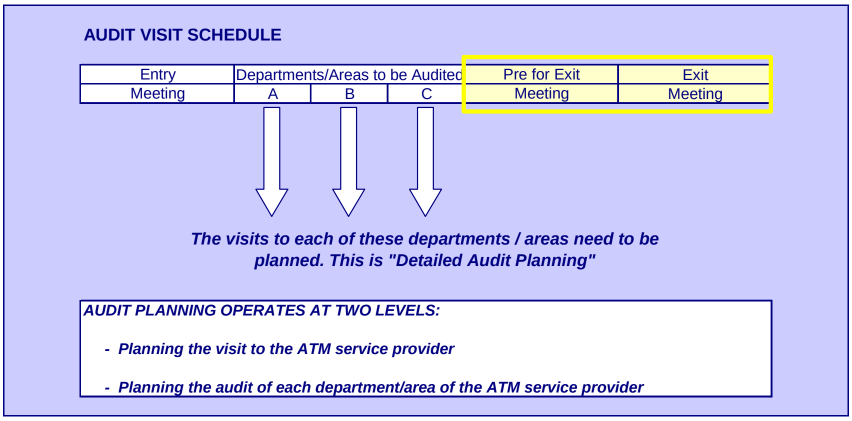
Throughout the audit process, auditors should work first with their pre-prepared check lists and plans / strategies. However as the audit investigation proceeds it will inevitably be necessary to deviate from or even significantly modify or revise these plans, or to follow audit trails in order to complete a verification. There is no problem with making such changes or deviations to the intended plan or strategy providing that the original audit objectives are satisfied. The important point to note is that such changes are as a result of conscious decision making by the auditor, who remains in full control of the process. Such changes are therefore 'controlled changes'.

TO NOTE THAT: a complete lack of audit planning coupled with the continuous following of audit trails in a haphazard way and simply investigating whatever looks interesting on the day is not regarded as professional auditing. Whilst it might reveal certain weaknesses it does not confirm in a systematic way compliance with specific requirements and hence is of little value to NSA senior management who need to make decisions.

Throughout the conduct of the audit auditors should always remind themselves that they need **evidence that proves to them** that practice is in conformity with the stated intentions of the service provider, as detailed in its documented safety-related arrangements, and complies with applicable safety regulatory requirements. A planned approach will assist this.

8.4.2.1 Auditor(s) Final Team Meeting

Before conducting an Exit meeting the audit team should meet at a final auditors' team meeting when all audit results should be **reviewed** and final conclusions reached. The audit team leader[34] will wish to identify all audit non-compliances that have been revealed throughout the audit process and their significance in relation to the implementation and effectiveness of the safety management system and compliance with the regulations.



AUDIT VISIT SCHEDULE

Entry	Departments/Areas to be Auditec			Pre for Exit	Exit
Meeting	A	B	C	Meeting	Meeting

The visits to each of these departments / areas need to be planned. This is "Detailed Audit Planning"

AUDIT PLANNING OPERATES AT TWO LEVELS:

- Planning the visit to the ATM service provider

- Planning the audit of each department/area of the ATM service provider

The audit team leader will need to produce a **summary statement** that will communicate the audit findings and identify the major concerns revealed by these findings. Such a summary statement should not be a list of audit findings (non-conformities), but the overall picture that the audit has revealed in relation to the number of nonconformities found in relation to the applicable safety regulatory requirements and areas of the organisation or processes undertaken. It is recommended that major concerns revealed by the audit are clearly communicated to the management team of the ATM service provider, together with examples of the findings that have led to such conclusions. The audit team leader will not be in a position to pass any form of judgment on the final conclusions that will be reached by the NSA and should not enter into any discussion on this matter.

All audit findings (non-conformities) should be used as an input to the summary statement, and written details of all findings should be produced by the auditor(s) and copies handed to the ATM service provider highest level manager attending the exit meeting. NSAs may wish to consider the advisability of requiring this manager to sign documentation indicating acknowledgement that such findings have been raised by the auditor(s) and communicated at the exit meeting. This can help to overcome possible future disputes over findings when the final report is received from the NSA.

[34] *Or the auditor wherever he/she is the only person forming the audit team. This footnote is also valid throughout the remainder of Section 8.4 of this document.*

8.4.2.2 Audit Exit Meeting

Before leaving the audited organisation the audit team leader should always ensure that the audit findings are presented to the audited organisation both verbally and in writing. Following the audit it would be normal practice to provide a formal report to the NSA within a specified timeframe.

> ***TO NOTE THAT**: **it is important that the report to the NSA is based only on the facts presented to the ATM service provider management upon completion of the audit.***

It is accepted good practice to conduct a short exit meeting, chaired by the audit team leader and attended by all audit team members and to which the management team of the audited organisation are invited.

It is an important meeting at which the audit findings are to be **clearly presented** to the audited organisation by means of a short presentation by the team leader, supported if necessary by the team members, and copies of the audit findings in the form of well written noncompliance statements are passed to the audited organisation[35] .

> ***TO NOTE THAT**: **some NSAs may require the auditors to obtain signed agreement with the audit findings in order to overcome the possibility of future dispute.***

Audit team leaders should endeavor to ensure that exit meetings are not conducted only with the safety/quality manager (or equivalent manager), but also with key members of the **senior management team**, including as a minimum the head of the service provider organisation or the head of ATM operations. It is important to convey to the organisation’s senior management that **the management system is their system** and not the safety/quality manager’s system.

(Space Left Intentionally Blank)

[35] *The NSA should provide standard forms for the recording and reporting of audit findings. For some examples of possible forms see the appendices to this document.*

Audit Exit Meeting - Typical Agenda

Introductions
Team Leader and individual audit team members
Service provider representatives
(retain a record of who attended the meeting)

Purpose of the meeting

Purpose / Objectives of the audit
(routine oversight / compliance with ESARRs etc.)

Scope of the audit
(areas of service provider audited)

Thanks for co-operation / assistance, etc.

Confidentiality
(indicating that all information will remain confidential)

Formal report
(when it will be sent to the service provider)

Audit limitations
(conclusions based on limited sample / snapshot in time)

Summary statement
(main areas of concern revealed by the audit)

Audit Findings
(non-conformities presented and explained)

Regulatory process for corrective action, follow up and audit close out

Questions

Exit meetings should be brief and should not be used to debate the findings at great length. It is only necessary to ensure that the service provider senior management understands the findings. It is important that all findings are expressed **factually** and **objectively** and that they are not merely auditor's opinions or simply unproven nonconformities resulting from the auditor's inability to undertake an effective audit investigation.

If there are a large number of audit findings then it may be acceptable to verbally present a sample of those upon which the major concerns are based, however copies of **all** findings should be provided to the service provider management. The NSA should provide specific documentation that will need to be used by auditors for the recording audit findings / summary statements and for providing this information to the service provider.

8.4.2.3 Important Points to Note with Respect to Audit Exit Meetings

It is important that audit findings are **expressed as factual evidence found** by the auditor **or the inability of a responsible person to provide appropriate evidence** during the audit process. This will help to prevent unnecessary debate about audit findings and will also safeguard the possible disagreement over audit findings[36].

[36] *See also the guidance on writing non-conformity statements in this document.*

The audit team leader will not be able to provide any conclusions of the audit as these will need to be carefully considered by the NSA before being communicated to the service provider. However, the audit team leader may indicate a general level of significance of audit findings if the NSA has provided a method for determination of such.

As a general rule, auditors **must NOT make any recommendations** to service providers in relation to the specific corrective action that must be taken to overcome a reported audit finding as this will effectively transfer the ownership of the failed process from the service provider to the NSA and render the NSA liable to any resultant consequences.

Auditors should follow the audit process requirements provided by the NSA. This is particularly important for NSAs commissioning recognised organisations to conduct audits on behalf of an NSA.

> ***TO NOTE THAT**: auditors should not make recommendations as to the corrective action that should be taken to correct any identified nonconformities. To do so immediately transfers the ownership of the problem and compromises the auditors' independence for future audits. For NSA auditors, making recommendations immediately renders the regulatory authority legally liable for any consequence of such recommended corrective actions.*

However, there should be a mechanism in place that enables a NSA auditor to react immediately to a **major safety-related issue revealed** by an audit such that the auditor, acting under delegated authority of NSA senior management, may require immediate action to be taken by the ATM service provider in advance of the normal audit reporting mechanism. NSAs will need to develop suitable defined processes to enable fast tracking of serious safety critical audit findings. Without such fast tracking mechanisms the NSA could become partly responsible for safety failings / incidents due to known significant problems remaining unattended to by the ATM service provider.

Indeed, it should also be noted that regulatory auditors, such as NSA auditors, may be **sometimes delegated the authority to request corrective** action on behalf of the NSA.

This does not complicate the audit process providing that the auditor understands that first they act as an auditor and then armed with the facts they then require corrective action to be taken. It is the auditor's client in the form of the “designated point of responsibility” in the NSA who needs to determine if corrective action is necessary, and the time frame, and NOT THE AUDITOR. However for regulatory audits the NSA auditor may be given a delegated responsibility and authority from the “designated point of responsibility” to drive the corrective action process until a satisfactory resolution of non-compliances has been obtained.

The delegation of authority to request corrective actions and the mechanisms to react to major safety-related issues revealed in an audit are special situations to be clearly defined in the audit processes established by Audit Management. These special arrangements should not apply wherever the audit team leader is personnel of a recognised organisation.

8.4.2.4 Non Fulfillment of Audit Objectives

In the event that an auditor or audit team is unable to complete the original audit objectives, for whatever reason, **the matter should be referred to** the audit management function within the NSA. It is this function that will decide if additional audit activity is required to complete oversight objectives

8.5 Auditing Techniques

The Appendices to this guidance illustrate typical approaches to providing a formal **"visit schedule"** for auditing an organisation, involving one or more auditors visiting different departments over a period of several days. These schedules identify which departments will be visited by each of the auditors and at what times. They also identify the key managers that the auditor(s) would like to meet either for the purpose of conducting a formal interview or to begin their audit process within that department.

It should be noted that such "visit schedules" are **provided in advance** to enable the organisation to ensure the availability of all key staff who might need to be involved in the audit process, not simply the ones that may have been identified on the schedule but others who the organisation feels it would be beneficial to have present for the audit, recognising that at any stage of the audit process auditors may need to speak with various staff to obtain information or documentary evidence to confirm the effective functioning of processes comprising the management of safety.

The audit team leader will need to ensure that the individuals closely adhere to the schedule otherwise there is a danger that the audit objectives will not be met. Individual auditors are responsible for conducting their respective parts of the audit by the application of best practice auditing techniques.

Auditors must be careful not to fall into the traps of strong willed managers who wish to control the audit process to their own advantage, who wish to carefully restrict the auditors to see only those staff who will give the answers that the manager wishes the auditor to hear, or those who wish to show the auditors only those documents and records that they know to be 'good' examples demonstrating how well the system works. **Auditors need to select for themselves** who they speak with, where they go in the organisation and what they look at and examine. Organisations being audited need to allow the auditors this freedom, and although the auditors will indicate in advance those areas of the organisation and even possibly some key staff that they would definitely like to see out of courtesy or as the starting point for their audit, the audit process will inevitably require the auditor to visit staff and examine documentation or records as necessary and determined by the auditor during the audit process to ensure that an accurate picture of the true situation in the organisation is obtained.

Upon entering each department of an organisation auditors may wish to conduct an interview with the manager or may only wish to meet the manager as a courtesy and then conduct their audit with other appropriate staff members. The auditors will not require the manager to accompany them when they visit staff members as this **could seriously inhibit** the process, instead it is normal practice to arrange for 'guides' or 'escorts' to accompany each auditor simply to help them to move from location to location and to introduce them to the various staff members.

The auditors will need to test the processes by taking appropriate **samples** of documents and records and by observing actual working practices, and by judging what they see against the **"audit base"**. The audit base will be a combination of the requirements together with the organisations approach to meeting the requirements and as defined within its declared management system documentation[37]. When the auditors find a departure from the audit base the auditor will record this departure as an audit finding in the form of an **"audit finding"** or **"non-compliance"**. The audit finding will be stated as a combination of the facts observed, where these facts have been found and identification of the exact requirement (regulation or company procedure or internal requirement) the departure is against. At the end of the audit, the audit team will look at all such audit findings and try to summarise what these findings are indicating (possible weaknesses in the overall system).

The amount of documentation examined, the number of staff interviewed or questioned will be planned to a limited degree in advance of the audit, and good auditors will always have a personal "plan of action" (or strategy) which they believe to be a suitable approach to obtain the necessary audit evidence. This personal "plan of action" will identify appropriate staff at all levels and organisation functions, however it will not be communicated to the organisation as it will need to remain flexible and is also dependent on the evidence that is revealed during the audit.

8.5.1 Audit Sampling

An audit is never a 100% check that a system is functioning fully effectively. It is **always a sampling activity** where the auditor **'tests' the system** by looking at a relatively small sample of everything that could be looked at in order to obtain a degree of confidence in the effective operation of the system. Depending upon the previously judged confidence in the system and/or the specific audit objectives an auditor may sample a management system by looking at a relatively small sample or a much larger sample. Where confidence in a management system is low then relatively larger samples should be taken.

8.5.2 Searching for Evidence of Compliance

Auditing involves a process of investigation where the auditor is entering the audit target area with an intention to verify that certain things are happening and that particular elements of the provider's documented arrangements are functioning effectively. The view should always be taken that the auditees are indeed operating their documented arrangements effectively unless the auditor is able to prove otherwise, and it is necessary for the auditor to undertake a suitable investigation to find evidence of compliance or noncompliance. Organisations are always able to find evidence to prove their case. It is the **evidence that they do not offer** which might indicate that their management of safety does not always function as intended and in a fully satisfactory manner, and it is therefore necessary for the auditor to remain fully in control of the audit process and what is examined to verify compliance.

Audits involve the collection of evidence in order to verify that what should be happening is actually happening. That practice is in line with intent. This requires the auditor to act like a detective, and working with 'clues' obtained from interviews and questions undertake the necessary investigations to find the evidence that proves compliance.

Interviews and questions will provide the auditor with the opportunity to view necessary documents and records.

[37] *For an example, see the figure included in Section 4.3.3 of this document. In that figure the audit base is formed by the "required procedures and required arrangements" and the "written procedures and written arrangements and their expected results".*

The auditor’s detailed checklists and associated plans of action will generally steer the audit process through a range of activities aimed at searching out evidence to confirm conformance with the High Level checklist.

The task of the auditor is to verify that what is prescribed in the documented arrangements is happening in practice, and that stated objectives are being achieved, (i.e. what is stated by management to be happening is happening). Information gained through interviews should be tested by obtaining the same information from other interviews or independent sources such as observation of actual practice. Auditors should examine whatever they consider necessary in order to obtain objective evidence of compliance, including historical information in order to have confidence in the effective operation of the SMS over a period of time.

The auditor always needs **"objective evidence"**. Auditors take the view that the auditees are “innocent” until proven “guilty” and search for objective evidence of compliance to stated requirements. If the auditor is unable to establish compliance wherever it should be documented, then a noncompliance must be recorded. It is important to note that the auditor must not simply allow auditees to offer evidence that proves compliance. The auditor must test the system by examining evidence of the auditors own choosing that enables the auditor to judge that there is indeed compliance. If noncompliance is suspected then the auditor must be absolutely certain of the facts before recording noncompliance, particularly if such noncompliance could result in enforcement measures by the NSA.

Auditors will need to gain confidence that the management of safety is implemented effectively at all times, including during early morning shifts, shift handovers etc. This will require auditors to sometimes undertake audits outside of normal office hours or even at times of significant high workloads to verify that normal practices are not subject to unsafe variations.

TO NOTE THAT**: **Auditors should not be afraid to challenge auditees when they think that the evidence presented does not confirm compliance. If further evidence is required they should request / try to find it.

The auditor will need to conduct investigations as necessary to establish that the specific provisions of the applicable safety regulatory requirements are being met in an effective manner. This will require the auditor to remain fully in control of the audit process, visiting specific locations in order to gather data and evidence. The auditor will have previously transposed the requirements being verified together with the organisation’s intended methods of compliance, as detailed in manuals and associated documents, into checklists and will now need to adopt a suitable strategy to gain access to information of the auditor’s choosing which will confirm compliance. It is the responsibility of the auditor to decide on suitable samples of items to examine which will provide confidence that the Service Provider is implementing the declared arrangements in a way which satisfies the stated provisions of the applicable safety regulatory requirements in an **effective** manner.

It is important for auditors to understand that it is necessary to check that processes adopted by the service provider result in effective outcomes. This is particularly important for ‘objective’ based regulations as opposed to those that are more prescriptive.

As a simple example of what is meant by this:

- ❑ *There is a process for Lesson Dissemination which is described in a procedure. The auditor will check to see that the procedure is followed, but will also need to check to see that some incidents of a safety significant nature which have been investigated and identified lessons needing to be disseminated (e.g. information to staff, changes to working practices, etc.) have subsequently resulted in avoidance of similar incidents.*
- ❑ *The incidents traced through the process should be selected by the auditor and NOT the auditee (auditees can always find a 'good' example to show to an auditor). The sample selection process should be steered by the auditor's intuition of which type of incidents would be appropriate to select, or by performing a quick 'trend analysis' on available data concerning the types of incidents being reported.*
- ❑ *The auditor may obtain this data by reviewing incident data or by talking with controllers to get a 'feel' for the types of incidents that are in the forefront of their mind. Controllers, engineering and other staff can also provide the auditor with a good impression of lessons that have been disseminated and acted upon.*

Auditors will need to establish if processes are being operated, not just in accordance with procedures but that they are also effective and achieving the desired outcome(s). They will need to plan their audit to obtain evidence from sources that will indicate if a process is effective, and this will require them to think about what might be seen or experienced in the organisation if the process is not effective. For the example above, if the lesson dissemination process is not effective then there is likely to be repetition of incident occurrences of a similar nature over a period of time, such incidents having been investigated to determine root causes and requiring changes to working practices, but repeats of similar incidents is a possible indicator that the changes to working practices have not taken place.

This is more challenging for an auditor than simply checking to see that a procedure is being followed as it requires more investigative approaches to auditing and will need to be considered during the audit planning stages. Such techniques are in line with ISO 9001:2000 concepts, and **will need** to be adopted if full confidence in the management of safety is to be obtained.

> ***TO NOTE THAT: auditing will need to verify that processes are being operated such that the outputs from processes and eventual outcomes are meeting objectives set by management. This will require auditors to be aware of the desired performance targets for outputs and outcomes and use this information to establish if processes are effective.***

8.5.3 Process Effectiveness

Many auditors have difficulty in the concept of establishing process effectiveness. They are very used to the idea of establishing conformity to a procedure or instruction, however procedural compliance is not always a guarantee of process effectiveness.

As an example consider the following:

- *There is a process of predictive preventive maintenance adopted by an organisation in relation to equipment providing essential inputs into an ATC centre. There are comprehensive maintenance schedules and associated maintenance procedures.*
- *An auditor verifies that the maintenance schedule is applied and that specific procedures are followed. However, examination of the equipment defect / failure history indicates that there are a significant number of defects / failures that are attributable to inadequate maintenance and are resulting in the equipment functionality availability targets not being met. Hence the maintenance process is not effective. Improvement of the maintenance process may require improvement to the maintenance schedules and/or procedures. Auditing only in relation to the procedures being followed and not also considering the process 'outcome' will not provide full confidence in the process.*

The International Standard ISO 9001:2000 is very much concerned with the need for processes to be managed effectively and monitored to verify conformance with process performance objectives. Auditing in relation to ISO 9001:2000 requires auditors to establish if the organisation is managing processes effectively and desired process 'outputs' and eventual 'outcomes' are being achieved[38].

It may help an auditor to think about the likely effects that would be seen if a process were not effective in order to assist understanding of how to audit for process effectiveness.

As an example consider a selection and recruitment process:

Likely effects of an ineffective selection and recruitment process:

- *High staff turnover as a result of recruiting staff who do not have the necessary aptitudes, attitudes or competence.*
- *High levels of staff absence due to staff being generally unhappy with their position.*
- *Inability to provide short notice staffing to cater for sickness etc. due to staff reluctance to cover for others.*
- *Generally bad attitudes (such as bad timekeeping).*
- *High level of incidents as a result of lack of attention to detail.*
- *Not filling out necessary reports*
- *Lack of improvement culture*

8.5.4 Process Management

A process needs to be managed effectively if it is to provide acceptable outputs and if the eventual outcome is to be as required.

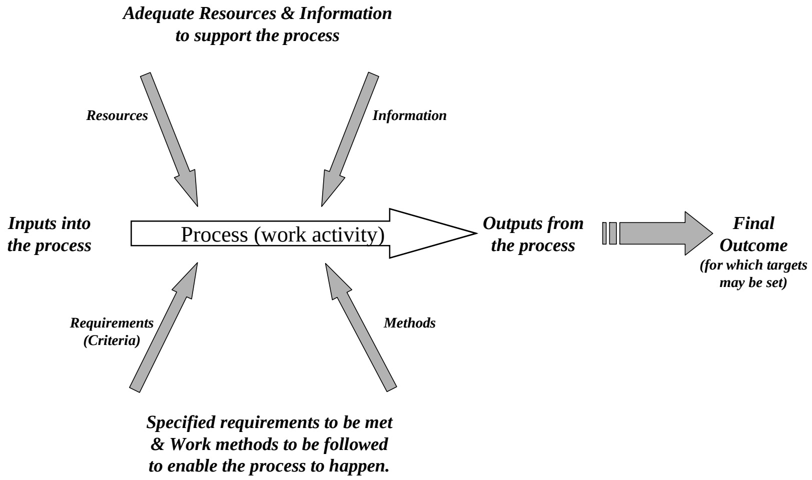
A simple example to illustrate the difference between an output and outcome:

- *A coffee machine dispenses coffee to the required specification. This is the output from the coffee making process.*
- *An organisation wants to provide refreshments to make their customers experience better. Customers drink the coffee and they enjoy the coffee. This is the outcome of the coffee making process.*

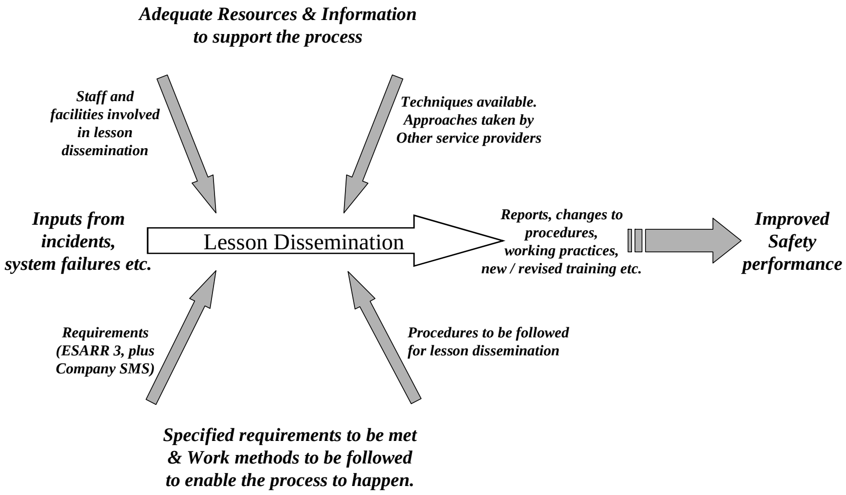
[38] *Examples of process 'outputs' and process 'outcomes': the information from a controller to a pilot is a process output, safe transit through airspace is the process outcome.*

- *It is clearly possible for the 'output' of the coffee machine to fully meet the specification, but the final 'outcome' could be that customers do not enjoy the coffee.*

Similarly, an ATM service provider may have processes that provide outputs that are considered to be acceptable but the final outcome is not fully satisfactory.


Adequate Resources & Information to support the process
Resources
Information
Inputs into the process
Process (work activity)
Outputs from the process
Final Outcome
(for which targets may be set)
Requirements (Criteria)
Methods
Specified requirements to be met & Work methods to be followed to enable the process to happen.

Processes need to be managed using a combination of adequate resources, correct and sufficient information, use of appropriate work methods and identification of requirements that must be met as the process is undertaken. It is the responsibility of a 'process owner' to ensure that all of these have been determined and are provided to ensure that the process is undertaken correctly and provides the necessary outputs. However the eventual desired outcome should be defined and checked. If the outcome is not as desired then the management of the process may need to be revised or the process may need to be re-engineered.


Adequate Resources & Information to support the process
Staff and facilities involved in lesson dissemination
Techniques available. Approaches taken by Other service providers
Inputs from incidents, system failures etc.
Lesson Dissemination
Reports, changes to procedures, working practices, new / revised training etc.
Improved Safety performance
Requirements (ESARR 3, plus Company SMS)
Procedures to be followed for lesson dissemination
Specified requirements to be met & Work methods to be followed to enable the process to happen.

This can be illustrated in relation to the "Lesson Dissemination" process, where the output(s) from the process may be various actions to be taken (procedure changes, training, etc.) but the outcome will be improved safety performance.

The management of the process will need to be achieved through the actions indicated in the above diagram.

Auditors will need to develop the technique of obtaining information from one source, working with the information to analyse and understand what it is revealing and then to use this information at another location in order to test the system.

For example:

Assuming that there is the following requirement:

“System Safety Assessments will need to be undertaken when there has been a significant change to the system or any system element (hardware or software)”.

- ❑ *To verify that this is indeed happening the auditor should first obtain from one source the list of system changes / modifications that have been undertaken in say the previous 18 months. This information may be contained in some form of equipment change log or configuration management system, possibly available on a database in the Engineering Support Department. The auditor may also ask for information from an Engineering Support section leader on what constitutes a ‘significant change’ and hence warrants a safety assessment (asking for details of the criteria for judging the safety significance of changes).*
- ❑ *Once this information is obtained, the auditor may then select two or three significant system changes and identify the responsible Engineer / Manager for these parts of the system. This Engineer / Manager may then be interviewed and requested to explain the process of system safety assessment before the auditor requests the safety assessments carried out as a result of the previously identified changes.*

8.5.5 Examples of Poor Auditing Techniques

Example 1 – Accepting a manager’s statement as factual evidence:

- ❑ *Reply from a manager / senior director - “We certainly always give safety the highest priority over any commercial considerations”.*
- ❑ *This statement provides no factual (objective) evidence. There is a need to see several examples of factual evidence that proves for particular decisions that safety has indeed been given the highest priority over any commercial considerations*
- ❑ *The auditor might then follow with a response - “May I see some examples where this has been the case?”*
- ❑ *The manager / senior director may now select a ‘good’ example(s) which demonstrates where they have indeed given priority to safety. This is of little value to the auditor as it does not confirm that for all decisions safety is given priority, and the manager / senior director is in control of what the auditor actually examines.*
- ❑ *The auditor should identify where in the organisation some decision have had to be taken where safety and commercial considerations could come into conflict, such as investment in new equipment, recruitment of new staff or maintenance programmes. The auditor should then access information relating to the decision making process (minutes of meetings, reports, e-mails, etc.) to obtain evidence that demonstrates that a selection of these decisions indeed put safety as the priority. This will require investigations by the auditor to identify specific cases requiring such decisions. These are best obtained at working level in the organisation in order to ensure that what is examined is not selected by a manager / senior director.*

Example 2 – Accepting a manager’s statement as factual evidence:

- ❑ *Trying to establish that safety-related responsibilities are understood and acted upon by a manager.*
- ❑ *Whatever a manager says is not fact, but an understanding obtained by an auditor who may not word the question so that it is understood by the manager, the manager may not be good at explaining, or the auditor may not understand or mis-hear the reply.*
- ❑ *Auditor’s question - “Could you please explain your safety-related responsibilities, and how you discharge these?”*
- ❑ *The manager can always find something to support what they say. It is much better to see if safety related responsibilities are being discharged through actions undertaken by managers. This will require the auditor to understand what the safety related responsibilities are and to look for evidence (of the auditor’s choosing) that will demonstrate that a selection of the responsibilities are being discharged.*

Example 3 – Accepting a very limited ‘sample’ as audit evidence:

- ❑ *Examination of records in one part of the organisation and relating to one activity only as evidence that the keeping of records is fully acceptable.*

Example 4 – Not taking larger samples wherever a small sample indicates a problem:

- ❑ *An auditor discovers a problem and correctly records a nonconformity. However, the auditor does not then take a larger sample to establish if the problem is more widespread.*
- ❑ *For example, a selection of Incident Investigation Reports is examined, and the sample reveals that there is one Incident Investigation that was not commenced until many days after the incident occurred.*
- ❑ *The auditor should take another random sample of Incident Investigation Reports but from a time period many months before or after those originally sampled. This will reveal if the original sample revealed only an isolated incident or that the lack of timely investigation is a common situation.*

Example 5 - Not looking for full evidence to confirm the effectiveness of a process:

- ❑ *An auditor is attempting to verify the “Lesson Dissemination” process required in ESARR 3.*
- ❑ *The auditor has identified how the process works, with trend analysis of equipment related concerns / problems / failures providing information relating to the need of a change of working practice in relation to unscheduled maintenance of equipment following significant reported equipment defects.*
- ❑ *The auditor verifies that there has been a change in the procedures relating to the reporting, investigation and correction of equipment defects, and there has been a formal communication to both operational and maintenance staff. The procedure amendments took place nine months before the audit, and the communication was made immediately after the revised procedure was released.*

- ❑ *The auditor should take samples of records in various parts of the organisation and in relation to different processes undertaken.*
- ❑ *The auditor could verify that operational and maintenance staff are aware of the changed working practices, however, the auditor should look closely at the Trend Analysis since the changed working practices were introduced, to judge the effectiveness of the changes.*
- ❑ *However, if the procedural changes had only taken place a few months before the audit it may not be possible to verify that the procedural changes have been fully effective, and the auditor would need to verify the effectiveness of the changed working practices at a future audit.*

Example 6 – Not accepting 'no' for an answer

- ❑ *Reply from a manager / senior director - "Unfortunately I cannot show you that document as it is located with another member of the team"*
- ❑ *Auditor might then follow with a response - "No problem, is it possible that you could obtain it and let me see it later today?"*
- ❑ *The auditor will need to judge if it is important to see this document now or if it can wait until later in the audit. However there is always a problem that the auditor may become so busy with other matters that they forget about this request, or run out of time to see the document, or the manager may simply (conveniently) forget to provide the document.*
- ❑ *Better audit tactics: if the auditor considers that it is necessary to see the document now then the auditor should politely request to visit and talk with this team member. If the team member cannot be found, request if someone else has access to the document. If no one else is available then ask if there is access to the electronic version of the document. If they say that it is password protected then at least look to see if the file exists with the appropriate title, then ask if any other persons have access to password protected electronic documents in the event that the person for some reason suddenly leaves the organisation. Remember that passwords should always be formally issued or recorded and there will always be some way of accessing using the services of the I.T. function. Previous drafts may not have been password protected, and may be recovered through the periodic backing up system.*
- ❑ *To note that failure to be able to access any document could indicate a problem with the document issuing and control process.*

8.5.6 Significantly Bad Audit Practices

Unfortunately there are many bad practices which have been adopted by some auditors and auditing organisations, often due to a misunderstanding of the audit process and the responsibilities of auditors, or the use of the wrong 'type' of person as an auditor, lack of effective training, etc.

The following are a few of the more common ones encountered:

- ❑ Inadequate notification of an audit and therefore not allowing sufficient time for the audited organisation to ensure staff availability.
- ❑ Unannounced audits, which although sometimes may be necessary, send out the message of distrust and attempting to trick or trap.
- ❑ Arrogance or a demanding attitude on the part of the auditor, as opposed to adopting normal courteous behavior.

- ❑ Misuse by auditors of internal auditing results. By either reproducing nonconformities found in the internal audit results as the regulators own audit results, or by not planning an audit but simply looking into the internal audit corrective actions. In either case the audited organisation will eventually decide that it is not a good idea to have an effective internal audit process if in turn this leads to closer examination of identified and corrected nonconformities by the NSA. External auditors should only examine internal audit documentation to verify that an organisations internal audit process is functioning effectively, they should therefore not become too interested in the actual internal audit results themselves (although it is inevitable that such information will act as a guide to the auditor of possible areas of concern and hence areas for further investigation).
- ❑ The use of recording devices to record audit interviews. This is not recommended as it will intimidate and prevent individuals talking freely. It again sends out a signal of distrust. In the event that a recording device is to be used to capture only the auditors notes, permission must be obtained from the organisations senior management, and such use should be very discreet.
- ❑ Not presenting a closing, or exit, meeting upon completion of the audit and before leaving the organisation audited, and hence not making the audited organisation's management aware of the actual audit findings. This could result in later dispute with findings reproduced in formal reports, or conclusions reached if such findings were not made known before leaving the organisation and management given an opportunity to obtain any necessary clarification. It is a golden rule of auditing that audit findings must be made known to the audited organisation before the auditors leave the organisation. The auditors may not be able to communicate conclusions or requirements for follow on actions as this is the overall responsibility of the NSA. However they should leave the audited organisation with written copies of the audit findings upon which final conclusions, audit reports and follow on actions will be based.
- ❑ The term "audit findings" means the actual facts found by the auditors and written in the form of "non-conformity statements". Many auditors have great difficulty providing such statements, and lack of competence in this respect results in either opinions or global conclusions (both unsupported by facts and hence invalid in any court of law).

SUMMARY OF AUDITING TECHNIQUES:

- ❑ ***Auditors always need "Objective Evidence" to verify that a process functions effectively.***
- ❑ ***"Objective evidence should be obtained by auditors examining documents / records etc. of their choosing and by selecting appropriate representative samples.***
- ❑ ***Auditors should not treat the spoken word of the auditees as "objective evidence". This must be obtained by observation. However information obtained from the spoken word of several individuals may be used as confirmation of understanding by an auditor.***
- ❑ ***When a non-conformity is found, auditors should take larger samples, sometimes in different parts of the organization, in order to establish if the non-conformity is an isolated incident or a common problem across the organisation.***

8.6 Recording and Reporting Audit Findings to the ATM Service Provider

It is important for auditors to report findings factually and objectively. Techniques should be adopted that require auditors to record the audit findings in a way that will avoid dispute with the auditees and will ensure that the findings can be fully substantiated and understood by both auditees and future auditors who may be required to verify the adequacy and effectiveness of corrective actions taken in response to an audit finding. The recommended approach to be followed requires an audit finding to be stated in a way that clearly and succinctly captures the essential facts relating to the finding. These facts are:

- ❑ The objective evidence revealed to the auditor,
- ❑ Where in the organisation this evidence has been revealed, and
- ❑ The regulatory (or organisational) requirement that is not being met.

These facts then need to be incorporated into what is referred to as a **“non-compliance statement”** or **“audit finding”**. In fact, being able of drafting non-compliance statements is essential for auditors in order to present the facts related to the finding.

As an example consider this situation:

- ❑ *The following has been revealed to the auditor by investigating the organisation’s approach to AIRPROX incident reporting. Controllers are required by the organisation’s procedures to record all AIRPROX incidents on a particular form and to record certain information relating to the incident (date, time, traffic conditions, involved aircraft etc.).*
- ❑ *However it has been noted by the auditor whilst monitoring the involvement of a supervisor in relation to a Controller’s request for assistance due to high traffic rates causing an effective overload situation, that an incident has arisen which has been effectively handled but not recorded at the shift end.*
- ❑ *In this case the objective evidence is something that has been observed by the auditor. There is nothing that is tangible that can be referred to such as a document. However the recognised approach to reporting this audit finding is to identify that the incident has been observed by the auditor and that there is no evidence that the incident has been reported in accordance with the organisation’s procedure. Information is therefore needed to be included in the recorded and subsequently reported audit finding that clearly conveys the facts as observed by the auditor*
- ❑ *A typical audit finding might be written as a non-conformity statement in the following way:*

  “At the time of audit it was observed that an AIRPROX incident occurred and was effectively handled by controller position X with the assistance of the duty Supervisor. Following shift handover it was subsequently noted that this incident had not been recorded on the controllers or supervisors incident log as required by SOP 308, issue 03 which requires all AIRPROX incidents to be recorded on a controllers log as soon as possible and in any event no later than shift handover.”

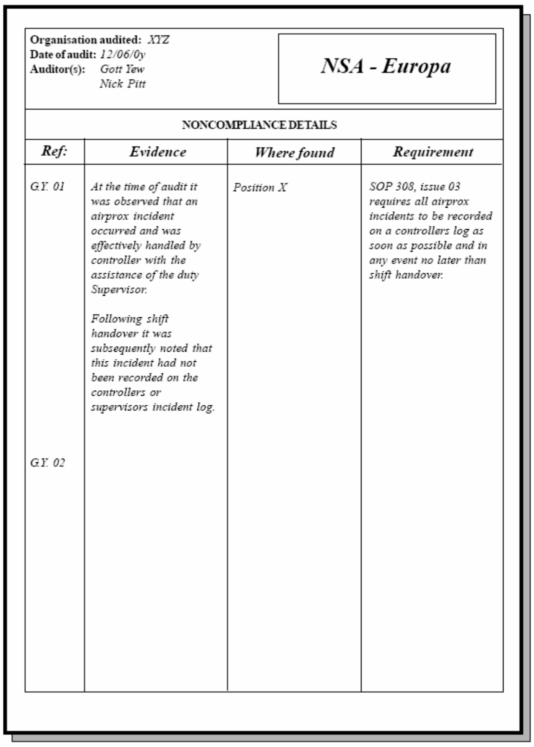
- *The three essential facts that have been captured are:*
  - *WHAT WAS OBSERVED BY THE AUDITOR? - The incident together with the controller and supervisors logs.*
  - *WHERE WERE THE FACTS OBSERVED? - At a particular controller and supervisory position.*
  - *WHY IS IT A NON-CONFORMITY? - Because there is a requirement specified in SOP 308, issue 03.*
- *From these facts it should now be possible to trace back to the incident, and there is a clear reference to a requirement that has not been met.*

It should be understood that unless an auditor is able to support audit findings with factual evidence then there is no nonconformity situation. If an auditor suspects that there is nonconformity then **he must obtain the facts to substantiate their view**.

The purpose of writing nonconformity statements in the style previously described is to ensure that bad audit practice of stating only opinions is avoided and the auditor is forced to work in an objective way and to obtain the necessary facts to prove that there is nonconformity.

> ***TO NOTE THAT: writing clear, factual non-conformity statements is one of the most difficult aspects for many auditors. Stating opinions is easy, and bad auditors will resort to this. However opinions are only opinions. They cannot be defended without facts. Whilst it may sometimes be acceptable to state opinions in reports alongside conclusions reached from an audit, they must all bear some relationship to the actual facts found.***

It may assist auditors to write clear and concise non-compliance statements if a standard audit non-conformity report form is used that requires information to be entered into particular fields by the auditor at the time a nonconformity is identified. An example of a typical form is reproduced below.



Organisation audited: *XYZ*
Date of audit: *12/06/0y*
Auditor(s): *Gott Yew*
Nick Pitt

NSA - Europa

NONCOMPLIANCE DETAILS

Ref:	*Evidence*	*Where found*	*Requirement*
G.Y. 01	*At the time of audit it was observed that an airprox incident occurred and was effectively handled by controller with the assistance of the duty Supervisor.* *Following shift handover it was subsequently noted that this incident had not been recorded on the controllers or supervisors incident log.*	*Position X*	*SOP 308, issue 03 requires all airprox incidents to be recorded on a controllers log as soon as possible and in any event no later than shift handover.*
G.Y. 02			

It is important that upon completion of the on-site audit and before departing from the service provider's facility the audit team leader should inform the service provider's management of the audit findings (verbally and in writing). Such findings will in practice be the factual details of nonconformities found during the audit, however the team leader may also indicate areas of 'concern' which whilst no direct evidence of nonconformity could be found give the audit team cause for concern that there may be a process / system weakness which should be investigated by the service provider. If such findings are not adequately communicated before leaving the service provider's facility dispute, over conclusions and / or findings detailed by the NSA in subsequent reports could arise.

TO NOTE THAT: it is of particular importance that conclusions reached by the NSA must always be traceable back to the audit findings.

The audit has been completed once the auditors have conveyed the findings to auditee management, verbally and in writing. Auditee management are fully responsible for the determination and implementation of appropriate corrective action in a timely manner to ensure that system weaknesses are rectified as soon as practicable. However, the NSA should be satisfied that corrective action proposed will deal with the root cause of the problem and when implemented is fully effective in eliminating the noncompliance found.

(Space Left Intentionally Blank)

9. REPORTING AUDIT FINDINGS AND AUDIT RECORDS

Auditors should follow the audit reporting process developed by the NSA audit management function. They should also use the report formats established in that process as a means of communicating to the NSA the results of the audits.

According with ESARR 1, Section 6.6, the audit report, including the details of the non-conformities, shall be forwarded to the “designated point of responsibility” within the National Supervisory Authority.

The audit team leader is responsible for finalising the audit report, organising its drafting in the audit team as appropriate, and submitting it to the “designated point of responsibility” in the NSA.

Section 5.3 of this guidance lists the **minimum contents** that auditors should normally include in the audit reports.

Auditors should particularly note that, depending upon the processes established by the NSA, the following may also be included as attachments to the report, or considered as separate record whose retention should be ensured:

- ❑ Auditor(s) check lists and associated notes,
- ❑ Copies of evidence (permission to use these should be obtained from the service provider),
- ❑ Auditor’s notes relating to audit samples, responses to questions, requests for information etc.

Reporting methods should ensure that the identified non-compliances are accurately reported, and **remain exactly as communicated** to the service provider before the audit team concludes the audit visit.

The report should also detail any general audit observations made by the auditor(s) relating to situations observed that whilst not a non-compliance could (in the considered opinion of the auditor) ultimately result in a non-compliance if the situation is not investigated by the service provider to clarify and confirm that the situation is under control. However, such situations should not be used by auditors as a means of attempting to communicate non-compliances which they believe to exist but for which the auditor has failed to undertake the necessary investigations to reveal factual evidence of non-compliance.

In such situations the NSA, may wish to advise the service provider that an investigation should be considered and may also wish to ensure that the situation is included as an additional subject for a future oversight visit. This should normally be done by the “designated point of responsibility” as part of the actions that may be needed following an audit. However, the NSA should not require investigations based only on auditor’s opinions unless there are very significant grounds for such.

> ***TO NOTE THAT: as pointed out in Section 5.3 of this guidance, such situations should not be used by auditors as a means of attempting to communicate non-compliances which they believe to exist but for which the auditor has failed to undertake the necessary investigations to reveal factual evidence of non-compliance.***

The processes established by Audit Management should require auditors to maintain specific records on its behalf. When following these processes, auditors should understand that audit records are not their personal property but the property of the NSA.

10. CORRECTIVE ACTION, AUDIT FOLLOW-UP AND CLOSE-OUT

10.1 Responsibilities for Action Following the Audit

Once the audit findings have been communicated to the audited organisation we then enter what is called the **"corrective action"** process.

The term "corrective action" has a specific meaning that relates to the action taken to eliminate the **underlying or root cause** of a problem or system weakness. It is not the term that should be used to refer to the action taken to eliminate the symptom. For example a medication such as an aspirin is often used to alleviate an undesirable headache. However the aspirin does not deal with what has caused the headache, such as stress or dehydration. It only acts to minimise the effect. Corrective action in response to a headache requires the identification of what has or is causing the headache and then implementing the necessary action to remove the cause, such as taking appropriate rehydration therapy in response to a headache caused by dehydration.

For audits that have been undertaken there will often be a requirement for the audited organisation to respond to the audit findings within a reasonable timeframe with appropriate corrective actions.

The purpose of the corrective action process is to identify the **"root cause"** of the problem that has resulted in the nonconformity found by the auditor, and then to determine a suitable corrective action that will address the root cause and so prevent future similar nonconformities. The root cause is usually a system weakness which is the responsibility of the management of the audited organisation to correct. Sometimes a staff member may be identified as being a root cause. However most staff failings can be traced back to a system weakness that has resulted in staff poor performance, for example lack of effective training, communication of requirements, etc.

In order to respond to an audit non-conformity and determine a suitable corrective action that addresses a root cause it is necessary for the management of the audited organisation to initiate the necessary investigation to establish if the audit finding was an isolated incident or an endemic situation, and also to fully identify what has given rise to the audit finding, i.e. the weakness in the system. There is often a tendency for such investigations not to be undertaken and instead to simply guess at what might have caused the problem. Working without factual data is not a good approach to solving problems.

Having undertaken an appropriate investigation and determined a likely root cause, the proposal for corrective action will need to be sent to the auditing organisation for formal review and agreement. Following the NSA's agreement, the corrective action will be implemented and at a later time some form of re-audit should be undertaken to verify that the implemented corrective action has indeed resulted in the elimination of further similar nonconformities.

Such re-audit activity results in the original audit finding being **"closed out"** if it is verified that the corrective action has effectively eliminated the root cause and 'symptoms' as found on the original audit are no longer evident. It may not always be necessary to undertake corrective action in relation to simple and straightforward audit findings. Some findings may be simple isolated documentation errors and omissions that are easily corrected and require no 'root cause' determination.

10.2 Planning and Conduct of Follow-up Audits

Whilst it is the responsibility of the audited organisation to determine and propose corrective action, it is often the case that this is left to the organisation's safety or quality function. However, it remains management's responsibility to investigate the circumstances surrounding the reported non-conformities and determine a likely root cause. In far too many audit situations the proposed corrective action is a 'quick fix' addressing the symptom of the problem only and not dealing with a likely root cause.

Once the corrective action is proposed there will be a need for the NSA to review the corrective action proposals for acceptability. The “designated point of responsibility” is the NSA focal point for this process. However, he/she may need to be assisted in this task. It is at this stage that many **auditors may be drawn back into the process in order to review the proposed corrective action** and advise on acceptance or rejection. They need to have a wide tolerance band of acceptability and must not try to 'impose' their solutions at this stage otherwise they will end up rejecting virtually all corrective action proposals.

It is the NSA that has the responsibility for ensuring that service providers understand when corrective action is necessary, and for providing the necessary process to be followed by the NSA in relation to all associated communications with the service provider together with the formal review, acceptance, follow up and close out of corrective actions and the auditing activities necessary to verify the effectiveness of corrective actions taken in dealing with the root causes of reported non-compliances. NSAs should provide a formal process that they require auditors to follow in relation to corrective actions, particularly where the auditors are working for a delegated NSA or contracted responsible organisation.

In many situations **audit follow up activity will be necessary** in order to verify not only that the corrective action has been taken, but that it has also been **effective** in dealing with the root cause of the problem, and that repeats of the originally observed symptoms (non-compliances) are no longer evident. If the situation is found to be satisfactory then the original audit finding(s) may be 'closed out'. The NSA has a responsibility to ensure the adequacy of the audit follow up and close out process and to keep good record relating to its activities at this important stage.

Follow up audits should be planned such that **similar samples** are taken to those that revealed the original non-conformities. This means not only similar samples but also samples designed to see that **related areas and activities** are also free from the originally observed symptoms.

There are many stages throughout the corrective action process where the process could go wrong. In particular it is the need to identify likely root causes which gives rise to the biggest problem, as often there is a tendency to just deal with the nonconformity found by the auditor and not investigate fully to identify a likely root cause. However there are other general weaknesses observed in audit corrective action processes such as badly written non-compliances, inadequate review of corrective action proposals and insufficient audit follow up sampling to verify that the root cause has been addressed and symptoms as originally identified by the audit are no longer evident.

(Space Left Intentionally Blank)

10.3 Audit Close-out

Once the NSA is satisfied that the root cause of an originally reported nonconformity has been addressed, and **no further symptoms of the problem** have been noted during the follow up audit then the audit may be ‘closed out’. This will require a formal sign off of the original audit finding and associated corrective action to indicate that the follow up audit has revealed no further similar findings and the audit report is ‘closed’. The date of the follow up audit and the verification action(s) should be recorded.

NSAs should not keep nonconformities ‘open’ for extended periods of time in view of the possibility that similar findings may be revealed during future ongoing oversight, they should require their auditors to undertake audit follow up verifications at appropriate times after corrective action implementation dates when it is judged that the corrective action taken would have had time to impact on the root cause and so prevent further similar nonconformities.

Corrective action verification and audit close out activities should be integrated with the annual programme of safety regulatory audits.

(Space Left Intentionally Blank)

11. APPLICATION OF AUDITING TO INITIAL OVERSIGHT

Section 6 describes in detail the use of auditing in safety oversight from a management perspective, including its use in initial and ongoing oversight processes.

The following guidance complements those contents to indicate to auditors the adaptations necessary when conducting safety regulatory audits as part of initial ongoing oversight of ATM service providers. The on-site auditing process remains the same. However there are specific approaches that need to be followed when planning for initial oversight audits when teams of auditors are involved.

11.1 Initial Oversight

The NSA will nominate an auditor to undertake an initial oversight of an ATM service provider. This should be an auditor who is competent to manage an initial oversight audit activity and lead an audit team. This auditor will be referred to as the audit “team leader” although it should be understood that dependent upon the size and complexity of the ATM service provider the audit team that is ultimately deployed to undertake the audit may comprise only the one auditor.

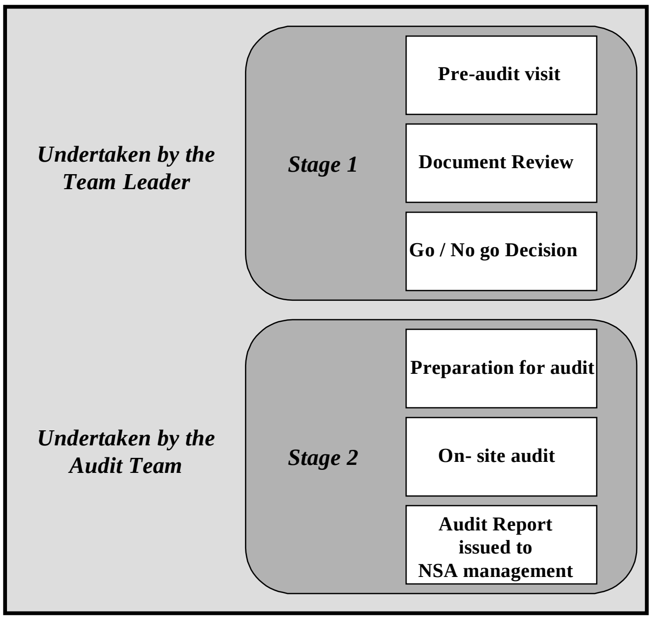
The team leader may need to undertake some form of pre-oversight visit in order to discuss the process with the service provider and to obtain some understanding of the organisation and facilities. The following process should then be adopted:

Stage 1 - often called a “Document Review”

To establish that the ATM service provider has developed an acceptable management of safety to meet all applicable safety regulatory requirements and to achieve the safety objectives of the ATM service provider.

Stage 2 – often known as “On-site Audit”

To verify that the provider’s management of safety is functioning effectively and is achieving the objectives of the applicable safety regulatory requirements and the safety objectives of the ATM service provider.



Examples of typical Initial Oversight audit schedules are provided in the Appendices to this document.

11.2 Planning an Initial Oversight Visit

An approach including the following steps and actions is proposed to audit team leaders and auditors when planning an initial oversight visit:

1

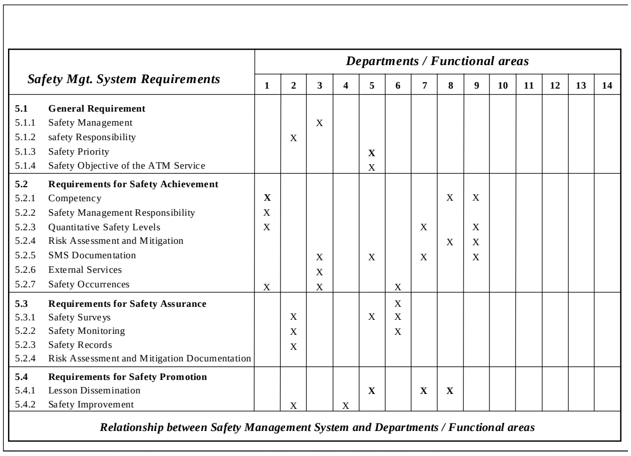
First of all, study the organisation and understand how it is organised and structured. Identify what departments exist and what work activities (processes) they undertake.

We can do this by studying documentation, undertaking pre-audit visits and by using Process Analysis techniques

2

Secondly, identify the different departments or areas of the organisation that need to be audited (the scope) and the requirements that need to be verified in each of them (the sample of requirements)

We may use some form of matrix chart to help us identify and record which requirements apply in each department / area and then we make sensible decisions as to which requirements will be verified in each of the areas.



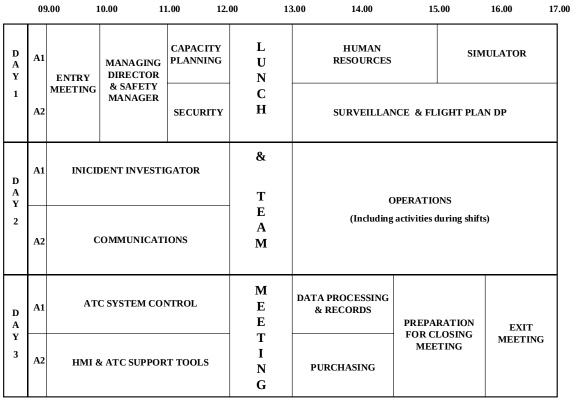
Safety Mgt. System Requirements	***Departments / Functional areas***													
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
5.1 General Requirement														
5.1.1 Safety Management			X											
5.1.2 safety Responsibility		X												
5.1.3 Safety Priority					**X**									
5.1.4 Safety Objective of the ATM Service					X									
5.2 Requirements for Safety Achievement														
5.2.1 Competency	**X**							X	X					
5.2.2 Safety Management Responsibility	X													
5.2.3 Quantitative Safety Levels	X						X		X					
5.2.4 Risk Assessment and Mitigation								X	X					
5.2.5 SMS Documentation			X		X		X		X					
5.2.6 External Services			X											
5.2.7 Safety Occurrences	X		X			X								
5.3 Requirements for Safety Assurance						X								
5.3.1 Safety Surveys		X			X	X								
5.2.2 Safety Monitoring		X				X								
5.2.3 Safety Records		X												
5.2.4 Risk Assessment and Mitigation Documentation														
5.4 Requirements for Safety Promotion														
5.4.1 Lesson Dissemination					**X**		**X**	**X**						
5.4.2 Safety Improvement		X		X										

Relationship between Safety Management System and Departments / Functional areas

3

We can then decide how much time needs to be spent in each of the departments and areas to undertake this verification. This will enable decisions in relation to the number of auditors, the duration of the audit and if any technical experts are required to support the audit team.

The output from this process will be some form of visit schedule that is agreed with and sent to the service provider in advance of the audit. The visit schedule will indicate the time to be spent by each auditor in the departments to be audited.



		09.00	10.00	11.00	12.00	13.00	14.00	15.00	16.00	17.00
DAY 1	A1	ENTRY MEETING	MANAGING DIRECTOR & SAFETY MANAGER	CAPACITY PLANNING	LUNCH	HUMAN RESOURCES		SIMULATOR		
	A2			SECURITY		SURVEILLANCE & FLIGHT PLAN DP				
DAY 2	A1	INICIDENT INVESTIGATOR			& TEAM	OPERATIONS (Including activities during shifts)				
	A2	COMMUNICATIONS								
DAY 3	A1	ATC SYSTEM CONTROL			MEETING	DATA PROCESSING & RECORDS	PREPARATION FOR CLOSING MEETING		EXIT MEETING	
	A2	HMI & ATC SUPPORT TOOLS				PURCHASING				

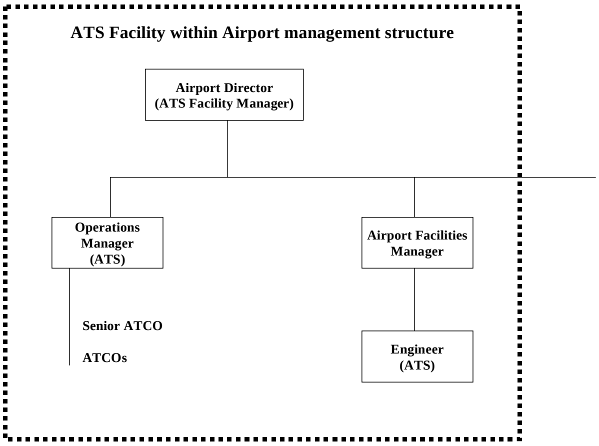
In addition, the individual auditors plan for their parts of the audit. They produce working documents to assist them during the audit (High Level check lists / Plans of Action / Low level check lists / documents to assist in the recording of evidences observed and audit findings, etc)

APPENDIX A

EXAMPLE OF PLANNING FOR INITIAL OVERSIGHT OF A SMALL SERVICE PROVIDER

It is assumed that the airport is a relatively small regional operation handling a combination of General Aviation, scheduled passenger services, light freight such as mail, etc (approximately 200 movements per day) serving a small city of approximately 300,000 together with the surrounding region and operated by the local government. It provides Air Traffic Services to aircraft within its Control Zone

The airport management team have delegated the provision of ATS to an Operations Manager, with the overall responsibility for the management of the ATS facility remaining the responsibility of the Airport Manager (identified as the Facility Manager for the ATS operation). Hence the ultimate responsibility for Safety Management lies with the Facility Manager. There is an engineering support function provided by the Airport Facilities Manager, drawing on specialist support services provided by external contractors. The ATCOs are supervised by a Senior Air Traffic Controller.


ATS Facility within Airport management structure
Airport Director (ATS Facility Manager)
Operations Manager (ATS)
Airport Facilities Manager
Senior ATCO
ATCOs
Engineer (ATS)

It is assumed that this ATS facility has been operating for many years and that it has developed a Safety Management System based on ESARR 3 which has been implemented for at least six months. The NSA has decided that it is now an appropriate time to undertake an Initial Oversight visit with a view to approving the facility.

General Sequence of Events

- Nomination of an individual within the NSA to manage the Initial Oversight of the ATM service provider (designated as Team Leader).
- Preliminary visit by the team leader to the ATM service provider to develop an understanding of the facility, its management structure, scale of operations and to obtain a copy of the SMS Manual (although in practice the regulator would in most cases already be familiar with the ATM service provider, for the purpose of this example it is assumed that the certificating NSA does not have this knowledge). Also to explain the Initial Oversight process.
- Undertake Stage 1 (Document Review) of the SMS Manual.
- Inform the service provider of the outcome from the document review (clarifications, additional documents that need to be viewed, identified weaknesses, etc.).
- Possibility of review of revised SMS Manual.
- Plan Stage 2 (the Initial Oversight visit - on site audit).

- Determination of ESARR 3 sample, resources required and audit schedule (Oversight visit schedule).
- Consideration for identified concerns resulting from the document review.
- Communication of Oversight visit schedule, proposed date for visit and necessary arrangements (it this case it can be recommended to be one to two months in advance of the visit for a small ATM service provider)
- Undertake detailed audit planning for the relevant ESARR 3 samples in the relevant areas of the ATM service provider.
- Undertake Initial Oversight visit.
- Provide ATM service provider with full details of audit findings in writing before leaving facility.
- Team Leader produces a full report of the Initial Oversight visit for the NSA designated point of responsibility. Provide details of findings exactly as indicated to the ANSP together with concerns and recommendations for NSA consideration and possible action. Report sent to designated point of responsibility in the NSA.
- Internal coordination takes place within the NSA in the light of the Report.
- NSA designated point of responsibility communicates Initial Oversight conclusions and necessary actions to ATM service provider.

It is assumed that the NSA is basically satisfied with the SMS Manual (that it conveys an understanding of the regulations, and indicates that appropriate mechanisms are in place to meet the regulations), however there is a concern that due to the very small size of the service provider and its integration within the overall airport management structure that the safety management function and safety survey process may not be fully effective, and hence this will be singled out for in depth audit activity.

Due to the small size of the service provider and the very limited number of managers and staff that will be available to the auditor(s) it would be inappropriate to conduct an initial oversight audit with more than one auditor. However NSAs need to consider the advisability of using two auditors to conduct initial oversight audits. (It has been noted that in some States an audit of this nature would be undertaken over two days using two auditors - it is considered that there are advantages to using two auditors if resources are available and in the early stages of auditing against the ESARRs it may be advisable for auditors to work in pairs).

Auditing to verify conformance with some requirements can at times be very difficult and time consuming, and the task is always easier when there are two auditors who are able to work together, share and exchange views, take notes and examine complex documentation. In some cases it may be necessary to take some documentation off-site in order to facilitate detailed study before continuing with the audit. Although this is not often undertaken, for Initial Oversight where the NSA needs to be satisfied that certain management disciplines are being effectively implemented such off site study may be necessary before confidence is obtained. This may be the case for documentation relating to Risk Assessment and Mitigation.

The Matrix chart below identifies the various departments / functional areas that comprise the service provider that is the subject of the oversight audit, together with the sample of ESARR 3 requirements that are to be verified.

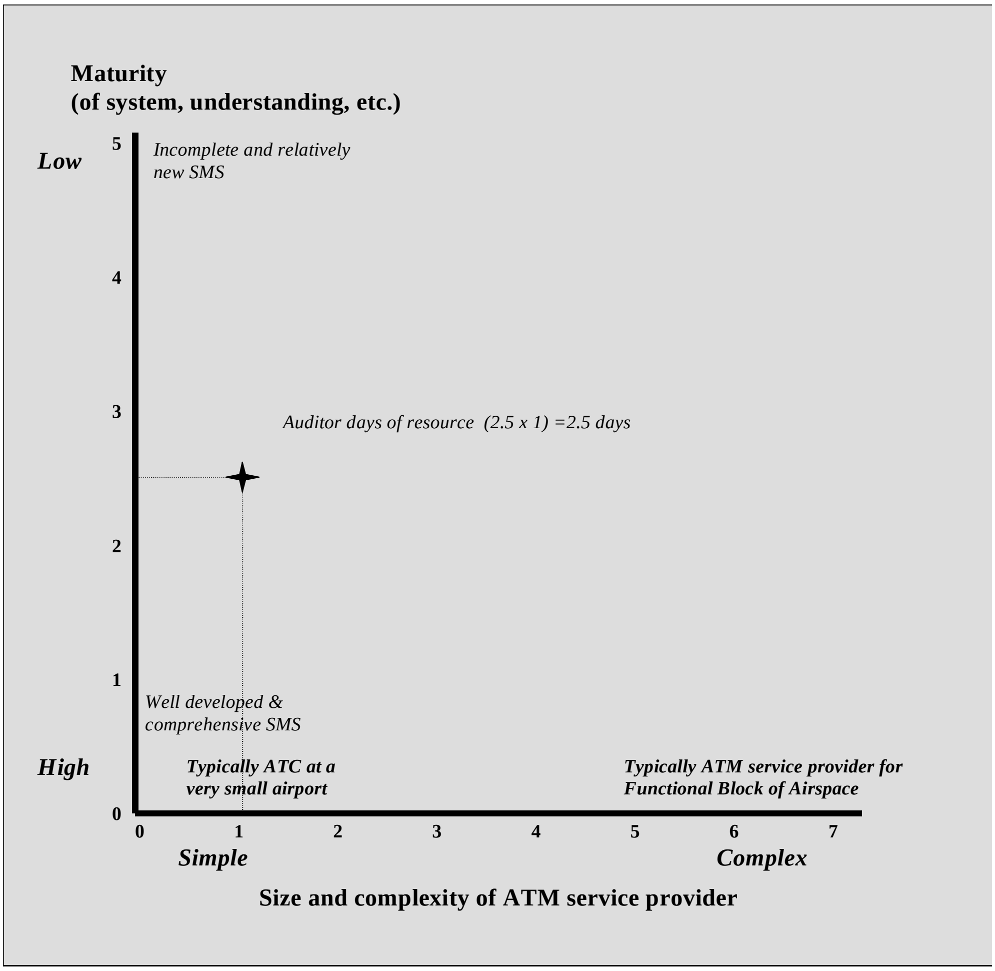
The audit team leader initially identified those ESARR 3 requirements that are relevant in the various areas of the service provider and has made a decision as to which specific requirements will need to be verified in each of the areas (only this final sample is indicated on the matrix chart). This is a very necessary planning activity. Auditing is always a sampling activity and for an Initial Oversight it is necessary to select an appropriate sample that is designed to verify those aspects off the SMS that have been fully implemented (for this example it is assumed that the service provider has implemented ALL ESARR 3 requirements for a minimum of six months).

Matrix chart identifying ESARR 3 requirements that are to be verified in the different parts of the ATM service provider

Departments / areas To be audited *ESARR 3 Requirements*		Facility Manager	Tower Operations	ATCOs	External Services	Operations Manager	Engineering
5.1	**General Requirement**						
5.1.1	Safety Management	x					
5.1.2	Safety Responsibility	x					
5.1.3	Safety Priority	x					x
5.1.4	Safety Objective of the ATM Service	x					
5.2	**Requirements for Safety Achievement**						
5.2.1	Competency	x	x				
5.2.2	Safety Management Responsibility	x	x				
5.2.3	Quantitative Safety Levels					x	x
5.2.4	Risk Assessment and Mitigation		x			x	x
5.2.5	SMS Documentation	x					
5.2.6	External Services				x		
5.2.7	Safety Occurrences			x	x	x	x
5.3	**Requirements for Safety Assurance**						
5.3.1	Safety Surveys	x	x				
5.3.2	Safety Monitoring			x			x
5.3.3	Safety Records			x		x	
5.3.4	Risk Assessment and Mitigation Documentation					x	x
5.4	**Requirements for Safety Promotion**						
5.4.1	Lesson Dissemination	x	x	x			x
5.4.2	Safety Improvement	x		x		x	x

Although this looks to be somewhat ambitious it should be recognised that due to the very small size of the organisation each of the requirements of ESSAR 3 may be verified in a relatively short space of time. However it is considered necessary to verify some requirements in more than one area of the ANSP in order to ensure that requirements are consistently met.

Using the previously developed model for resource determination, it is now possible to arrive at an estimate of the level of audit resource that might need to be used in relation to this example service provider.



For this example it is assumed that the organisation is relatively mature and that the document review has not revealed any significant concerns. The full SMS has also been in operation for a minimum of six months (hence the mid point of the 'maturity' axis). It is also assumed that the auditor is experienced and has a good knowledge of the service provider organisation and operations.

Note: In addition, audit resource is also required to ***plan and report*** *the initial oversight audit, and generally it can be estimated that a similar amount of audit resource will be required as that necessary to conduct the audit. Therefore for this example the total resource that is necessary to plan, conduct and report the initial oversight is likely to be* ***in the region of 5 man/day.***

(Space Left Intentionally Blank)

Example Visit Schedule - Small Airport ATC Facility (One Auditor for Two Days)

<u>Day 1</u>	
09.00	Entry Meeting
09.30	Facility Manager
12.30	Lunch
13.30	Tower Operations
15.00	ATCO
16.30	External Services
18.00	Close Day 1
<u>Day 2</u>	
09.00	ATCO
10.30	Operations Manager
12.30	Lunch
13.30	Engineering
15.30	Preparation for Exit Meeting
17.00	Exit Meeting
18.00	Close Day 2

(This visit schedule will need to be agreed with the service provider)

Tabular Representation of the Oversight Visit Schedule

09.00 10.00 11.00 12.00 13.00 14.00 15.00 16.00 17.00 18.00

DAY 1

Entry Mtg.	**Facility Manager**	**LUNCH** (working)	**Tower Operations**	**ATCO**	**Manager resp. for provision of External Services**

DAY 2

ATCO	**Operations Manager**	**LUNCH** (working)	**Engineering**	**Preparation For Exit Meeting**	**Exit Meeting**

Tabular Representation of Oversight Visit Schedule (indicating oversight audit sample – *sample NOT indicated to organisation audited*)

09.00 10.00 11.00 12.00 13.00 14.00 15.00 16.00 17.00 18.00

DAY 1

Entry Mtg.	**Facility Manager**	**LUNCH**	**Tower Operations**	**ATCO**	**Manager resp. for provision of External Services**
	ESARR 3 5.1 5.3.1 5.2.1 5.4.1 5.2.2 5.4.2 5.2.5	(working)	ESARR 3 5.2.1 5.4.1 5.2.2 5.2.4 5.3.1	ESARR 3 5.2.7 5.3.2 5.3.3 5.4.1	ESARR 3 5.2.6 5.2.7

DAY 2

ATCO	**Operations Manager**	**LUNCH**	**Engineering**	**Preparation For Exit Meeting**	**Exit Meeting**
ESARR 3 5.2.7 5.3.2 5.3.3 5.4.2	ESARR 3 5.2.3 5.3.4 5.2.4 5.4.2 5.2.7 5.3.3	(working)	ESARR 3 5.1.3 5.3.2 5.2.3 5.3.4 5.2.4 5.4.1 5.2.7 5.4.2		

(Space Left Intentionally Blank)

APPENDIX B

EXAMPLE OF PLANNING FOR INITIAL OVERSIGHT OF A SERVICE PROVIDER OVER SEVERAL VISITS

Considering the previous example relating to an airport service provider, if we assumed that the ANSP is in the process of developing the Safety Management System, and although it is not yet complete the NSA feels that it would be appropriate to undertake an initial oversight visit to verify selected aspects of the SMS following which a series of visits would be undertaken over a period of time culminating in eventual NSA acceptance of the full SMS.

In this case the Initial Oversight is undertaken over a series of visits, with each visit verifying effective implementation of selected parts of the SMS only. Again, the matrix chart may be used to plan and record the full intended initial oversight. However there will also need to be separate matrix charts relative to each visit. For the sake of example it is assumed that the service provider has not fully implemented ESARR 3 requirements (as indicated on the first matrix chart – chart a), the first visit therefore can only focus on what has been implemented, with the subsequent matrix charts (b) and (c) identifying the samples to be taken on subsequent visits as the system is completed and following suitable periods of implementation.

Matrix Chart (a) - Partial Implementation of the SMS

Departments / areas To be audited ***ESARR 3 Requirements***	**Facility Manager**	**Tower Operations**	**ATCOs**	**External Services**	**Operations Manager**	**Engineering**
5.1 General Requirement						
5.1.1 Safety Management	x					
5.1.2 Safety Responsibility	x					
5.1.3 Safety Priority	x					x
5.1.4 Safety Objective of the ATM Service	x					
5.2 Requirements for Safety Achievement						
5.2.1 Competency	x	x				
5.2.2 Safety Management Responsibility	x	x				
5.2.3 Quantitative Safety Levels					x	x
5.2.4 *Risk Assessment and Mitigation*						
5.2.5 SMS Documentation	x					
5.2.6 *External Services*						
5.2.7 Safety Occurrences			x	x	x	x
5.3 Requirements for Safety Assurance						
5.3.1 *Safety Surveys*						
5.3.2 *Safety Monitoring*						
5.3.3 Safety Records			x		x	
5.3.4 *Risk Assessment and Mitigation Documentation*						
5.4 Requirements for Safety Promotion						
5.4.1 *Lesson Dissemination*						
5.4.2 *Safety Improvement*						

ESARR 3 requirements not addressed within the existing SMS of the service provider – requirements addressed have been implemented for a minimum of six months.

The first initial oversight visit will only verify ESARR 3 requirements that have been fully addressed in the previously identified areas of the organisation.

Matrix Chart (b) - Partial Implementation of the SMS

Departments / areas To be audited ***ESARR 3 Requirements***	**Facility Manager**	**Tower Operations**	**ATCOs**	**External Services**	**Operations Manager**	**Engineering**
5.1 General Requirement						
5.1.1 Safety Management						
5.1.2 Safety Responsibility						
5.1.3 Safety Priority						
5.1.4 Safety Objective of the ATM Service						
5.2 Requirements for Safety Achievement						
5.2.1 Competency						
5.2.2 Safety Management Responsibility						
5.2.3 Quantitative Safety Levels						
5.2.4 Risk Assessment and Mitigation		x			x	x
5.2.5 SMS Documentation						
5.2.6 ***External Services***						
5.2.7 Safety Occurrences						
5.3 Requirements for Safety Assurance						
5.3.1 Safety Surveys	x	x				
5.3.2 Safety Monitoring			x			x
5.3.3 Safety Records						
5.3.4 Risk Assessment and Mitigation Documentation					x	x
5.4 Requirements for Safety Promotion						
5.4.1 ***Lesson Dissemination***						
5.4.2 ***Safety Improvement***						

After a period of say nine months the service provider has addressed these additional requirements. They have been implemented for a minimum of six months.

5.2.6 / 5.4.1 / 5.4.2 remain outstanding.

The second initial oversight visit should now verify the additional ESARR 3 requirements that have been fully addressed. Verification should be undertaken in the previously identified areas.

Additionally the NSA may decide to re-verify requirements previously verified if nonconformities had been found or if additional confidence on consistent implementation is required.

It may also be appropriate for some previously verified requirements to be re-verified if it is considered that subsequent SMS additions may have effected the effective functioning of previously verified processes.

(Space Left Intentionally Blank)

Matrix Chart (c) - Full Implementation of the SMS

After a further period of say nine months the service provider has addressed these additional requirements. They have been implemented for a minimum of six months.

The service provider has now finally addressed all of the requirements of ESARR 3 within its SMS..

Departments / areas To be audited *ESARR 3 Requirements*	Facility Manager	Tower Operations	ATCOs	External Services	Operations Manager	Engineering
5.1 General Requirement						
5.1.1 Safety Management						
5.1.2 Safety Responsibility						
5.1.3 Safety Priority						
5.1.4 Safety Objective of the ATM Service						
5.2 Requirements for Safety Achievement						
5.2.1 Competency						
5.2.2 Safety Management Responsibility						
5.2.3 Quantitative Safety Levels						
5.2.4 Risk Assessment and Mitigation						
5.2.5 SMS Documentation						
5.2.6 **External Services**				x		
5.2.7 Safety Occurrences		x				
5.3 Requirements for Safety Assurance						
5.3.1 Safety Surveys						
5.3.2 Safety Monitoring						
5.3.3 Safety Records						
5.3.4 Risk Assessment and Mitigation Documentation						
5.4 Requirements for Safety Promotion						
5.4.1 **Lesson Dissemination**	x	x	x			x
5.4.2 **Safety Improvement**	x		x		x	x

The third initial oversight visit should now verify the additional ESARR 3 requirements that have been fully addressed. Verification should be undertaken in the previously identified areas.

Additionally the regulator may decide to re-verify requirements previously verified if nonconformities had been found or if additional confidence on consistent implementation is required.

Note: Safety Occurrences has been sampled in order to obtain information about safety incidents that may then be used to verify the lesson dissemination process

There have been a total of three visits over a period of 18 months to undertake and complete the Initial Oversight of this service provider. Each of the visits has required the NSA to verify appropriate ESARR 3 requirements in relevant areas of the organization. Due to the need to allow time for Entry meetings, lunch, preparation for Exit meetings, Exit meetings and the unavoidable duplication of effort in relation to some of the audit activities themselves the three visits combined will require more resource than a single Initial Oversight visit. NSA management needs to be aware of this and consider the desirability and necessity to undertake initial oversight in this manner. However it may often be very appropriate to adopt this approach in order to pro-actively encourage a service provider to work towards the goal of a full SMS within a reasonable and realistic timeframe. The three visit schedules providing for this Initial Oversight and using the sample of ESARR 3 requirements indicated on the previous matrix charts are as follows:

09.00 10.00 11.00 12.00 13.00 14.00 15.00 16.00 17.00 18.00

DAY 1

Entry Mtg.	**Facility Manager** ESARR 3 5.1 5.2.1 5.2.2 5.2.5	**Operations Manager** ESARR 3 5.2.3 5.2.7 5.3.3	**LUNCH** (working)	**Tower Operations** ESARR 3 5.2.1 5.2.2	**ATCO** ESARR 3 5.2.7 5.3.3	**Engineering** ESARR 3 5.1.3 5.2.3 5.2.7	**Manager resp . For provision of External Services** ESARR 3 5.2.7

DAY 2

Preparation For Exit Meeting	**Exit Meeting**

FIRST VISIT

09.00 10.00 11.00 12.00 13.00 14.00 15.00 16.00 17.00 18.00

DAY 1

Entry Mtg.	**Facility Manager** ESARR 3 5.3.1	**Operations Manager** ESARR 3 5.2.4 5.3.4	**Tower Operations** ESARR 3 5.2.4 5.3.1	**LUNCH** (working)	**ATCO** ESARR 3 5.3.2	**Engineering** ESARR 3 5.2.4 5.3.2 5.3.4	**Preparation for Exit Meeting**	**Exit Meeting**

SECONDVISIT

09.00 10.00 11.00 12.00 13.00 14.00 15.00 16.00 17.00 18.00

DAY 1

Entry Mtg.	**Facility Manager** ESARR 3 5.4.1 5.4.2	**Tower Operations** ESARR 3 5.2.7 5.4.1	**ATCO** ESARR 3 5.4.1 5.4.2	**LUNCH** (working)	**Engineering** ESARR 3 5.4.1 5.4.2	**Operations Manager** ESARR 3 5.4.2	**Mgr. resp . for Provision Of External Services** ESARR 3 5.2.6

DAY 2

Preparation For Exit Meeting	**Exit Meeting**

THIRD VISIT

(Space Left Intentionally Blank)

APPENDIX C

EXAMPLE OF PLANNING ON-GOING OVERSIGHT VISITS

Following Initial Oversight the NSA will need to develop an ongoing oversight programme that will effectively verify implementation of the full management of safety, the arrangements intended to meet the applicable safety regulatory requirements, over a two year period and preferably in different but relevant areas to those targeted during the Initial Oversight (this may be dependent upon the confidence gained in relation to particular SMS elements).

The NSA will also need to consider the need to verify the continued effectiveness of safety regulatory processes that are cross functional. The ESARR 3 lesson dissemination requirement is a good example of a process that operates through the different areas / departments of an organisation and so will need to be checked in several different areas to verify effectiveness.

The on-going oversight programme will effectively need to ensure that over a timeframe of two years, as required by ESARR 1, all applicable safety regulatory requirements are verified in all relevant areas of ATM service providers.

This will require an ongoing oversight programme to be constructed for each ATM service provider under the jurisdiction of an NSA. The totality of oversight programmes for all ATM service providers will require senior management of an NSA to carefully consider the safety regulatory audit resource requirements. It will also be necessary to ensure that safety regulatory audits are undertaken such that **risk areas** identified in individual ATM service providers from initial or ongoing oversight activities are subject to appropriate levels of future auditing (where necessary increasing the level of oversight), and that the NSAs total ongoing oversight programmes and resource levels fully take into consideration the level of confidence in individual ATM service providers such that sufficient audit resources are deployed by the NSA where there is low confidence in a particular ATM service provider.

A simple demonstration of how this can be effected in relation ONLY to ESARR 3 requirements is described.

TO NOTE THAT: in practice ALL regulatory requirements must be subject to ongoing safety regulatory oversight over a period of two years. However for simplicity only ESARR 3 is addressed in the examples provided.

Ongoing Oversight Example

The matrix chart below shows the typical relationship of ESARR 3 requirements to the various functional areas of an airport ATC.

For an Initial Oversight a sample of requirements / areas would be selected. However for Ongoing Oversight audits it will be necessary to select samples in the relevant areas of the organisation that were preferably not previously sampled during the Initial Oversight, and in addition verifying that previously sampled areas / requirements where nonconformities were identified are subject to verification (and where necessary audit close out). The examples on the following pages show how Ongoing Oversight may be effected over **four** subsequent visits, where the first visit is concerned primarily with auditing only those areas where nonconformities were found and is therefore mainly concerned with re-sampling to verify that corrective actions have been taken and that root causes have been effectively addressed.

After the four visits in the space of the two year period the process would then begin again, but working with the knowledge and confidence obtained throughout the previous two years to adapt the future oversight activities to focus on specific areas/processes where there may be less confidence or where problems have previously been revealed. Nonetheless, it is important to continue to re-verify at least some areas which have been found to be satisfactory previously in order to ensure that they continue to meet the necessary requirements.

Departments / areas To be audited ***ESARR 3 Requirements***	**Facility Manager**	**Tower Operations**	**ATCOs**	**External Services**	**Operations Manager**	**Engineering**
5.1 General Requirement						
5.1.1 Safety Management	x				x	x
5.1.2 Safety Responsibility	x	x	x	x	x	x
5.1.3 Safety Priority	x	x	x	x	x	x
5.1.4 Safety Objective of the ATM Service	x			x	x	x
5.2 Requirements for Safety Achievement						
5.2.1 Competency	x	x	x	x	x	x
5.2.2 Safety Management Responsibility	x	x	x	x	x	x
5.2.3 Quantitative Safety Levels	x			x	x	x
5.2.4 Risk Assessment and Mitigation	x			x	x	x
5.2.5 SMS Documentation	x	x	x	x	x	x
5.2.6 External Services	x			x		x
5.2.7 Safety Occurrences	x	x	x	x	x	x
5.3 Requirements for Safety Assurance						
5.3.1 Safety Surveys	x			x		x
5.3.2 Safety Monitoring	x	x	x	x	x	x
5.3.3 Safety Records	x	x	x	x	x	x
5.3.4 Risk Assessment and Mitigation Documentation	x			x	x	x
5.4 Requirements for Safety Promotion						
5.4.1 Lesson Dissemination	x	x	x	x	x	x
5.4.2 Safety Improvement	x	x	x	x	x	x

As an example the first On-going Oversight visit might be primarily concerned with the verification of effective corrective actions and audit ‘close out’ from the previous Initial Oversight.

Departments / areas To be audited ***ESARR 3 Requirements***	**Facility Manager**	**Tower Operations**	**ATCOs**	**External Services**	**Operations Manager**	**Engineering**
5.1 General Requirement						
5.1.1 Safety Management						
5.1.2 Safety Responsibility						
5.1.3 Safety Priority						
5.1.4 Safety Objective of the ATM Service						
5.2 Requirements for Safety Achievement						
5.2.1 Competency						
5.2.2 Safety Management Responsibility						
5.2.3 Quantitative Safety Levels						
5.2.4 Risk Assessment and Mitigation				[✓ x]		x
5.2.5 SMS Documentation						
5.2.6 External Services	x			[✓ x]		[✓ x]
5.2.7 Safety Occurrences						
5.3 Requirements for Safety Assurance						
5.3.1 Safety Surveys	x					
5.3.2 Safety Monitoring	[✓ x]	x		x		x
5.3.3 Safety Records						
5.3.4 Risk Assessment and Mitigation Documentation				[✓ x]		[✓ x]
5.4 Requirements for Safety Promotion						
5.4.1 Lesson Dissemination	x			[✓ x]	x	
5.4.2 Safety Improvement	x			x	x	

During the Initial Oversight non-conformities were found in these areas (mainly relating to External Service provision of Engineering functions).

The second On-going Oversight visit might focus mainly on Management functions, Safety Occurrences, Lesson Dissemination and Safety Improvement in relation to operational activities.

Corrective actions from previously identified nonconformities may be verified at separate or routine On-going Oversight visits.

Departments / areas To be audited *ESARR 3 Requirements*	Facility Manager	Tower Operations	ATCOs	External Services	Operations Manager	Engineering
5.1 General Requirement						
5.1.1 Safety Management	x				x	
5.1.2 Safety Responsibility	x				x	
5.1.3 Safety Priority	x				x	
5.1.4 Safety Objective of the ATM Service	x				x	
5.2 Requirements for Safety Achievement						
5.2.1 Competency		x			x	
5.2.2 Safety Management Responsibility		x			x	
5.2.3 Quantitative Safety Levels						
5.2.4 Risk Assessment and Mitigation						
5.2.5 SMS Documentation						
5.2.6 External Services						
5.2.7 Safety Occurrences		x	x		x	
5.3 Requirements for Safety Assurance						
5.3.1 Safety Surveys	x					
5.3.2 Safety Monitoring	x				x	
5.3.3 Safety Records	x				x	
5.3.4 Risk Assessment and Mitigation Documentation	x				x	
5.4 Requirements for Safety Promotion						
5.4.1 Lesson Dissemination	x	x	x		x	
5.4.2 Safety Improvement	x	x	x		x	

Ongoing Oversight visit number three, focusing mainly on the provision of Engineering and External services. (Previously identified non-conformities might also be verified, however for the sake of simplicity samples relating to these have not been identified on this example).

Departments / areas To be audited *ESARR 3 Requirements*	Facility Manager	Tower Operations	ATCOs	External Services	Operations Manager	Engineering
5.1 General Requirement						
5.1.1 Safety Management						x
5.1.2 Safety Responsibility				x		x
5.1.3 Safety Priority				x		x
5.1.4 Safety Objective of the ATM Service				x		x
5.2 Requirements for Safety Achievement						
5.2.1 Competency				x		x
5.2.2 Safety Management Responsibility				x		x
5.2.3 Quantitative Safety Levels				x		x
5.2.4 Risk Assessment and Mitigation				x		x
5.2.5 SMS Documentation				x		x
5.2.6 External Services	x			x		x
5.2.7 Safety Occurrences	x	x		x		x
5.3 Requirements for Safety Assurance						
5.3.1 Safety Surveys				x		x
5.3.2 Safety Monitoring				x		x
5.3.3 Safety Records				x		x
5.3.4 Risk Assessment and Mitigation Documentation				x		x
5.4 Requirements for Safety Promotion						
5.4.1 Lesson Dissemination	x			x		x
5.4.2 Safety Improvement	x			x		x

On-going Oversight visit number four, focusing mainly on Safety Surveys and Lesson Dissemination.(Again, previously identified nonconformities might also be verified, however for the sake of simplicity samples relating to these have not been identified on this example).

Departments / areas To be audited *ESARR 3 Requirements*	Facility Manager	Tower Operations	ATCOs	External Services	Operations Manager	Engineering
5.1 General Requirement						
5.1.1 Safety Management						
5.1.2 Safety Responsibility						
5.1.3 Safety Priority						
5.1.4 Safety Objective of the ATM Service						
5.2 Requirements for Safety Achievement						
5.2.1 Competency						
5.2.2 Safety Management Responsibility						
5.2.3 Quantitative Safety Levels						
5.2.4 Risk Assessment and Mitigation						
5.2.5 SMS Documentation						
5.2.6 External Services						
5.2.7 Safety Occurrences						
5.3 Requirements for Safety Assurance						
5.3.1 Safety Surveys	x			x		x
5.3.2 Safety Monitoring	x	x	x	x	x	x
5.3.3 Safety Records						
5.3.4 Risk Assessment and Mitigation Documentation						
5.4 Requirements for Safety Promotion						
5.4.1 Lesson Dissemination					x	x
5.4.2 Safety Improvement					x	x

(Space Left Intentionally Blank)

APPENDIX D

EXAMPLE AUDIT PLAN FOR INITIAL OVERSIGHT OF A LARGE SERVICE PROVIDER

ACC with around 3000 flights per day; 24 en-route sectors. Audit conducted by five auditors over three days against ESARR 3 requirements.

The ANSP provides ATM services at three locations; sites A and B are large facilities with sophisticated management support functions whilst site C is a smaller facility where there are few staff members dedicated to management functions. The ANSP also operates a number of communications and related infrastructure systems that are essential to the provision of ATM. The infrastructure services are operated and managed from a fourth location, an Infrastructure Control Centre. The Infrastructure Control Centre has responsibility for the sourcing, maintenance and operation of safety-related equipment at the organisation's other sites.

The ANSP has operated a management system of its own development for some years that has recently been amended in order to comply with the requirements of ESARR 3 although the ANSP has indicated that few changes were necessary. It is therefore expected that the organisation will have a mature safety management system. Although the service provider is required to meet a wider set of applicable safety regulatory requirements, only ESARR 3 will be detailed for the sake of illustration.

The verification plan (audit sample) developed by the audit team leader is shown in Table 1.

The verification plan seeks to verify compliance with all of the requirements of ESARR 3 within the organisation. Some of the requirements will be verified in more than one location in order to gain confidence that the appropriate processes are being applied consistently and with the intended outcomes throughout the organisation. Verification of compliance of those requirements in those areas not assessed during initial oversight will be achieved through later ongoing oversight audits. *(It is assumed for this example that the Document Review has not revealed any concerns in relation to the level of understanding of applicable regulatory requirements or the processes that the service provider has put in place designed to meet the requirements).*

Those areas selected for verification in more than one location represent the more important elements of an SMS or where the different types of operation may require different implementations of the requirements. For example, requirement 5.1.1 (Safety Management) is considered by the audit team leader to be fundamental to verifying that the organisation has a functioning SMS and will be assessed in both the simple and one of the complex ATM sites and at the Infrastructure Control Centre.

Similarly, requirements 5.1.2 (Safety Responsibility) and 5.2.1 (Competency) will be assessed at both the Infrastructure Control Centre and one of the ATM sites. This is considered appropriate in order verify that the concept of safety responsibility and competency is understood and appropriately implemented in the different disciplines.

In other areas, requirement 5.2.7 (Safety Occurrences) for example, the requirement will be assessed in both the simple and complex ATM sites in order to gain assurance that suitable processes are established in both environments.

Finally, the Infrastructure Control Centre has responsibilities for safety-related equipment at the organisation's other sites. For this reason, the audit team's efforts in verifying compliance with requirements relating to the setting of safety levels, risk assessment processes and safety management of external suppliers will be focused on this facility during the initial oversight audit.

There are four separate locations that need to be visited by the audit team, with appropriate requirements being sampled at each location

ESARR3 requirement	**ATM Site A**	**ATM Site B**	**ATM Site C**	**Infrastucture Control Centre**
5.1.1 Safety Management	X		X	X
5.1.2 Safety Responsibility		X		X
5.1.3 Safety Priority			X	
5.1.4 Safety Objective of the ATM Service	X			
5.2.1 Competency			X	X
5.2.2 Safety Management Responsibility	X			
5.2.3 Quantitative Safety Levels				X
5.2.4 Risk Assessment and Mitigation			X	X
5.2.5 SMS Documentation	X			
5.2.6 External Services				X
5.2.7 Safety Occurrences	X		X	
5.3.1 Safety Surveys		X		X
5.3.2 Safety Monitoring	X			
5.3.3 Safety Records				X
5.3.4 Risk Assessment and Mitigation Documentation		X		
5.4.1 Lesson Dissemination	X			X
5.4.2 Safety Improvement		X		X

Table 1: Verification plan (audit sample) for a large ANSP

Because of the size of the organisation and the distance between the sites that are operated by the ANSP, the audit team leader has chosen to use two teams of auditors for the site visits. The audit team consists of five auditors in total.

Team A will consist of the audit team leader and two other auditors (one with specialist knowledge of operational matters and the other with specialist knowledge of engineering matters). Team B will consist of two auditors, again one with specialist operational knowledge and the other with specialist engineering knowledge. All members of the team have good knowledge of systems and of audit techniques.

Team A			
	Day 1 (ATM Site A)	Day 2 (ATM Site A)	Day 3 (ATM Site C)
Morning 1	Introductions and Entry meeting	Operations Watch Manager Engineering Watch Manager	Introductions and Entry meeting
Coffee			
Morning 2	Unit Manager and Safety Manager	Selected members of the Unit's staff	Unit Manager
Lunch			Audit team co-ordination discussion
Afternoon 1	Safety Manager, Operations Manager and Engineering Manager	Exit meeting	Unit Manager Line engineer Line air traffic controller
Coffee			
Afternoon 2	Operations Manager and Engineering Manager	Travel to ATM Site C	Selected members of the Unit's staff
Evening	Audit team co-ordination discussion		

Team B			
	Day 1 (ATM Site B)	Day 2 (Infrastructure Control Centre)	Day 3 (Infrastructure Control Centre)
Morning 1	Introductions and Entry meeting	Travel to Infrastructure Control Centre	Operations Manager
Coffee			
Morning 2	Unit Manager and Safety Manager	Introductions and Entry meeting	Operations Manager Safety Manager
Lunch			Audit team co-ordination discussion
Afternoon 1	Safety Manager, Operations Manager and Engineering Manager	Facility Manager Operations Manager	Selected members of the Centre's staff
Coffee			
Afternoon 2	Selected members of the Unit's staff Exit meeting	Safety Manager	Exit meeing
Evening	Audit team co-ordination discussion		

Table 2 Audit timetable for a large ANSP

Having reviewed the documentation supplied by the organisation the audit team members have considered the best way in which to verify compliance with the requirements and planned for their respective parts of the audit. As an example of this detailed planning, for verifying ESARR 3 requirement 5.2.7 (Safety Occurrences) at Site A the following staff will need to be interviewed:

- ❑ Operations Manager,
- ❑ Engineering Manager,
- ❑ an ATC Watch Manager,
- ❑ an Engineering Watch Manager, and
- ❑ Members of the unit's staff selected by the auditor.

Having made an estimate of the amount of time that each interview will take in order to achieve verification of compliance, the audit team leader develops an audit timetable as shown in Table 2. Because the two teams will be working separately the timetable includes programmed opportunities for the two teams to jointly discuss their findings and to confirm the validity of statements made to the auditors, about locations that are being visited by the other team etc. Because of the distances between the organisation's sites, the audit visit schedule also includes travelling time to permit the two audit teams to travel between the sites.

It is normal practice to produce the visit schedule in advance of determining a suitable audit team, with the team leader utilising their experience to decide on the overall duration of the audit, team composition and key areas to be audited. In this example the team has been determined in advance of the visit schedule being produced. The advantage here might be to capitalise on team views before finalising the visit schedule, and this may work well where the regulator only employs a relatively small number of auditors and most teams will only comprise two auditors, however it is difficult to determine the team composition until at least a draft visit schedule has been produced by a team leader.

(Space Left Intentionally Blank)

APPENDIX E

EXAMPLE OF AN AUDIT VISIT SCHEDULE FOR AN AUDIT OF A GEOGRAPHICALLY REMOTE REGIONAL AIRPORT (TWR/APP) AND ACC

Situation:

- ❑ 20,000 movements a year for the airport
- ❑ 45,000 movements a year for the ACC
- ❑ Mixture of civil and military traffic
- ❑ 28 controllers in total

Objectives & Scope of the audit:

The objective of the audit was to obtain confidence that the facility is compliant with the ESARR 3, requirements for the reporting and investigation of safety occurrences and the national regulations based on ESARR 5 in relation to the competence and training of air traffic controllers, the reporting and investigation of safety occurrences and the low visibility procedures.

The scope of the audit related to the Airport Tower facility and an ACC located a short distance away.

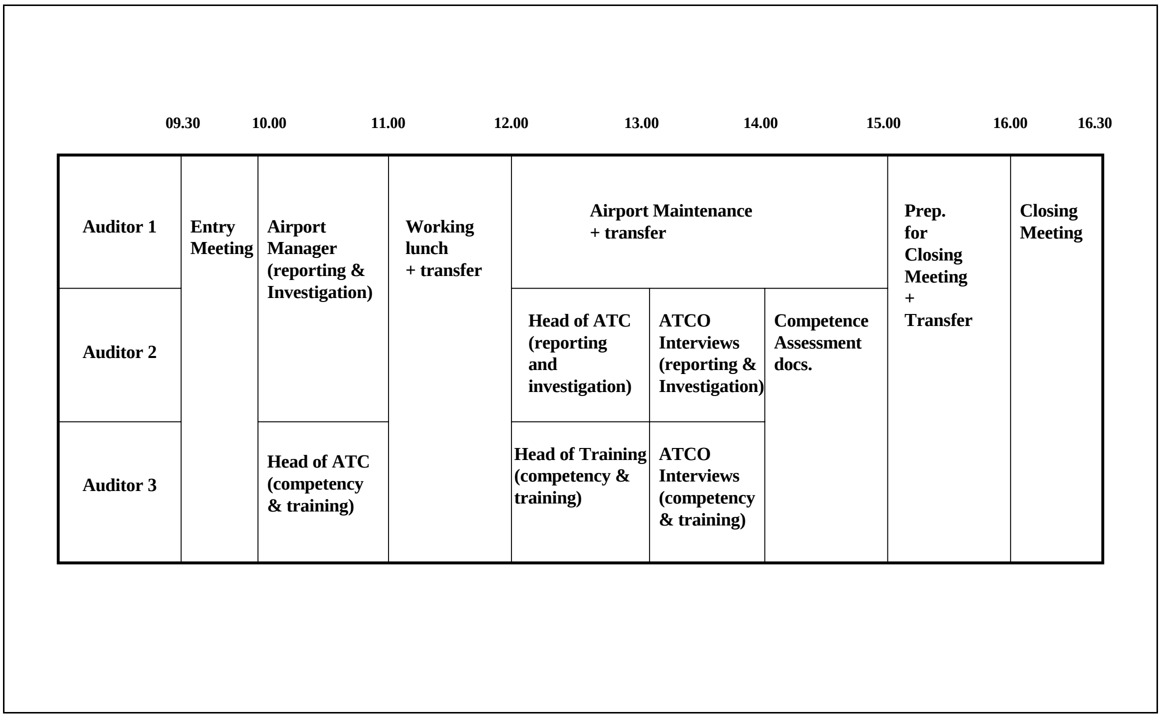
Reference Documents (Audit base):

- ❑ ESARR 3, Section 5.2.7
- ❑ ESARR 5, Sections 5.2.2.6 and 5.2.2.1.c, together with the national corresponding regulations relating to:
  - ATM Services' Personnel,
  - Air Traffic Controller Licence, Ratings and Endorsements,
  - Principles of Air Traffic Controller Refresher Training,
  - Competence Assessment Procedures and Requirements for ongoing competence for Controllers.

Audit Visit Schedule:

The visit will involve three auditors, for a one day visit. References to “transfer” in the schedule relate to the need to travel between the Tower and ACC locations.

(Space Left Intentionally Blank)



	09.30	10.00	11.00	12.00	13.00	14.00	15.00	16.00 16.30
Auditor 1	**Entry Meeting**	**Airport Manager (reporting & Investigation)**	**Working lunch + transfer**	**Airport Maintenance + transfer**			**Prep. for Closing Meeting + Transfer**	**Closing Meeting**
Auditor 2				**Head of ATC (reporting and investigation)**	**ATCO Interviews (reporting & Investigation)**	**Competence Assessment docs.**		
Auditor 3		**Head of ATC (competency & training)**		**Head of Training (competency & training)**	**ATCO Interviews (competency & training)**			

(Space Left Intentionally Blank)

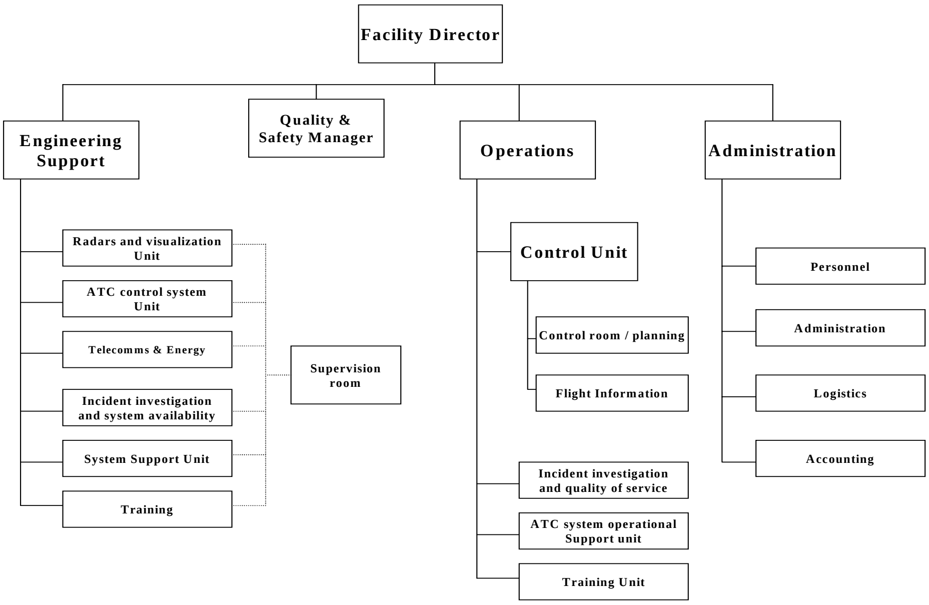
APPENDIX F

EXAMPLE OF AN AUDIT VISIT SCHEDULE FOR AN AUDIT OF A LARGER ACC

Situation:

- ❑ 750,000 movements a year
- ❑ Coordination with military activities
- ❑ 20 active control units
- ❑ Staff involved:
  - Administration department: 20 persons.
  - Operations department: 250 Controllers, 40 other staff.
  - Engineering department: 70 Technical systems supervision and configuration persons, 40 other staff.
- ❑ SMS in place for at least one year

ACC Organisation:



Objectives and Scope of the Audit:

Initial oversight of the Area Control Centre (ACC) - Operations and Engineering departments.

Reference Documents (Audit base):

- ❑ ESARR3 - All requirements except Sections 5.2.3, 5.2.4, 5.3.4, 5.2.6.

MATRIX CHART TO IDENTIFY ESARR 3 REQUIREMENTS TO BE VERIFIED IN EACH DEPARTMENT

Departments/area to be audited ESARR 3 requirements	Facility manager	Safety and quality manager	Operations department manager	Operations/ incident investigation and quality of service unit	Operations/Control Unit	Operations/control unit/ATCOs	ATC systems operational support	Operations/Training Unit	Engineering support manager	Radars and visualisation unit	ATC systems unit	Telecom and energy unit	Engineering/incidents investigation and quality of service	Engineering/ in-line supervisors	Engineering/training coordination	Administration/training coordination
5.1 General requirements																
5.1.1 Safety management	X	X	X						X							
5.1.2 Safety responsibility	X	X	X	X	X	X	X		X	X	X	X	X	X		
5.1.3 Safety priority	X	X	X	X					X				X			
5.1.4 Safety objective of the ATM service	X	X	X	X					X				X			
5.2 Requirements for Safety Achievement																
5.2.1 Competency		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
5.2.2 Safety management responsibility	X	X	X						X							

Departments/area to be audited / **ESARR 3 requirements**	**Facility manager**	**Safety and quality manager**	**Operations department manager**	**Operations/ incident investigation and quality of service unit**	**Operations/Control Unit**	**Operations/control unit/ATCOs**	**ATC systems operational support**	**Operations/Training Unit**	**Engineering support manager**	**Radars and visualisation unit**	**ATC systems unit**	**Telecom and energy unit**	**Engineering/incidents investigation and quality of service**	**Engineering/ in-line supervisors**	**Engineering/training coordination**	**Administration/training coordination**
~~***5.2.3 Quantitative safety levels***~~																
~~***5.2.4 Risk assessment and mitigation***~~																
5.2.5 SMS Documentation	X	X		X	X	X	X		X	X	X	X	X			
~~**5.2.6 External services**~~																
5.2.7 Safety occurrences	X	X	X	X	X	X	X		X	X	X	X	X	X		
5.3 Requirements for Safety Assurance																
5.3.1 Safety surveys	X	X	X	X			X		X	X	X	X	X			
5.3.2 Safety monitoring	X	X	X	X	X		X		X	X	X	X	X			
5.3.3 Safety records		X	X	X					X		X		X			
~~**5.3.4 Risk assessment and Mitigation documentation**~~																

Departments/area to be audited ESARR 3 requirements	Facility manager	Safety and quality manager	Operations department manager	Operations/ incident investigation and quality of service unit	Operations/Control Unit	Operations/control unit/ATCOs	ATC systems operational support	Operations/Training Unit	Engineering support manager	Radars and visualisation unit	ATC systems unit	Telecom and energy unit	Engineering/incidents investigation and quality of service	Engineering/ in-line supervisors	Engineering/training coordination	Administration/training coordination
5.4 Requirements for Safety promotion																
5.4.1 Lesson dissemination			X	X	X	X	X	X	X	X	X	X	X	X	X	X
5.4.2 Safety improvement	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Use of the Matrix

In order to plan the audit, it is necessary to identify the requirements relevant in each department and decide which requirements are to be verified in each department.

The matrix chart above identifies the requirements to be verified at the ACC. This matrix chart may support decisions on the audit resources needed in terms of number of auditors, technical expertise required, and number of days for the audit

Audit Visit Schedule:

Day 1		
09.00	Entry meeting	
10.00	Facility manager: 5.1 5.2.2 5.2.5 5.2.7 5.3.1 5.3.2 5.4.2	
12.00	Lunch	
13.00	Safety and quality manager: 5.1 5.2.2 5.2.5 5.2.7 5.3.1 5.3.2 5.3.3 5.4.2	
15.00	Operations/ incident investigation unit 5.1.2 5.1.3 5.1.4 5.2.1 5.2.5 5.2.7 5.3.1 5.3.2 5.3.3 5.4	Engineering / incident investigation unit 5.1.2 5.1.3 5.1.4 5.2.1 5.2.5 5.2.7 5.3.1 5.3.2 5.3.3 5.4
18.00	Close day 1	

Day 2		
09.00	Operations department manager: 5.1 5.2.1 5.2.2 5.3.1 5.3.2 5.3.3 5.4	Engineering department manager: 5.1 5.2.1 5.2.2 5.3.1 5.3.2 5.3.3 5.4
10.30	Operations/Control unit: 5.1.2 5.1.3 5.1.4 5.2.1 5.2.5 5.2.7 5.3.1 5.3.2 5.4.1 5.4.2	Engineering/ATC systems unit: 5.1.2 5.2.1 5.2.5 5.2.7 5.3.1 5.3.2 5.4.1 5.4.2
12h30	Lunch	
13.30	Visit of the control/flight information room and supervision room	
15.00	Operations/ATC systems operational support unit 5.1.2 5.2.1 5.2.5 5.2.7 5.3.1 5.3.2 5.4.1 5.4.2	Engineering/ radars and visualisation unit 5.1.2 5.2.1 5.2.5 5.2.7 5.3.1 5.3.2 5.4.1 5.4.2
17.00	Auditors meeting	
18.30	Close day 2	
10.00	Visit of the control room and supervision room 5.1.2 5.2.5 5.2.7 5.4.2	

Day 3		
7.30	Visit of the control/flight information room and supervision room	
8.30	2 ATCOs 5.1.2 5.2.1 5.2.5 5.2.7 5.4.1 5.4.2	Engineering / Telecom and Energy unit 5.1.2 5.2.1 5.2.5 5.2.7 5.3.1 5.3.2 5.4.1 5.4.2
10.00	Operations/training unit 5.2.1 5.4.1 5.4.2	Engineering/training unit 5.2.1 5.4.1 5.4.2
12.00	Lunch	
13.30	Administration/training coordination unit 5.2.1	2 supervisors 5.1.2 5.2.1 5.2.5 5.2.7 5.3.1 5.3.2 5.4.1 5.4.2
15.00	Safety and quality manager: 5.2.5 5.3.1 5.3.2 5.3.3	
16.00	Auditors meeting (preparation of exit meeting)	

Day 4	
9.00	Facility manager (audit findings presentation)
10.00	Exit meeting

(Space Left Intentionally Blank)

APPENDIX G

ADDITIONAL EXAMPLES OF TYPICAL AUDIT VISIT SCHEDULES FOR INITIAL OVERSIGHT OF AN ACC

	Topic	***Person met***
	DAY 1	
14h00 - 14h30	***Opening meeting***	
14h30 - 15h00	**Safety Policy / Priority to Safety**	**Head of ACC**
15h10 - 15h55	**SMS Documentation / SMS Structure**	**Safety Manager**
16h00 - 16h40	**Safety Responsibilities / Safety Promotion / Safety Reviews**	**Head of Operation Dept.**
16h55 - 17h35	**Safety Responsibilities / Safety Promotion / Safety Reviews**	**Head of Technical Dept.**
17h45 - 18h30	*Auditors meeting*	
	DAY 2	
9h00 - 09h45	**Incident Reporting / Operation manuals**	**Control Subdivision**
9h55 - 10h40	**Risk Assessment & Incident Reporting**	**Studies Subdivision**
10h50 - 12h15	**Incident reporting**	**Investigation Division**
12h20 - 12h50	**SMS Documentation / Safety Promotion**	**Control Room Visit**
Lunch		
14h15 - 14h55	**Risk Assessment / Incident Reporting**	**Radar Division**
15h00 - 15h30	**Risk Assessment / SMS Documentation**	**Energy Division**
15h40 - 16h15	**Risk Assessment / Safety Promotion**	**Technical Investigation Division**
16h20 - 16h55	**Incident Reporting**	**Quality of Service Division**
17h00 - 18h30	*Auditors meeting*	
	DAY 3	
9h00 - 9h30	**Operation Manuals**	**Documentation Division**
09h35 - 10h15	**Technical Incident Reporting**	**Technical Supervision Room Visit**
10h20 - 11h00	**Staff Competence / Training**	**Operation Instruction Division**
11h15 - 12h00	**Safety Culture / Incident Reporting**	**Controllers interview**
Lunch		
13h30 - 15h30	*Auditors meeting*	
15h30 - 16h30	***Closing Meeting***	

APPENDIX H

EXAMPLE OF AUDIT CHECK LIST DEVELOPMENT AND APPLICATION

An auditor will need to develop working documents to assist them to undertake an audit. These documents are an output from the detailed audit planning process and will help the auditor to undertake an effective audit.

The basic process of planning will require the auditor to produce:

- ❑ A High Level check list (if not already provided),
- ❑ An auditor's "Plan of Action" or strategy,
- ❑ A Low Level check list.

The following is an example of this process.

> ***ESARR 3 Requirement:***
>
> ***An ATM service provider shall, as an integral part of the management of the ATM service, have in place a safety management system (SMS) which:***
>
> ***5.2.7 Safety Occurrences***
>
> ***Shall ensure that ATM operational or technical occurrences which are considered to have significant safety implications are investigated immediately, and any necessary corrective action is taken.***

The High Level Check List that can be derived from this ESARR 3 requirement is:

- ❑ ***Does the ATM service provider have [as an integral part of the management of the ATM service] an SMS which ensures that ATM operational or technical occurrences which are considered to have significant safety implications are investigated immediately, and any necessary corrective action is taken?***

Or keeping this to the point without loss of meaning:

- ❑ ***Does the ATM service provider ensure that ATM operational or technical occurrences which are considered to have significant safety implications are investigated immediately, and any necessary corrective action is taken?***

The answer to this question is simply YES or NO, and it is the task of the auditor to find objective evidence that will enable the auditor to answer this question with a YES or NO. A basic principle of auditing is that UNLESS the auditor has **objective** (factual) evidence that proves this not to be the case then the answer must be yes.

The auditor must ensure that he/she looks for such evidence in the appropriate part of the organisation and with the appropriate people.

(Space Left Intentionally Blank)

However, as an example, an ATM service provider may declare in its SMS that the approach taken to meet this ESARR 3 requirement is as follows:

> ***Extract from SMS Manual:***
>
> ***Air navigation system operational or technical occurrences that are considered to have significant safety implications should be investigated immediately and any necessary corrective action taken.***
>
> ***The incident investigator will maintain an incident reporting system that must be used by all staff who become aware of a safety related incident.***
>
> ***Corrective and / or preventive actions resulting from the incident investigation will be logged in the incident reporting system and tracked by the Safety Incident Investigator.***
>
> ***The SMS Manager will monitor the incident reporting system and ensure that any corrective actions implemented are subject to formal verification for effectiveness.***

The auditor will apply the same technique and turn these statements (internal organisational requirements) into additional high level check List questions and ADD them to the question(s) derived from ESARR 3 as follows:

Does the ATM service provider ensure that ATM operational or technical occurrences which are considered to have significant safety implications are investigated immediately, and any necessary corrective action is taken?

- Are air navigation system operational or technical occurrences that are considered to have significant safety implications investigated immediately and any necessary corrective action taken?
- Does the incident investigator maintain an incident reporting system?
- Is the [incident reporting] system used by all staff who become aware of a safety related incident?
- Are corrective and / or preventive actions resulting from the incident investigation logged in the incident reporting system?
- Are they tracked by the Safety Incident Investigator?
- Does the SMS Manager monitor the incident reporting system?
- Does the SMS Manager ensure that any corrective actions implemented are subject to formal verification for effectiveness?

These questions have now effectively become the auditor's personal audit objectives, and the audit task is therefore to verify that all of the above are happening, or not as the case may be. It is the auditor that must answer these questions after conducting sufficient audit investigations. These questions are **not asked** of those being audited (the answers would always inevitably be Yes!!!)

This high level check list will be used during the audit to act as a constant reminder of what the auditor should be verifying, and will enable the auditor to maintain a record of progress. Use of this check list helps to maintain objectivity throughout the audit process.

Upon completion of the audit this high level check list together with the answers YES or NO will provide a formal record of what the auditor intended to verify and what the audit actually revealed. Additionally the auditors notes will provide a record of what was examined together with answers provided by the audited personnel.

The high level check list has identified what the auditor must verify, the auditor now needs to determine a suitable strategy or "Plan of Action" that will enable the auditor to obtain the necessary **objective evidence** to be able to answer these questions simply with a YES or NO. The auditor will need to think about the specific locations where such evidence is likely to be available and key staff that will need to be interviewed and how can provide access to the necessary evidence.

By examining the High Level check list the following key staff are identified:

- ❑ Incident Investigator,
- ❑ Staff (ATCOs and Engineering support staff),
- ❑ SMS Manager.

The auditor's plan of action therefore might be to trace the reporting, subsequent investigation, associated corrective action and verification of a number of significant incidents.

This might require the auditor to begin the audit with ATCOs and Engineering support staff to examine the process that they follow when an incident has occurred, and then to follow this process for some specific incidents working with the Incident Investigator and then the SMS Manager. Finally the auditor may wish to check that the resultant corrective action and verification took place and may also wish to re-verify some specific corrective actions to establish that root causes are being addressed by the corrective actions taken. This may require the auditor to work with key managers and staff in relevant departments.

A logical sequence and timings therefore might be:

- ❑ ATCOs (30 minutes)
- ❑ Engineering support staff (30 minutes)
- ❑ Incident Investigator (45 minutes)
- ❑ SMS Manager (45 minutes)
- ❑ Managers / staff in Operations (30 minutes)
- ❑ **Total 3 hours**

It is not possible to be totally accurate with this plan of action and a degree of flexibility will always need to be maintained as audit information is revealed. However by thinking in advance the auditor is far more likely to not only be able to quickly access the necessary objective evidence, but will also be able to retain control of the audit rather than being led by the auditees.

The plan of action will need to be supported with a Low Level check list of specific documents, records etc. that need to be examined by the auditor and some specific questions that will need to be asked of managers and staff to obtain information and access to evidence. Throughout the on-site audit the Low Level check list will act in support of the audit process and will remind the auditor of all of the samples and questions that the auditor identified whilst planning the audit.

(Space Left Intentionally Blank)

A possible Low Level check list for the previous plan of action might be as follows:

ATCOs (30 minutes)

- Talk with one ATCO who has just come off duty.
- Could you please explain what actions you take when a significant safety incident has occurred?
- How do you determine what is significant?
- Do you maintain some form of record of incidents?
- Is it possible to see this record?
- Take a sample of two incidents that occurred three and six months ago (examining the record provides the auditor with some examples which may be tracked though the Incident Investigator and SMS Manager)

Engineering Support Staff (30 minutes)

- Repeat the above.

Incident Investigator (45 minutes)

- Could you please describe the process of investigating incidents?
- Are some incidents regarded as more significant than others?
- How is significance determined and by whom?
- How long do incident investigations typically take?
- Are there any time requirements that must be met for incident investigations?
- Who needs to be involved with investigations and how do you ensure the right people are involved?
- Is it possible that I can view the investigation reports that were produced in response to the following incidents (those previously identified with ATCO and Engineering support staff).
- May I see the minutes of the meetings that were held to discuss the corrective actions in response to these incidents?
- (Examine data in files and look closely at process followed to see how long they took, who was involved and what the investigations revealed).
- How is corrective action determined?
- In relation to incidents viewed identify the specific corrective actions, who was involved and the actions recommended / taken?

SMS Manager (45 minutes)

(Working with previously identified incidents and associated corrective actions)

- Could you please explain the process that you follow when tracking incidents and associated corrective actions?
- Are other staff sometimes involved with this process?
- What records are maintained?
- Is it possible to see the records for the following incidents (view records relating to previous sample of operational and engineering incidents)?
- How do you verify that the corrective action is taken?

- Is it possible that I can see the records relating to the corrective action taken in response to these sample incidents?
- (View the records and look for evidence of specific actions taken to verify that corrective action was taken).

Managers / Staff in Operations and Engineering Support (30 minutes)

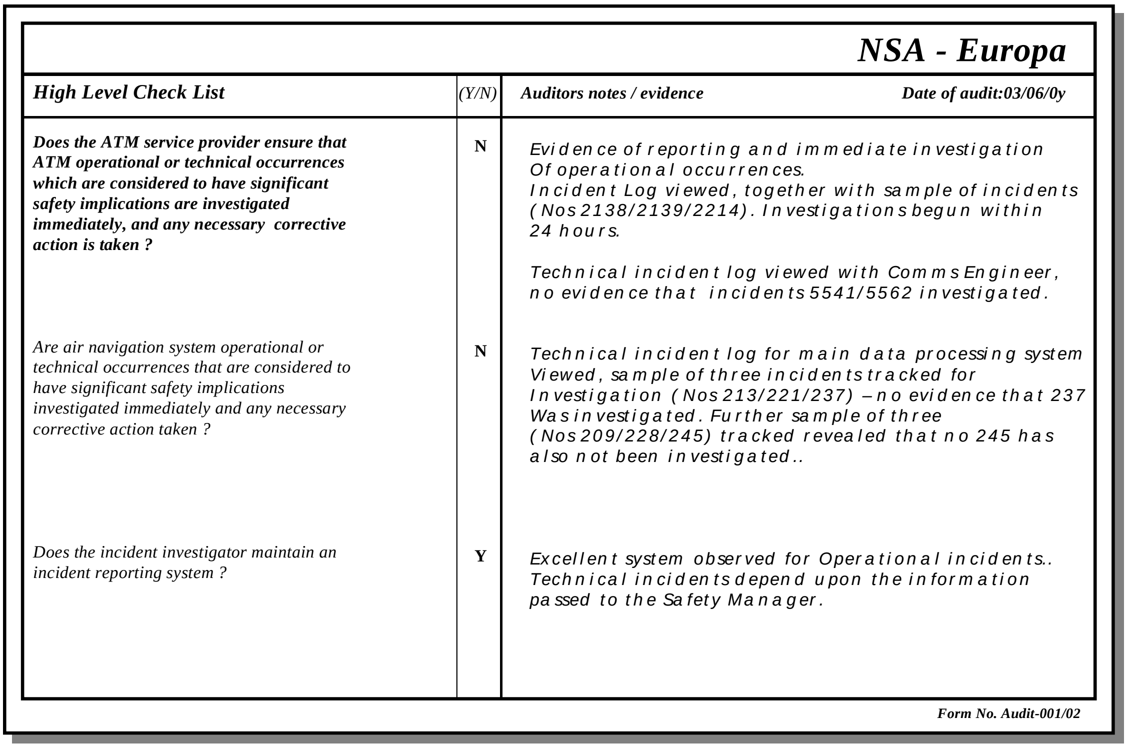
- In relation to the sample incidents, verify that the managers and staff in both operational and engineering support are aware of them and have some records demonstrating that they discussed and determined corrective action.
- Re-verify the action taken (to confirm that the corrective action was effective and to confirm the findings of the SMS Manager who has previously undertaken verification).

(Space Left Intentionally Blank)

APPENDIX I

EXAMPLES OF AUDIT FORMS

Example of a typical form used to record the High Level check list and auditors notes.



NSA - Europa

High Level Check List	*(Y/N)*	***Auditors notes / evidence*** ***Date of audit:03/06/0y***
Does the ATM service provider ensure that ATM operational or technical occurrences which are considered to have significant safety implications are investigated immediately, and any necessary corrective action is taken ?	**N**	*Evidence of reporting and immediate investigation Of operational occurrences. Incident Log viewed, together with sample of incidents (Nos 2138/2139/2214). Investigations begun within 24 hours. Technical incident log viewed with Comms Engineer, no evidence that incidents 5541/5562 investigated.*
Are air navigation system operational or technical occurrences that are considered to have significant safety implications investigated immediately and any necessary corrective action taken ?	**N**	*Technical incident log for main data processing system Viewed, sample of three incidents tracked for Investigation (Nos 213/221/237) – no evidence that 237 Was investigated. Further sample of three (Nos 209/228/245) tracked revealed that no 245 has also not been investigated..*
Does the incident investigator maintain an incident reporting system ?	**Y**	*Excellent system observed for Operational incidents.. Technical incidents depend upon the information passed to the Safety Manager.*

Form No. Audit-001/02

(Space Left Intentionally Blank)

APPENDIX J

MINIMUM CRITERIA RECOMMENDED FOR TRAINING IN RELATION TO SAFETY REGULATORY AUDITING

In order to implement the ESARR 1 requirements as regards the training and qualification of auditors, an NSA should recognise specific training courses as acceptable means to train its auditors and the auditors from recognised organisations who conduct audits on behalf of the NSA.

Such recognition should only take place after the NSA is satisfied that a training programme meets criteria previously defined by the NSA in order to meet the minimum requirements established in ESARR 1.

The criteria included in this appendix is considered by the Safety Regulation Commission as a recommended means to meet those requirements, and therefore provide a harmonised basis for its use by NSAs in the EUROCONTROL Member States.

General Principles

Intended safety regulatory auditors should receive initial training designed to provide them with the necessary knowledge and skills to be able to begin the process of personal competency development in relation to safety regulatory auditing. This should be supported by personal competency development activities following which there should be an evaluation of the competence acquired.

It is recognised that attendance at a single training course alone is unlikely to be sufficient in itself to fully develop the competence of an auditor. Consequently, a training approach is necessary to provide at least a minimum acceptable level of competence and provide the auditor with a firm foundation for further competency development.

This should as a minimum involve a three stage approach involving:

i) Initial training to provide a minimum basic level of auditor knowledge and skills.

ii) Exposure to audit processes in order to reinforce the initial training and to provide an opportunity for personal competency development.

iii) Follow up training to verify the effectiveness of the initial training and the adequacy of initial auditor competency and review the results of his/her exposure to real audit processes, together with training reinforcement and supportive auditor techniques training.

Formal examination should be used at the end of these three stages to verify knowledge acquired in relation to auditing activities and best practices to be adopted.

Ongoing competency development will then enable auditors to conduct safety regulatory audits in a fully effective manner, coupled with periodic evaluation of competency.

The overall objectives of a safety regulatory auditor training programme should therefore aim to provide intended safety regulatory auditors with sufficient understanding of the basic principles of auditing to enable them to undertake in depth and searching auditing of ATM service providers as an integral part of the safety oversight process activities.

Audit Training Programme

These objectives could be met by delegates attending as a minimum an initial auditing techniques training course specifically focused on the auditing of ATM safety management systems, following which they will be required to undertake training audits in a working ATM service provider before returning to the training environment for their results to be reviewed and to receive additional training in auditing techniques.

A suitable minimum format for this training is as described as follows:

a) **STAGE 1 - Initial training in auditing techniques. The training objectives should aim to provide students with:**

- ❑ An understanding of the difference between initial and on-going oversight audits and their application in relation to the assurance of conformity of ATM organisations with applicable safety regulatory requirements.
- ❑ The confidence and ability to plan, conduct and report an initial oversight audit of an ATM organisation for compliance with applicable safety regulatory requirements.
- ❑ The ability to plan, undertake and report an audit of a specified operational aspect of an ATM organisation.
- ❑ An understanding of the audit corrective action and close out process.
- ❑ An understanding of how to plan ongoing audit activities working with previous initial and on-going oversight audit results and risk analysis data.
- ❑ An ability to verify that safety management system processes are effective in achieving regulatory objectives.

It is considered that these points would require a minimum of 35 hours of formal tuition.

b) **STAGE 2 - Practical field training auditing activities in an ATM environment should provide students with:**

- ❑ An opportunity to apply their audit knowledge and skills in practical working environments.
- ❑ Experience to be presented and reviewed in the subsequent follow up training

Options for this practical stage may include the conduct or participation in audits of ATM service providers, audits of own organisation or audits conducted in another State.

c) **STAGE 3 - Follow up training should aim to provide students with:**

- ❑ Confirmation that they have understood and been able to apply in practice the knowledge and skills acquired on the initial training course.
- ❑ Sharing of experiences relating to audit situations.
- ❑ Additional audit techniques training aimed at competency development.

It is considered that these points would require a minimum of 18 hours of formal tuition.

These high level objectives should be broken down into a combination of knowledge and skills that need to be acquired throughout the course, and for which delegates will be **formally assessed at the end of the complete three stage training** programme by means of a **formal examination**.

Knowledge & Skills

Intended safety regulatory auditors should leave the training programme with a good understanding of the following:

- The purpose of auditing.
- Application of auditing in relation to initial oversight of an organisation.
- Application of auditing in relation to on-going oversight.
- The relative responsibilities of auditors, auditees and the audit client.
- How to plan, manage and report regulatory oversight audits.
- Team auditing.
- Responsibilities of audit team leaders.
- How to document audit findings.
- Auditing as a positive approach to continuous improvement.
- Auditing as a means of verifying process effectiveness.

They should leave the training programme with the following skills:

- The ability to plan, undertake and report a full initial oversight of an ATM organisation against defined regulatory criteria.
- The ability to lead and coordinate an oversight team.
- The ability to conduct necessary pre-audit communications and oversight entry / exit meetings with auditee management.
- The ability to plan an audit of selected aspects of an ATM operation either as a stand alone audit forming part of an on going regulatory oversight activity, or as an integral part of an initial oversight of an ATM operation.
- The ability to plan an audit that will verify the effectiveness of a safety management system process.
- The ability to report audit findings objectively and to base conclusions on factual data.
- The ability to quantify the level of risk attached to an ATM operation and, hence, determine the level and frequency of future oversight activities.

More specifically, the contents of the initial training (Stage 1) should cover as a minimum:

- ATM Safety Regulation in Europe
- Basic principles of auditing
- Auditing as an approach to safety oversight
- An overview of the general oversight process
- Document Review
- Initial oversight planning
- Audit planning

- Audit team meetings
- Audit protocol
- Detailed check lists
- Searching for evidence
- Entry / Exit meetings
- Recording audit findings
- Evaluating and presenting audit results
- Report writing
- Corrective action and audit close out
- Verification audits
- Planning on-going oversight
- Future audit programming based on risk

The practical field training audits (Stage 2) should be based on:

- One or more practical audits conducted according to recommendations and techniques presented during Stage 1.

The contents of the follow-up training (Stage 3) should cover as a minimum:

- Review of results of Stage 2
- Lessons learned and difficulties encountered
- Audit planning overview
- Additional audit techniques
- Process management and auditing
- Process based management systems
- Auditing using the ‘Process Approach’ principle.
- Internal audits / surveys.

**** End of Document ****