# ATM Safety Management
# Interface between ANSP and NAA/NSA

## Study and Selection of Good Practices

EUROCONTROL

# DOCUMENT CHARACTERISTICS

| TITLE |
|---|

## ATM SAFETY MANAGEMENT INTERFACE BETWEEN ANSP AND NAA/NSA - STUDY AND SELECTION OF GOOD PRACTICES

| Document identifier | Edition number: | 1.0 |
|---|---|---|
| | Edition date: | 28.02.2011 |


**ABSTRACT**

This report is the result of bilateral interviews with ANSPs as well as NSAs and attempts to meet three objectives. The first is to paint a picture of the current situation at the safety interface between ANSP and NSA, the second is to collect a series of practices which have been put in place while the third is to identify what practices would improve where necessary the interface and promote a more mature relationship which and could thereby improve the effectiveness and efficiency of the ANSP/NSA interface processes.



| KEYWORDS | | | |
|---|---|---|---|
| ANSP | NSA | NAA | SMS |
| Oversight | QMS | Reporting | Interface |
| Competency | Regulatory requirements | Investigation | Safety |
| Safety assessment | | | |



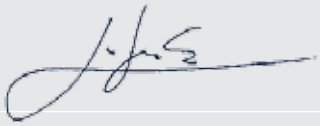
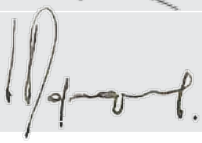
| CONTACT PERSON(S) | TEL. | UNIT |
|---|---|---|
| Ivana Bušić | +32 2 729 4632 | DNM/COO/NOM/SAF |


| STATUS, AUDIENCE AND ACCESSIBILITY | | | | | |
|---|---|---|---|---|---|
| **STATUS** | | **INTENDED FOR** | | **ACCESSIBLE VIA** | |
| Working Draft | ☐ | General Public | ■ | Intranet | ☐ |
| Draft | ☐ | CND Stakeholders | ☐ | Extranet | ☐ |
| Proposed Issue | ☐ | Restricted Audience | ☐ | Internet (www.eurocontrol.int) | ■ |
| Released Issue | ■ | Electronic copies of this document can be downloaded from: www.eurocontrol.int | | | |

# DOCUMENT APPROVAL

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

| | AUTHORS | DATE |
|---|---|---|
| Lead author & Project Manager | Ivana Bušić  | 28-02-2011 |
| Co-author | Anthony F. Seychell  | 28-02-2011 |

| AUTHORITY | NAME AND SIGNATURE | DATE |
|---|---|---|
| Safety Team Chairman | Hans-Jürgen Morscheck  | 14-03-2011 |
| SRC Chairman | Harry Daly  | 14-03-2011 |
| Head of Safety Unit | Antonio Licu  | 14-03-2011 |
| Head of Oversight Division | Juan Vázquez-Sanz  | 14-03-2011 |
| Head of Network Operations Management | Nicola Cooper  | 14-03-2011 |
| Chief Operating Officer DNM | Joe Sultana  | 14-03-2011 |
| Director Network Management | Jacques Dopagne  | 15-03-2011 |

# DOCUMENT CHANGE RECORD

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

| EDITION NUMBER | EDITION NAME | REASON FOR CHANGE | PAGES AFFECTED |
|---|---|---|---|
| 0.0 | 03/05/2010 | Document creation | All |
| 0.1 | 17/05/2010 | First issue for internal review | All |
| 0.2 | 16/06/2010 | Draft for review ST and SRC (Part 1) | Pages 7-10, 41, 46 |
| 0.3 | 09/02/2011 | Add Part 2, Format change, Proposed issue for review ST and SRC | All |
| 1.0 | 28/02/2011 | Released issue | 59-61, 70 |


## PUBLICATIONS

EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

**Tel:** +32 (0)2 729 11 52
**Fax:** +32 (0)2 729 51 49
**E-mail:** publications@eurocontrol.int

# CONTENTS

# FOREWORD

As an ANSP, our prime objective is to run our operations as safe and as effectively as possible, in the interest of our customers, i.e. the airlines in general and their passengers more specifically. In order to do that, we need to build up good communication within our own organisation, as well as with fellow ANSPs, and of course with our national supervisory authorities.

I remember a few years ago vivid discussions with my colleagues from the Safety Team on how these relationships with our NSAs were evolving. I was surprised to hear how many differences there were in the way ANSPs and NSAs were dealing with each other, the latter in spite of Pan-European wide accepted safety regulations, and well known practices on safety management. The level of detail and frequency of safety audits for example varied significantly from one country to the other. Notification, assessment and oversight of changes were also showing huge differences from one country to the other. The relationship itself between an ANSP and its NSA was either very structured, or was found to be very loose.

What was the optimum in all of this? Was there a way to make these relationships more effective, more mature, and by doing so increasing the performance of our operations even more in terms of safety, cost and efficiency?

Therefore the Safety Team asked the Agency to study the current practices on the interface between ANSP and NSA and to check if in certain cases excellent practices could be found, ready to disseminate more widely.

The result of this work is in this report in front of you. The contents are a reflection of the openness of the ANSPs to share in detail their experiences, and I am very thankful to my colleagues NSAs for having done the very same. On behalf of the Safety Team, I strongly support the recommendations in this report, and I do believe that the best practices that have been identified will help us tremendously in performing safer and anticipating faster, together with our NSAs, all the changes that our industry is facing.

**Hans-Jürgen MORSCHECK**
***Acting Chairman of the EUROCONTROL Safety Team***

The delivery of the highest possible levels of safety for end users of the European Air Traffic Management (ATM) network is a prime concern and ambition of all stakeholders in the European aviation sector.

To remain relevant and effective, the ATM sector must be agile in its legislative, rule-making, service provision and regulatory oversight operations and proactive in all its work to manage risk to the safety of the end user.

The formulation of and compliance with clear, pragmatic, proportionate and risk based rules for ATM from a single source are essential components to securing highest possible safety standards. However, to maximise the effectiveness of those rules, they must exist within a complimentary environment and process of partnership and cooperation to deliver the positive outcomes intended by the rules and demanded by the end-user.

That atmosphere of cooperation must have embedded attributes, which are inherent in all the activities of all actors and include: consistency, clarity of purpose and accountability, an acceptance of each actors' roles and responsibility, sufficient resources, mutual trust and confidence and a shared belief in the objectives to deliver positive outcomes.

The EUROCONTROL Safety Regulation Commission and Safety Team have worked in equal partnership and with a common purpose and ambition to create this document. It is commended to you as a catalyst towards securing an atmosphere of mutual cooperation between all European ANSPs and Regulatory Oversight agencies. It seeks to present and offer mechanisms, tools and approaches to encourage continual improvement in developing and securing the positive relationship between ANSPs and Regulatory oversight actors essential to maximise mutual benefits and deliver enduring positive outcomes for the safety of European air travellers.

**Harry DALY**
***Chairman of the EUROCONTROL Safety Regulation Commission***

# EXECUTIVE SUMMARY

Over the last ten years, both ANSPs and NSAs have made significant progress in implementing a systematic safety framework. Whilst ANSPs have applied safety management systems in accordance with ESARR 3 and Commission Regulation (EC) No 2096/2005, NSAs have been guided by ESARR 1 and Commission Regulation (EC) No 1315/2007 to implement their own requirements as to provide structured safety oversight.

In order to ensure a dialogue on the above, ANSPs and NSAs have over the years been developing working arrangements at national and local level. These working arrangements vary from one state to another. It is important therefore to identify those practices on the interface between ANSP and NSA which can be regarded as most successful in the interest of air navigation services that are managed with high standards of safety but at the same time also meeting the demands of efficiency, capacity and cost. These practices can then be disseminated with the aim to be shared and possibly be applied Europe-wide by the ANSP and NSA community. Finally, such best practices will be important in the establishment of an effective safety interface between the ANSP and the NSA in a FAB context.

This report attempts to meet three objectives. The first is to paint a picture of the current situation at the safety interface between ANSP and NSA, the second is to collect a series of practices which have been put in place while the third is to identify those practices which would improve where necessary the interface and promote a more mature relationship.

Part I of this report is the result of bilateral interviews with both ANSPs and NSAs. Fourteen states have participated and their results provide a mix of small versus large states, low versus high traffic, as well as different locations and business cultures in Europe. In addition, Maastricht UAC also took part in the study.

The activity looked into following five areas considering the roles and responsibilities as well as the current practices of each.

1. The type of interaction between ANSP and NSA (e.g. joint formal bodies, focal points established, coordination where required, etc.);
2. Existing practices and processes in auditing (e.g. frequency, level of detail, coordination on preparation, conducting and follow-up actions);
3. Interaction between national stakeholders (AAIB, NSA, NAA, ANSP) and arrangements/processes for occurrence reporting and investigation (understanding of roles/responsibilities, what is to be notified and to whom, on severities, feedback, oversight of respective SMS processes);
4. Processes for notification, acceptance and oversight of changes with potential impact on safety (understanding of requirements, roles and responsibilities, level of regulatory involvement in the process, etc);
5. Level of involvement of the NSA in ATCO and ATSEP competency (processes and arrangements).

Institutional arrangements vary significantly, but functional separation between ANSP and NSA has been achieved in all states which participated in this study. NSAs, sometimes understaffed, have been looking at various ways to increase their level of competency. Sharing of staff between states, or seconding ATM safety experts from ANSP to NSA, under controlled conditions, are some of the solutions found.

Most ANSP and NSA interviewees have developed ways of meeting each other in a structured way. This is done via formal and regular meetings, or via focal points. The implementation of a quality management system by both the NSA and the ANSP has also been reported as a way to process the relationship between them. In some cases formal manuals are available on how such dialogue is managed. Safety may be the sole point on the agenda, but other regulatory matters (e.g. economic regulation, civil-military coordination, etc.) may also be discussed in combination with safety or in the interest of safety.

Safety oversight is mostly conducted through audits, although complementary methods exist. The way in which audits are conducted varies, but most follow an agreed annual or multi-annual structured and transparent plan. The NSAs which were interviewed felt that there should be greater harmonisation between NSA processes leading to alignment of the certification

process of ANSPs. This was considered especially important in the FAB context. The interviewees were also of the opinion that the principle of oversight should be to measure the effectiveness of regulation rather than its existence.

The way in which mandatory occurrence reporting is organised varies between Member States. Although every state has a reporting flow from ANSP to NSA (in various formats), the process for follow-up differs. Some NSAs do their own incident investigation while others only check that the ANSP has an adequate process in place to carry out internal investigations. Some NSAs check whether the ANSPs follow up the corrective actions to prevent recurrence of incidents.

All states which participated in this data gathering exercise apply Commission Regulation (EC) No. 1315/2007 on safety assessment but there is a wide degree of interpretation on how to meet its requirements. This is reflected in the processes addressing changes, and specifically the notification of changes. Additionally, the level of documentation which is required by the NSA from the ANSP varies. In some cases, the NSA is involved (sometimes actively in a coordinating role) together with the ANSP from the beginning of the project, particularly in the case of large changes. Checklists are in use, as are various methods of notification and follow-up procedures (some of them highly automated).

Competence assessment of ATCOs is one of the areas with the least variation between states and does not seem to cause many difficulties. Various ATCO competency assessment schemes are in place in ANSPs, which must surely have an impact on the oversight of FABs. The situation with respect to ATSEPs is different, because there is no harmonised interpretation of the requirement.

FABs have to be in place and operating by the end of 2012. However, lots of work still needs to be done. The progress on how to implement safety oversight varies from FAB to FAB.

Apart from the above practices, a number of which are highly mature, general considerations and areas for improvement were flagged up during the interviews.

It is not straight-forward to propose one-size-fits-all solutions because each state has its own local considerations. Bearing these constraints in mind Part II of the report describes the approach which has been followed to come up with fit-for-purpose solutions. The results shown can be implemented with varying degrees of ease as well as create overall awareness.

A group of subject matter experts from ANSPs and NSAs met to analyse and refine, where necessary, the observed practices. A number were selected and then ranked according to a classification scheme consisting of two main criteria: significance and ease of application.

It is expected that the highest ranked practices can be applied by the Europe-wide ATM community to increase the maturity and effectiveness of the respective ANSP/NSA interface, either in the national context or in the future FAB environments.

# INTRODUCTION

## 1.1 Background

Over the last ten years both ANSPs and NSAs have worked on a systematic implementation of a safety framework. The legal framework for service providers has been a safety management system in accordance with ESARR 3 (as transposed into national legislation) and the Commission Regulation on common requirements for ANSPs. NSAs on the other hand have been guided by ESARR 1 and Commission Regulation (EC) No 1315/2007 to implement their own requirements for a systematic and structured safety oversight function.

Harmonised approaches and best practices for SMS implementation for ANSPs have been developed by appropriate communication between ANSPs. The latter has been achieved with the help of organisations such as EUROCONTROL and CANSO. As far as the former is concerned, the EUROCONTROL Safety Team has been the main consultation body making this harmonisation happen.

In a similar way, NSAs have been harmonising their approaches to safety oversight via the EUROCONTROL Safety Regulation Commission.

Whilst the above working arrangements have been successful in achieving good coordination within groups of stakeholders, it has been observed and reported that the national working arrangement between NSA and ANSP varies from one state to another. It is to be expected that within a state the way in which the ANSP and the NSA interface with one another will be the result of a long development process, and will depend on various factors such as culture, size of organisation, extent of resources and competencies, views of people and the way in which legislation/regulations is/are being interpreted. On the other hand, it is to be expected that certain national interfaces will have developed into a more successful and more efficient relationship than others.

It is therefore important to analyse whether best practices on the interface between ANSP and NSA exist, and if so, whether they can be disseminated for application to the Europe-wide ANSP and NSA community.

Successful dissemination of best practices will be important for a pragmatic and effective safety interface between the regulator and service provider, not only at national level but even more so within the future FAB context.

The above matter has been raised at meetings of the Safety Team, the Safety Regulation Commission, and during their joint sessions. These groups have recommended that the matter should be investigated in more detail and to report back with the results.

The report lists in Part I all the observed practices and in Part II highlights the good practices which can be implemented and hopefully lead to success stories for good working arrangements between ANSP and NSA.

## 1.2 Objectives

The objectives of the project on the interface between ANSP and NAA/NSA are:

- to have a picture of the present situation;
- to collect a series of practices which have been put in place;
- to identify those practices which would improve the interface and promote a more mature relationship between ANSPs and NSAs.

This report is presented in two parts where Part I addresses the first two points above while Part II looks into the third one.

## 1.3 Structure of the Report

### 1.3.1 Part I

Part I is the result of a series of interviews with ANSPs and NSAs, where they explained how the interface functions in their respective environment.

The various factors influencing the interface can be clustered around the eight headings mentioned below:

- Institutional arrangements (Organisation & NSA staffing);
- Roles and responsibilities;
- Relationship ANSP/NSA;
- Safety oversight audits;
- Management of occurrence reporting and investigation;
- Safety assessment of safety-related changes;

- Competence assessment;
- Functional Airspace Blocks (FABs).

The details of the report therefore are structured around the above sections.

Part I focuses mainly on the current situation. The sections expounding on the headings above are divided into two parts:

1. an introduction on the topic and a generic part which contains a collection of similar practices in use;

2. a number of examples where these were considered to provide additional information which was not included in the first part of the section.

Another chapter summarises the various considerations raised by the participants during the interviews.

N.B. Geography, culture and size have a direct impact on the interface and the practices adopted in the various countries. This has to be taken into account when considering any of these examples for local application.

### 1.3.2 Part II

This part of the report describes the work of a group of subject matter experts from ANSPs and NSAs who met to analyse and refine, where necessary, the observed practices shown in Part I. A number were selected and then ranked according to a classification scheme consisting of two main criteria: significance and ease of application.

Part II therefore consists of a number of good practices[1] which, when applied European-wide, could enhance the interface between ANSP and NSA. These can be implemented with varying degrees of ease as well as create overall awareness.

1 Best practices are to be understood to signify practices which are appropriate for application within a particular organisation, given its specific business culture, size etc. This means that a practice which works well within one organisation might be less successful in another, if the latter has a significantly different business context, size, culture etc. One size may not fit all. Therefore the selection of practices will be subject to this type of reflection.

## 1.4 Acknowledgements

This work was possible only thanks to the contributions of a large number of people in both ANSPs and NSAs. Without their open and honest input, it would not have been possible to obtain the necessary information.

EUROCONTROL wishes to express its appreciation for the support and assistance provided.

Appendices 1 and 2 to this report lists these persons and their organisations.

# PART I

# INVENTORY OF EXISTING PRACTICES IN INTERFACE BETWEEN ANSP AND NAA/NSA

# CHAPTER 1 – INTRODUCTION

The information-gathering exercise was conducted mainly by means of bilateral interviews. The exercise had been proposed to both ANSPs and NSAs with the aim of collecting a series of best practices established to deal with the various elements of safety oversight activities.

The interviews focused on:

- existing arrangements and interaction processes between NSA and ANSP;
- strengths and weaknesses of the existing institutional arrangements and processes;
- the evolution of the processes and any lessons learned.

A number of ANSPs and NSAs provided verbal/written input when it was not possible to hold meetings.

Care was taken to ensure that the interviewees included representatives from different types of ANSPs and NSAs (e.g. small vs. large, high- vs. low-density traffic, different geographical locations). Fourteen states volunteered to provide their input to this study. All participating ANSPs operate one or more ACCs, besides providing APP and TWR services.

In addition, Maastricht UAC also took part in the study and the information gathered from this very unique ANSP is considered to be highly significant for the future FABs' arrangements.

With the project objective in mind, the interviews looked in detail at the following:

- type of interaction in place between ANSP and NSA (e.g. joint formal bodies, focal points established, coordination when required, etc.);
- existing auditing practices and processes (e.g. frequency, level of detail, coordination on preparation, conducting and follow-up actions);
- interaction between national stakeholders (AAIB, NSA, NAA, ANSP) and arrangements/processes for occurrence reporting and investigation (understanding of roles/responsibilities, what is to be notified and to whom, on severities, feedback, oversight of respective SMS processes);
- processes for notification, acceptance and oversight of changes (understanding of requirements, roles and responsibilities, level of regulatory involvement in the process, etc.);
- level of involvement of NSA in ATCO and ATSEP competency (processes and arrangements).

# CHAPTER 2 – CURRENT SITUATION

## 2.1 Institutional Arrangements

### 2.1.1 Organisation

Several forms of institutional arrangements are in place, but all of them reflect the SES requirement of separation between regulator and service provider. Some states have opted for functional separation while others have established institutional separation, which takes several forms.

It was observed that the regulator could be a government department/directorate or an independent state authority. It was also noted that in some states, irrespective of the status of the regulator, the rulemaking and oversight tasks were split between different government entities. In such cases, the Ministry of Transport is normally the rulemaking entity, while oversight is conducted by the NSA. It is often the case that, owing to lack of sufficient expertise, the Ministry of Transport has to resort to using NSA staff to assist in rulemaking activities.

The financing of regulatory activities is also reflected in the type of regulatory arrangement employed by the state. Where the regulator is a government department, its funds are usually available from the national budget. Independent authorities, on the other hand, have the ability to generate their own funds through CRCO charges, special levies, cost recovery or a combination of one or more of these means.

Where institutional separation has been established, ANSPs are often corporatised and take the form of a private company wholly owned by the government. This enables ANSPs to decide their own financing methods independent of the government budget, although they are not allowed to make a profit from their ATM activities, in accordance with ICAO rules.

### 2.1.2 NSA staffing

Institutional arrangements have a profound effect on regulatory activities, with a consequent impact on the interface. In the majority, the interviewed NSAs indicated a lack of staff and/or of adequate expertise.

In comparison with NSAs, ANSPs – given their corporate nature – are often in a position to offer a better remuneration to their employees. Consequently NAAs/NSAs find it difficult either to attract ANSP personnel or to employ persons with the right competence/experience.

One solution which a few states have employed to address this situation is to arrange for the ANSP to loan/second some of their staff to assist the NSA. This assistance can be in the form of either actually performing the regulatory tasks or training the NSA staff. Such a solution could lead to a conflict of interests for the staff involved. This has been recognised by the states, and various forms of agreement have been formulated to protect the interests of all parties. It was reported that these agreements have achieved their intended objectives.

Training of NSA staff by the ANSP could involve either having NSA staff working for a limited period at the ANSP, or alternatively having a few ANSP trainers working as on-the-job instructors at the NSA.

Several NSAs ensure that their staff receive the most comprehensive and up-to-date training or in-service training available and have instituted their own training programmes to address such matters. Typically these programmes specify basic qualifications, training requirements and on-going working experience, with a number of them following the NSA Training Initiative at EUROCONTROL IANS. Databases of staff competences are maintained to ensure the proper and effective development of personnel, and a unit training plan is developed.

In one case, it was noted that it was mandatory for NSA staff to receive recurrent or continuation training. In this particular NSA, staff attend workshops/short courses every two years dealing with new rules, legislation, new approaches, good practice and sharing lessons.

In some cases, NSAs of adjacent states share their staff to cover areas where they have a lack of expertise. This method is cost-effective as NSAs do not need to train their staff in all areas of oversight, particularly those areas which are highly technical.

Another case was where a Qualified Entity is used for auditing the non-safety-related requirements of Commission Regulation (EC) No. 2096/2005. This approach has various advantages and disadvantages. The prime advantage is that the Qualified Entity has extensive auditing experience particularly with respect to quality and process management. On the other hand, the Qualified Entity has limited experience in the ANS field.

It was reported that an NSA can never achieve or maintain the same level of current competency as the ANSP because the latter has constant day-to-day exposure in many technical areas, whereas the NSA comes into contact with such areas only through its oversight activities. The view of many NSAs is that their role is to ensure the correct application of safety management processes by the ANSP and not to question the details of each and every report made by the ANSP.

## 2.2 Roles and Responsibilities

The relationship between NSA and ANSP reflects the clear distinction between the roles which they play in ensuring a safe service. The ANSP has to provide a safe service while the NSA is obliged to conduct oversight to ensure that the service is safe and that public safety is safeguarded. Most ANSPs welcome the independent view provided by NSAs. At times, the attention of the NSA gives added impetus to the application of safety management processes at the ANSP.

In almost all cases, primary national aviation legislation gives the NSAs comprehensive and autonomous legal powers. Basically, ANSPs have the accountability for ensuring and proving that the service which they deliver is and remains safe and is compliant with all regulations and acceptable standards and targets. It is the role of the NSAs to receive arguments and evidence that this is the case, to assess and evaluate the information received and then to issue acceptance, approvals or licences, together with any directives, variations, endorsements or revocations which they deem appropriate. Although NSAs have these extensive legal powers (including the right to prosecute), the working relationship with the ANSPs is mutually viewed to be extremely important and that it remains good, effective and enduring. In most cases, consensus is reached without the NSA having to use its absolute authority.

A number of NSAs reported that their increased confidence in the proper application of the safety management processes by ANSP often leads to less frequent oversight interventions from their part owing to improved internal monitoring at the ANSP.

Interpretation of the various regulatory requirements sometimes leads to different understandings of what needs to be done. This naturally leads to serious discussions between NSA and ANSP until a common understanding is reached. The tendency for a difference of interpretation of regulatory requirements decreases as both sides mature and have greater experience in their respective safety roles. Part of this maturity involves an improved communication process between the two parties via explicit and systematic application of interface processes and procedures.

Most NSAs have a manual on how to conduct oversight activities, which they have communicated in some way to the ANSP.

In some cases, the manual/regulatory framework specifies the deliverables expected from the ANSP and processes to show the information flow between the two parties.

Other states prefer to issue an Aeronautical Information Circular (AIC) specifying the kind of information which they would expect an ANSP to submit for consideration in respect to a particular oversight task.

The roles and responsibilities also need to be clearly defined at the level of the ANSP in order to avoid any grey areas in its dealings with the NSA and to ensure that each individual clearly knows his/her safety role and responsibility.

## 2.3 Relationship ANSP/NSA

The internal distribution of responsibilities within national aviation authorities (not only the NSA but also the links to rule-making bodies, the AAIB, the economic regulator and the military) has an impact on the effectiveness of the interface with the ANSP. In some organisations, the oversight tasks are assigned to units belonging to different directorates or organisations. Consequently, a clear internal communication process is essential in such cases in order to ensure effective coordination.

Different states have come up with different solutions how to address this matter. Some of them use a detailed national regulatory framework or manual which clearly specifies links with external agencies, e.g. ANSPs, military units or other national aviation bodies.

The implementation by the NSA of a quality management system also improves the relationship between various bodies. A QMS based on ISO 9001:2008 requires the organisation to seek customer feedback on its activities, thus identifying and clearing up any issues which compromise the relationship.

A lack of staff has also an effect on the relationship, and some NSAs draw up an annual task sheet showing the distribution of oversight tasks between their personnel in order to ensure that each area is covered in the necessary detail. These task sheets identify the primary NSA focal point and also the substitutes in case the primary focal point is not available.

ANSPs have adopted various forms of safety management. Many have a corporate SMS, backed by a unit SMS. Others have a centralised safety management function, with deployment of local safety officers. Consequently, it is essential that the ANSP SMS identifies those positions/posts responsible with the interface with the NSA.

Some ANSPs at their end have nominated a focal point with links to all the aviation authorities (both national and international) in order to ensure that information reaches the right entity. This focal point helps the ANSP to be up to date with the regulatory issues being discussed, to provide feedback/comment on these issues, and thus to be in a better position to deal for them once regulations are implemented.

In all states visited, there are bodies or working groups between ANSP and NSA meeting at regular intervals. These intervals vary from state to state and can be annual, half-yearly, quarterly or even more frequent. Normally, the frequency of the meetings reflects the seniority of the participants. Thus, the DG of the NSA and the CEO of the ANSP tend to hold an annual meeting, whilst very frequent meetings are attended by safety manager/project manager and their counterparts in the NSA, often to discuss very specific/technical issues.

The relationship between the parties varies according to the size of the ANSP. In a number of states, there are more than one ANSP. Normally there is one big ANSP providing ACC, APP and TWR services while the smaller ones are usually limited to the provision of TWR and AFIS. Meetings with these small ANSPs tend to be less frequent in view of the kind of service they provide, the associated lower risk and the availability of their personnel.

Several NSAs organise SMS workshops and/or courses for the smaller providers in order to improve the ANSPs working methods and share lessons learned, with the added benefit of an enhanced relationship between all parties.

#### 2.3.1 Example 1

The NSA holds frequent interface meetings with the ANSPs. The most formal are with the largest provider. The formal interface is managed at two levels, i.e.

- strategic, and
- tactical.

At strategic level directors and senior managers from the ANSP meet quarterly with the senior NSA managers. Both sides are supported by their experts as necessary.

Another meeting is held quarterly, at which the safety manager and his counterpart discuss issues arising from the safety regulations.

At tactical level, there would be ad hoc meetings for specific initiatives and technical activity task forces. Day-to-day oversight is exercised via various activities which include audits, inspections and reviews of projects.

The NSA procedures address each ANSP equally, irrespective of size, although a risk-based approach to safety oversight is adopted.

The good relationship between the NSA and the ANSPs is attributed to the fact that the NSA staff is recognised by all stakeholders to be expert in the fields/areas being regulated, and that the organisation maintains this respect because of its integrity, transparency and objectivity.

The history of the major ANSP is seen as a key contributor to the competence of the NSA. Historically, most of the NSA staff came from this ANSP, with many of the recruits having years of experience of operations. Consequently, this wealth of experience and the close relations with the ANSP have ensured that the NSA has great confidence in how this ANSP operates.

To maintain this good relationship, the NSA ensures that it:

- has an honest and open relationship;
- uses appropriate and timely processes;
- is objective and fair-minded in all its activities;
- recruits the right people from industry who have:
  - recognisable expertise and experience,
  - a good track record and reputation;
- ascertains that its personnel remain up-to-date by:
  - providing the right (formal) training for its staff,
  - maintaining close contact with the ANSPs in order that this exposure further enhances the NSA expertise;
- remains open to suggestions;
- supports a just culture and is protective of confidential information it receives from ANSPs.

If an ANSP does not agree with an NSA decision/instruction, it is still expected to implement the decision and position which the NSA directs. However, the ANSP has the legal right to challenge the process applied by the NSA in making its decision. This is done by means of a claim to the highest level of the NSA or to the national aviation authorities. If an NSA procedure/process is found not to have been correctly followed, the NSA has to re-visit its decision. If the ANSP is still unsatisfied with the decision, it can challenge the decision in court under a judicial review.

In the pursuit of their activities, NSA personnel have the right:

- to enter any aviation-related building without the need for prior notification or approval (possessing access cards);
- to access any document they wish to see;
- to seize such documents.

However, the applicable national regulations stipulate that all information obtained from ANSPs is confidential and cannot be divulged to other parties. The only exception is where safety is seriously compromised and the NSA might be constrained to prosecute the organisation/individual.

Another aspect which helps the NSA maintain its good relationship with the ANSPs is its robust internal consultation process, in which both the rule-making and the oversight sections review a draft prior to it being forwarded to the ANSPs for comments. The regulator uses a number of external experts to provide additional review of the draft.

This consultation process is described in the applicable national regulations.

The regulator is also obliged to carry out an impact assessment for new or amended regulations, which includes:

- the matters to be addressed;
- the various options available;
- the option eventually chosen;
- the reason(s) for the choice;
- the envisaged impact, including that on operations and resources.

Finally, in its effort to maintain the good relationship with ANSPs, the NSA has its own internal management processes (similar to QMS).

### 2.3.2 Example 2

The ANSP has a special unit, which is not part of its SMS, that is the formal interface with the NSA. This unit handles all requirements, not just safety requirements, via one of its personnel dedicated full-time to safety matters. This single point of contact at organisation level is considered an advantage (easier to follow actions, avoid duplication, etc.)

The unit handles all communications (via a secure electronic portal) between ANSP and NSA. Technical matters are referred to the relevant departments. At times, the NSA may wish to meet safety management personnel to discuss technical matters. In such cases, the safety representative of the interfarce unit also attends to ensure that the unit is always kept in the loop with regard to communication with the NSA.

No formal body has been established between the ANSP and the NSA on safety matters, but ad hoc joint groups are set up to discuss various matters (interoperability, licensing, etc.).

There are lots of meetings at technical level and cooperation is good. The relationship is considered open and constructive. It was built up over the last few years on the basis of good dialogue, starting with discussions on ESARR 4.

To ensure an open atmosphere, there are no terms of reference for the meetings, nor are minutes kept.

The agenda for the monthly unit/NSA oversight meetings is:

- report on current situation;
- regulatory matters and their outcome;
- results of inspections/audits and updates of the inspections/audit programme;
- AOB.

In addition, there are occasional safety oversight meetings. Again, these meetings have no terms of reference, but this time minutes are kept for record purposes. As these meetings are technical in nature and often focus on a particular project/matter, they are held with ANSP safety management personnel and relevant project managers. However, a representative of the interface unit is also present to ensure that it is kept in the loop.

The transfer of documents/information/notifications between ANSP and NSA is via a secure portal to which only the two organisations have access.

National law stipulates that all information obtained from the ANSPs is confidential and cannot be divulged to other parties. In addition, the NSA has its own confidentiality regulations and its staff are made aware of them. Owing to this confidentiality agreement, the NSA does not share information with other authorities. If other authorities require information about ANSPs, a special request has to be submitted to the Ministry of Transport. The Ministry of Transport together with the NSA and their legal departments will then evaluate the request and decide whether or not it is in the public interest to release the information.

### 2.3.3 Example 3

The relationship between ANSP and NSA has always been good but has improved considerably after the audit method was amended. The NSA does not regard its regulatory/oversight tasks as policing but rather as a different role in the safe provision of service which also happens to be the same goal as that of the ANSP. The NSA is looking into how to further improve its relationship with the ANSP, and both parties have identified areas where they feel that there is scope for improvement.

A number of formal bodies exist at various levels.

The highest level of formal interface is strategic in nature and composed of representatives of all the major aviation stakeholders. The DGs/CEOs of the ANSP, the NSA and major national airlines sit on this team. Safety is only one of the topics on the agenda.

A second strategic ATM working group looks mostly at airspace matters, because these have been identified as primary safety concern.

There is a joint NSA/ANSP group dealing with safety oversight, and it looks into non-conformities and issues identified during audits and inspections. This relatively new group is a result of the increased maturity of both parties.

### 2.3.4 Example 4

The interface between NSA and ANSP is at various levels, broadly split into three. Throughout the year meetings are held as described below.

The DG of the NSA and the CEO of the ANSP (together with their respective managers) meet twice to four times a year to discuss strategic matters.

The Safety Manager meets his/her respective NSA counterpart at regular intervals as needed.

The ANSP's Projects and Technical Unit meets the NSA four or five times a year to discuss projects.

Ad hoc meetings regarding big projects are held as needed. This approach has been adopted for the FAB, where it is felt that there is a particular need for communication, particularly in the harmonisation of regulations.

The state has more than one service provider with most of the small ANSPs operating TWR and one also providing a low-level approach service. The NSA holds a formal annual meeting with the approach service provider. Safety is not the only topic on the agenda, and the meeting looks into all aspects of aviation. The NSA also plans to meet the other small ANSPs on an annual basis, but this has been difficult to organise owing to constraints on resources from all sides.

### 2.3.5 Example 5

In a state where there are two ANSPs, one providing services at airports (TWR, APP) and en-route in the lower airspace while another provids en-route services in the upper airspace, the NSA has adopted a uniform approach for their oversight. The second ANSP has also been designated by another state to provide services in its upper airspace. In view of the special nature of the second ANSP, a dedicated oversight manual has been developed in collaboration with the NSA of the other country. This document is now also to be used to develop an oversight manual for the future FAB.

Several NSA personnel are nominated as 'account-holders' (focal points) for different areas. They are ATM specialists, who collect all the information related to their particular areas and forward it to the specialist NSA staff as necessary. The account-holders also coordinate with the ANSP regarding audits/inspections, though they do not draw up these plans.

If the ANSP does not agree with NSA interpretations/instructions, there is an escalation process, with the issue being referred to higher-level management.

More formal interfaces exist in the form of:

- a ministerial advisory group on airspace, made up of the regulator, the military and ANSPs;
- a national aviation safety group chaired by the DG of the regulator and with the CEO of one of the ANSPs as vice-chairman.

### 2.3.6 Example 6

The NSA/ANSP relationship is regarded as good and effective, although there might occasionally be areas or decisions, especially related to safety cases and allocation of severity classes, which are debated vigorously as the two sides challenge some argument or decision. This debate is considered to be part of the day-to-day activities, and in the end a consensus is always reached.

Although the interface is formally via the DG of the NSA and the CEO of the ANSP, a number of persons on both sides have been identified as focal points for specific activities. They coordinate and prepare the work, which is then formally channelled through the DG and the CEO. A formal NSA/ANSP group, consisting of the DG of the NSA, the CEO of the ANSP and a number of experts, has been set-up.

In addition, NSA/ANSP working groups are formed as needed. These operate on informal basis, and deal with matters such as:

- the State Safety Programme;
- the route network;
- civil-military coordination;
- FABs.

The NSA has its own handbook on how to perform its oversight activities. It addresses:

- certification and on-going compliance;
- audit methodology;
- interoperability.

This handbook was based on EUROCONTROL SESIS guidance material and also makes reference to ESARR 1 guidance material.

### 2.3.7 Example 7

The interface between the ANSP and the NSA is broadly speaking split into five levels. Throughout the year, meetings are held as described below.

An annual meeting looks into continuous oversight, analysing actions derived from the initial certification action plan and from NSA audits.

A State Safety Programme (SSP) meeting has recently been initiated. It is held annually and is undertaken in the spirit of ICAO's SSP. An action plan has been formulated to address high-level risks, including those either involving ANSP matters or those areas where ANSP action may have an impact.

Another annual meeting addresses the ANSP's overall safety performance.

Half-yearly meetings follow up progress regarding specific action plans, e.g. EAPPRI (the European Action Plan for the Prevention of Runway Incursions) and ANS (prevention of unstabilised approaches.)

Rule-making is done by a separate unit within the national aviation authority (NAA). Meetings are held between the NSA, the ANSP and the NAA to come with a common position particularly with respect to the SES and EASA. The NAA has its own experts but often relies on the safety expertise of the ANSP and the NSA.

### 2.3.8 Example 8

The need for clear national ATM oversight regulation was felt years ago and the NAA and the ANSP wrote a joint manual on safety regulatory oversight, detailing the roles and responsibilities of, as well as cooperation between, the two parties in order to achieve a common safety target. The first release was in 2004 and included reference to ESARRs. Subsequent versions were amended to include reference to EU regulations and directives.

This manual also specifies the deliverables expected from the ANSP. In addition, it has a specific process which condenses the information flow between ANSP and NSA and vice versa. This process specifies:

- reference to the appropriate regulation (e.g. AST);
- sender (e.g. AST focal point);
- receiver (e.g. NSA Safety unit);
- form of communication (e.g. email);
- trigger (when the system generates an alert to the appropriate persons that the information needs to be sent);
- comments.

The system controlling this process is also linked to the calendar of the ANSP's Safety Manager so that he also receives the trigger message.

There are no scheduled formal meetings between the two parties, but the executives from both sides meet quarterly to review the whole situation, and the meeting discusses various matters, not only safety.

The interface is considered to be rather informal as long as it follows the joint safety oversight manual. However, if it is felt that the informal interface is not functioning properly, the joint safety oversight manual also specifies escalation procedures, which could lead to a formal meeting to discuss the matter.

### 2.3.9 Example 9

A joint body, composed of representatives of the Ministry of Transport, the Ministry of Defence, the NSAs (civil and military) and the ANSP, has been established to coordinate the interaction between NSA and ANSP. There are regular and ad-hoc meetings as and when required.

Besides this body, there is also a working group to discuss SES matters in order to unify, as far as possible, the state's position on the SSC. This working group is composed of representatives from all NSAs (including MET), the service providers (ANSP and MET) and the DGCA as national rule-maker.

### 2.3.10 Example 10

NSA oversight also includes economic aspects. The economic regulator holds monthly meetings with the ANSP. These are chaired and run by the relevant economic department, but the NSA safety unit is also present to make sure that safety is not sacrificed for economic reasons.

## 2.4 Safety Oversight Audits

Safety oversight is mostly based on audits, although some states use other oversight methods in addition to audits.

The NSA draws an annual audit plan, which is normally finalised and distributed to the ANSP(s) in the fourth quarter of the previous year. In addition to such a plan, several NSAs also draw up a list of the auditors assigned to the various units/tasks, and often this is sent to the ANSP for information purposes.

During the year, the audit programme is adhered to as far as possible, but it is flexible enough to permit amendments to accommodate the needs/constraints of both the NSA and the ANSP(s). The programme mostly follows a risk-based approach and is drawn up taking into account:

- experience from previous audits/inspections;
- occurrence reports;
- interviews.

Oversight audits are performed to check compliance with one or more of the following sets of regulations:

- ICAO provisions;
- EU regulations and directives;
- EUROCONTROL standards and ESARRs;
- national legislation.

In most cases, audits look at the steady state as well as at changes, whilst at the same time looking for continuous improvement.

In larger ANSPs, the auditors often check the headquarters and ACCs annually. The other units are audited on periodic basis, usually depending on their size, level and the complexity of the traffic they handle.

Many NSAs are adopting a risk-based approach to auditing, as this provides significant benefits in terms of addressing key risk areas whilst at the same time ensuring the effective deployment of their auditors. Good management by the ANSP helps immensely in the oversight tasks. The more confidence an NSA has in the way in which an ANSP manages its processes and risks, the less need there is for closer scrutiny and monitoring.

Some states reported that categorising non-conformities by importance helps the overall process, because it identifies the main areas of concern without effort being required to address minor issues, such as document editions, updates, typos, etc.

Most participating NSAs follow the auditing process as described above, although there are a number of variations, which are described in the examples.

Some NSAs are relying on a complete ANSP internal audit programme (safety, quality, security processes) and receive on periodic basis a summary report on the results of such internal audit programme. The NSAs then use these results together with other inputs such as occurrence reporting for their own planning of the oversight audit programme.

NSAs have the authority to conduct ad hoc inspections, and these are also used as an oversight tool. The results of these inspections could trigger ad hoc oversight activities, e.g. audits. Many of the participants commented that inspections were not an ideal tool, as they have the following disadvantages:

- the required information may not be available at short notice to the NSA inspector, because the person who has it is not available at the site;
- inspections could cause disruption in the OPS room/engineering sites.

#### 2.4.1 Example 1

In one state, oversight is performed by several NSA personnel nominated as 'account-holders' (focal points) for different areas. They are ATM specialists, who collect all the information related to their particular areas and forward it to the specialist NSA staff as necessary. The account-holders also coordinate with the ANSP regarding audits/inspections, though they do not draw up these plans. Such plans are drawn up by the audit team, but they look only at processes because they audit across all domains.

#### 2.4.2 Example 2

The NSA uses a risk-based approach to auditing, aided by an IT tool to grade the various units. The NSA uses this tool to obtain a better understanding of its regulatory customers and then rank them 1-15 on the basis of key indicators such as past performance, reliability and financial strength, to name but a few. Grade 1 is considered to be the best, and in such cases a focal point is nominated to follow the ANSP/ATSU and pay annual visits. Grade 15 is the worst, meaning that several persons would be dedicated to this particular ANSP/ATSU, paying numerous visits over the year. Projects are also audited as part of the checks on compliance with the relevant regulations and also to assist in their final acceptance.

NSA auditors were considered to be approachable and also sensitive not to cause disruptions in the units.

#### 2.4.3 Example 3

The NSA, three months prior to the date of audit, sends a formal notification to the ANSP. A month later, the NSA sends the audit plan and a form requesting various types of information, e.g. points of contact, persons available for interview, data regarding the area to be audited. Normally, it is stipulated that a person can participate in a maximum of only two interviews. The NSA imposes this restriction in order to ensure that it has a wider spread of information and viewpoints rather than be restricted to those of one person. The ANSP has two weeks in which to submit the required information and return the completed form, i.e. the information must reach the NSA six weeks before the date of audit.

One month prior to the audit the NSA distributes to all concerned the final audit plan, which is based on the information submitted by the ANSP in the NSA

form. Subsequent changes to this final audit plan, which are expected to be only of a minor nature, are discussed and agreed during the opening meeting of the audit.

Approximately 10 audits, each lasting between 1 and 3 days, are carried out annually across all areas. A new system is on trial, in which some of the surveillance audits are carried out by the ANSP's own corporate audit section, which is independent of all other units of the ANSP and reports directly to the CEO. Currently, an NSA auditor accompanies the ANSP team as an observer. If the trial is successful, some of the NSA audits may be cancelled on a risk-based argument. Consequently, the number of NSA audits would be reduced. This new process would only be used for surveillance (new) audits and not for follow-up audits.

Another important development in the audit process is the way in which non-conformities are corrected. In the past, the NSA used to set target dates for the completion of corrective actions (CA). Now the ANSP reviews non-conformity and submits a corrective action plan, which may be part of a project activity or even a separate project, to the NSA. The NSA then decides whether or not to accept the proposed CA plan and its deadlines/target dates. It does not comment on the proposed corrective action. The effectiveness of the CA is subsequently checked during a follow-up audit. This process was started about late 2009. It is reported to be a much better and efficient arrangement and has led to greater cooperation and understanding between the two parties.

### 2.4.4 Example 4

Previously NSA audits were carried out according to the competence of the auditors, i.e. ATS units were audited by auditors having an ATS background, but only on ATS matters. The same unit could be audited again in the same year by other auditors having a different background. A two-man audit team would check larger units, whilst only one auditor would visit the smaller units. Since the beginning of 2010, the NSA has been conducting trials with joint auditing teams having ATS, CNS and airport backgrounds. Although the scope of such audits would be wider, it is expected that such an approach would reduce the number of audits conducted at units, leading to less disruption.

### 2.4.5 Example 5

The annual audit plan is risk-based, taking into account several aspects, such as:

- cooperation with the NSA;
- non-compliance;
- handling and solving of non-conformities;
- ANSP's proactive behaviour.

The NSA is also building a causal model to help identify risks. Information from this model is to be used in the audit risk-based approach. The primary objective of the NSA audits is to ensure that ANSP management is really in control.

In its risk-based approach, which was in use for several years on aircraft maintenance companies and is now used for all its oversight activities and not just ATM, the NSA awards points to several factors: the lower the score the better. Green and red limits (Optimal vs. Improvement Necessary) are identified. Organisations which obtain a high score (Red) have several audits a year, which could include up to three large audits (4 man-weeks each). Green organisations, on the other hand, have fewer audits and might even have just one large audit in a year. This has been found to be a very good system, although the NSA is reviewing it, after it noted that the scoring was subjective and at times differed between NSA individuals.

### 2.4.6 Example 6

The NSA would like to base its oversight more on trust rather than on enforcement. An experiment was carried out to establish a basis for mutual trust, in which the result of the ANSP's self-assessment using EUROCONTROL's Safety Maturity Survey Questionnaire was compared with the assessment of the NSA based on its oversight activities. The two parties then discussed the areas where the two organisations had differences of opinion on what had to be complied with. In this way, it is felt that both organisations get a clearer view of the situation and can harmonise their understanding of requirements.

### 2.4.7 Example 7

The NSA, in coordination with the ANSP, established an annual surveillance plan which includes audits, change management and periodic meetings. The audits focus on themes requiring monitoring, e.g. follow-ups, changes and national performance

management. The oversight checks that the ANSP system is well organised and properly managed. No inspections are carried out.

This state has more than one ACC, and several regional approach centres. There are also a significant number of airports of varying sizes ranging from major to regional to very small local fields.

To reflect the large size of the ANSP, the NSA is correspondingly large. It employs around 20 staff in its Central Division, backed by about 50 auditors nationwide, distributed amongst various regional offices. The NSA staff have a wide variety of aviation backgrounds backed by several years of experience in the field.

To ensure impartiality and also increase the exposure to different units, the lead auditors normally do not audit units within their region.

The annual audit plan is seen to be dealing with the 'corporate' level, so at this stage, contact between the ANSP and the NSA regional units is not encouraged. The NSA in fact recognises only one focal-point for corporate matters, namely the ANSP's safety manager. All parties are expected to have carried out their internal coordination and discussion before the annual plan is formally finalised.

For the on-site audit, the site audit plan is sent to the Head of ATS Unit and its safety manager/officer. Amongst other things, the plan specifies the schedule and the list of people (jobs/positions/tasks but not individuals) who are expected to participate. Each ACC is audited by the NSA once every three years, while each regional approach centre is audited every other year. The ANSP's HQ is audited annually.

In the past, each site was the subject of an individual audit. This method was seen to have shortcomings with respect to the small (AFIS) airfields, which often had an interface with a larger airport and even with one of the regional approach centres. Consequently, when these small fields were audited, it was often necessary to audit the coordination process/procedure with the larger units. This meant that the larger units would be audited several times a year for the same process/procedure, which in turn might even be part of the larger unit audit. This was felt to be causing too much disruption and unnecessary work.

The new method audits a regional approach centre and its interaction with all other units in its area of responsibility. In addition, half of these units are subjected to more detailed scrutiny. The following year, the other half are scrutinised in detail. Applying this method has considerably reduced the number of major audits, as it has eliminated the repeated work of scrutinising the coordination with the larger unit. A major audit is now performed by a four-man team, who scrutinise the regional approach centre for one week.

Audits are based on criticality and confidence in the unit's safety maturity. While the ACCs are considered to be safety-mature, because they employ well-tested methods and experienced staff, some airports are considered to be in need of greater oversight. Factors which affect this decision are complexity of operations, traffic levels, age of ATCOs (young, fresh from college, very few years of experience vs. old, highly experienced in many different ATC domains), unit training, etc.

After an audit is completed:

- the audit report is sent within one month of the audit;
- the ANSP proposes a corrective action plan within two months of receipt of the audit report;
- the authority accepts or rejects the corrective action plan within one month of receiving it;
- the corrective actions are followed up and the audit findings are closed;
- the findings are closed once the corrective actions are considered to have been taken.

Different levels of follow-up are used depending on the type of actions, ranging from a simple declaration to formal checking.

The ANSP conducts a significant amount of internal auditing. In addition, each ACC (and even the NSA) undergoes an ISO audit every third year. In view of this, the staff interviewed feel that there could a risk of units being over-audited, particularly if there is a lack of coordination between the various audit plans. Also, whilst all auditors check the processes, the scrutiny of details depends on the background of the auditor.

The NSA audit, however, is still viewed by the ANSP as extremely beneficial, as it ensures that people do not become complacent.

### 2.4.8 Example 8

Scheduled audits are conducted at each ANSP at least once in the course of each year. Not all aspects are reviewed, but the NSA is in the process of developing an Excel spreadsheet tool to ensure that all elements are audited at least once over a two-year period. Although each service provider is audited once a year, it is recognised that the same audit strategy is not appropriate for all service providers. Consequently, each audit is tailored to the scope/complexity of the service providers' operations

In addition, one-off audits are conducted prior to the acceptance of significant new changes, where this is considered appropriate.

The NSA reserves the right to conduct additional audits should a situation arise in which the level of confidence in an ANSP falls below expected standards (for example if adverse trends are detected in key risk areas). To date, it has not proven necessary to subject an individual ANSP to such additional audits.

As part of the development of the annual audit plan a lead focal point is identified for each audit. This "point of responsibility" is responsible for:

a) being the NSA focal point for the audited organisation (audit planning/scope definition/ checklist development);
b) coordinating and producing/receiving the audit report;
c) identifying the need for corrective actions;
d) keeping appropriate records.

Generally, the NSA aims to give each provider around three months' notice of a planned audit.

The closure of identified non-conformances is tracked using a dedicated database established for this purpose. Guidance on the audit finding corrective action process is provided to ANSPs via an advisory document which is available from the NSA website. Auditees are required to provide proposals for corrective action for low- and mid-level findings within one month of the audit. Most severe findings require immediate action to be taken, depending on the nature of the finding. The NSA audit report may include recommendations for consideration by the auditee, but implementation by the audited organisation is at its discretion following consideration of the benefits and risks associated with its action. The implementation of recommendations arising from previous audits is reviewed as part of the scope of each audit.

On completion of corrective actions, the ANSP is required to inform the NSA and provide appropriate evidence when requested. Depending on the nature/ severity of the finding, the NSA may re-audit the activity prior to formal closure. Identified weaknesses are also subject to ongoing review as part of the ongoing annual audit programme activity.

Given the increasing number of regulatory requirements under development (e.g. interoperability implementing rules), the challenge of meeting the regulatory requirement (ESARR 1 transposition into EC 1315/2007 on safety oversight) is likely to require increased adoption of standardised checklists/tools (Europe-wide). The NSA is currently in the process of developing a spreadsheet-based tool in order to provide a means of ensuring that this regulatory requirement is being fulfilled.

Ad hoc/targeted inspections may be undertaken where information or evidence identifies a need. In such circumstances, notification to the organisation is at the discretion of the NSA senior management. In addition, targeted inspections are undertaken prior to the NSA acceptance of specific changes.

## 2.5 Management of Occurrence Reporting and Investigation

All states visited have a mandatory occurrence reporting scheme in place. In some countries, this is backed up by a voluntary and/or confidential reporting scheme.

Occurrences to be reported are specified, and the list is based on ESARR 2. In line with regulatory requirements, all states have an independent body which investigates aircraft accidents and serious incidents. The ANSP notifies the AAIB of such occurrences either directly or via the NSA/NAA. In several states, the organisation responsible for reporting to EUROCONTROL (AST) is actually the ANSP.

It was noted that only a few states have identified which organisation follow up the implementation of

AAIB safety recommendations (SRs). In some states, the ANSP and the NSA do not get direct feedback from the AAIB. The investigation report is only available via third parties (the Ministry of Transport) or from the AAIB website.

In some states NSAs have the authority to conduct their own investigations, particularly into those occurrences which do not fall within the AAIB's remit. However, NSAs often ask for the ANSP's internal investigation report on such occurrences in order to review it. They can instruct the ANSP to investigate in more detail if it is felt that the initial internal investigation did not go into sufficient depth. To ensure a more harmonised risk assessment of occurrences some states recommended the use of the Risk Analysis Tool (RAT).[2]

It was reported that in some cases AAIB investigators either have a pilot background or are ex-ATCOs who left the service quite some time before. Consequently, in some cases, the AAIB safety recommendations either fail to address ATM questions or are based on old practices.

#### 2.5.1 Example 1

All occurrence reports from ANSPs, aircraft and airport operators are sent to a dedicated email address and are automatically forwarded to the appropriate oversight personnel. The details are maintained in a database and the NSA compiles a summary report of ANSP occurrences every six months and forwards it to EUROCONTROL.

NSA involvement is normally limited to a review of the ANSP's investigation reports and requests for clarification. In the case of significant occurrences, the NSA may conduct its own investigation.

When auditing ANSP occurrence reporting processes, the NSA ensures that there is a common understanding on when an occurrence report must be issued.

#### 2.5.2 Example 2

Occurrence reporting is primarily via an electronic form. The system is automatic and any report filed under the Mandatory Occurrence Reporting (MOR) Scheme is automatically sent to a generic mailbox at the NSA, where it is filtered and forwarded internally. In addition, ANSP staff also have the facility to file a paper report and submit this direct and in confidence to the NSA. In such cases, the ANSP does not have a copy of the report.

Finally, staff can also have recourse to a completely independent, confidential (but not anonymous) national reporting system which is available to all individuals employed in or associated with aviation and maritime safety and is intended to contribute to the enhancement of aviation and maritime safety. All occurrences reported to this organisation are thoroughly investigated internally (independently of NSA investigations). These investigation reports, and in particular their recommendations, are forwarded to the NSA.

Under the national MOR Scheme, all occurrences are to be reported within 96 hours. Once a report is received, the NSA evaluates it and decides whether or not to investigate. There is a focal point at each unit whom the NSA contacts to obtain the required data, and, if need be, to inform the persons involved of the investigation.

As we understand, both ATCOs and ATSEPs file occurrence reports.

The NSA has its own ATS investigators to look into those incidents which do not attract the attention of the AAIB. Though these occurrences might not be considered as serious incidents in the eyes of the law, the NSA can still consider them serious enough to warrant investigation. These ATS investigators not only look at the occurrences themselves but also at the NSA processes in order to identify any possible shortcomings in the oversight.

2 For EU states RAT is now mandatory as required by the Commission Regulation (EU) No 691/2010.

### 2.5.3 Example 3

Occurrence reports, based on an MOR scheme, are sent primarily to the NSA, although accidents and serious incidents need to be reported in parallel to the AAIB. In addition, occurrences as defined in ESARR 2/EU Directive 42/2003[3] are also forwarded to the regulator (the Ministry of Transport), as this organisation is the national focal point for ECCAIRS. ATCOs/ATSEPs can submit an individual report to the Ministry of Transport/ECCAIRS. Under a special written agreement (backed by national law), they forward reports via the ANSP safety management process and need not to send it directly to the Ministry of Transport.

At the moment there is no NSA/NAA standard reporting form. However, a template is soon to be developed. All reporting is confidential, although there is no law to secure data from access by public prosecutor. Only de-identified reports are sent by the ANSP to the NSA/Ministry of Transport/AAIB, but in the event of an investigation these authorities have access to the names. The NSA does not carry out occurrence investigations, but it can still have access to the reports, although it is more interested in causes and corrective actions. Since the NSA does not have investigators, it can only monitor the ANSP occurrence investigation process. The information submitted is considered essential to feed the risk-based approach to audit planning and execution.

Occurrence investigations are carried out by the ANSP, which has investigators at local unit level, although some of them are only part-time, especially in the smaller units (Towers). Occurrences are notified (reported) by the units, with copies submitted internally as necessary. Reporting is mandatory, but the ANSP investigation report is forwarded to the NSA only if the latter so requests. If the NSA requests the investigation report, an interim report is normally submitted within two weeks, whilst the final report is sent after about eight weeks.

Under national law, the ANSP is obliged to provide technical support/expertise to the AAIB. Certain ANSP staff can be nominated by the AAIB to act as its investigators, although the lead investigator is still from the AAIB. The ANSP and AAIB have a formal bilateral agreement on the use of these ANSP personnel.

The NSA has no formal or written agreement with the AAIB nor is it able to use the ECCAIRS database owing to IT incompatibility. When the AAIB issues ATM safety recommendations, the NSA monitors them and requests the ANSP to report on their implementation.

### 2.5.4 Example 4

Occurrence reports are handled by a special unit in the NAA (not the NSA). All occurrence reports, not just ATM, are handled by this unit. It will then review these reports and distribute them internally to the appropriate sections. The unit can also investigate these occurrences (assisted by the ANS section) or ask for information about them. It also does trend analysis for the whole aviation sector. On the basis of its investigation or trend analysis, this unit can issue recommendations to the service providers. It is also the contact point for ECCAIRS.

This state has also set up a special office in the Ministry of Transport to look into all matters related to civil aviation safety. This office is also particularly involved in the process regarding the handling of safety recommendations.

In the past, AAIB SRs were passed directly to the NSA. Nowadays they are sent to the Ministry of Transport safety office. This unit decides on the implementation of SRs. The decision process includes a thorough consultation phase with the NSA and the aviation industry and is aimed at identifying the main safety concerns and effective measures to improve the situation.

3 A list of examples of serious incidents is now also shown in the Annex to Regulation (EU) No 996/2010 on the investigation and prevention of accidents and incidents in civil aviation.

The Ministry of Transport safety office then decides on how to deal with the safety concern. This can take one of three forms:

- Usually, a binding project framework is formulated and issued to the NSA. On that basis, the NSA then plans and conducts a safety project and implements the measures in the usual manner. The project is followed by the Ministry of Transport, and the success of the measures is again reassessed by NSA and reported to the Ministry of Transport.

- When minor shortcomings are identified, but no binding directive is warranted, the Ministry of Transport issues a recommendation to the NSA. While no immediate action is requested from the NSA, the issue is followed up by both the NSA and the Ministry of Transport.

- If action has already been taken by the NSA or no further action is justified, the Ministry of Transport decides not to take further steps on the matter. When measures are already planned, the Ministry of Transport follows their implementation and outcome. If the safety action taken is rated unsatisfactory by the Ministry of Transport, the case is reassessed.

There is a prescribed list of occurrences which have to be reported. Full data is sent, but all reports are non-punitive, except in the cases of gross negligence or criminal conduct. This "just culture" reporting is supported by an appropriate article in national law. On the other hand, national law regrettably still allows prosecutors access to AAIB data, even though this is meant for ICAO Annex 13 purposes. This state has in fact filed a difference with ICAO regarding Annex 13. This anomaly has long been recognised and steps are in hand to address it. It is expected that an amendment will shortly be made and the difference with Annex 13 removed.

There have been occasions when the prosecutor acted on AAIB information without asking advice from the NSA. Judicial authorities can also access the NSA database, but a court order is required in this case.

### 2.5.5 Example 5

There is a prescribed list of occurrences which have to be reported. The NSA is the contact point for ECCAIRS and the AST. The NSA does not carry out investigations.

Accidents and serious incidents are investigated by the National Safety Board, an autonomous administrative body which was set up to investigate any kind of incident, but which in practice is currently active in the following sectors: aviation, shipping, rail transport, road transport, defence, health care (human and animal welfare), industry and networks, pipelines, construction and services, water, and crisis management and aid provision.

Other incidents (occurrences) are investigated by the ANSPs, who then forward their investigation reports to the NSA. Such reports are mainly used by the NSA to build up a database of occurrences for analysis. However, the NSA has the authority to ask the ANSPs to provide more information and look into an investigation in more detail. In addition, any occurrence which the NSA considers to be serious (the ANSPs are provided with a list) must be reported immediately and may also trigger an inspection.

The Ministry of Justice has the right to access the NSA information, a situation which not everybody is happy about. It seems that the National Safety Board is not subject to this rule; it is mandated to establish the truth rather than to apportion blame.

### 2.5.6 Example 6

A MOR scheme is in place and Aircraft Operators, Airport Operators and ANSPs all have to submit a report on the same occurrence to the AAIB, which is the sole investigation body. In addition, the occurrence report has to be copied to the NSA. The AAIB, which is responsible for ECCAIRS and AST, maintains an occurrence database and ensures that it receives the report from all three sources. The law is very strict on reporting, and non-compliance could lead to substantial fines or even imprisonment. The list of reportable occurrences is based on ESARR 2.

Voluntary reporting is implemented, but is not considered to have been a success, as only a few reports have been received. No reasons were given for this lack of success.

Although the AAIB is theoretically the sole investigation body, it normally limits itself to accidents and serious incidents. Occurrence investigation is conducted by the ANSPs. The AAIB can, on the basis of the original occurrence report, ask for copies of the ANSP's investigation results. The AAIB has the

authority to change the severity assigned by ANSPs, given that it has more sources of data, including the military, available to it. The AAIB can nominate expert investigators from the ANSPs to assist in its investigations. However, the AAIB is still accountable for the investigation.

In the past, internal ANSP occurrence investigation reports were also sent to the NSA, but only occurrence data is now forwarded. The NSA uses this information as a basis for its audits.

The AAIB and the NSA have issued a joint statement to the ANSPs guaranteeing the confidentiality of occurrence reporting. The roles and responsibilities are clear to all parties, but it was not specified what form these take. The NSA has no formal agreement with the AAIB regarding the handling of occurrences, but such an agreement exists between the national regulator and the AAIB. The plan is to have such an agreement by the end of 2010.

### 2.5.7 Example 7

Occurrence reporting can be automatic and/or manual.

Automatic reporting is triggered by safety nets. It is an easy method of obtaining reports but requires analysis to remove false alerts.

Manual (human) reporting is via a special IT tool, and all occurrences are notified direct to the NSA. A large number of safety events (about 23,000 a year) are reported. To avoid duplication of work, the ANSP's database is linked to the NSA's ECCAIRS. The huge number of reports was considered to be too much for the NSA to classify properly. Consequently, agreement was reached with the ANSP for it to do the classification work in accordance with a pre-defined methodology.

Additionally, significant occurrences are notified within five working days to the AAIB. The AAIB safety recommendations (SRs) are sent to the NSA, which in turn forwards them to the ANSP to formulate an appropriate answer. The ANSP and the NSA then discuss the proposed answer between them.

All safety events are reported to the NSA and all significant events are assessed in detail. If there is a significant safety concern, the NSA can issue a safety directive imposing safety measures on the ANSP. The NSA does not conduct investigations/analysis. These are either carried out by the AAIB (in the case of accidents/serious incidents) or internally within the ANSP. However, the NSA may select events of significant interest and ask for ANSP analysis and actions. If the situation so warrants, the NSA may impose the ANSP to conduct further analysis of a particular incident(s). Periodic meetings are held in order to monitor progress on these actions.

As part of SSP, the state has an aviation safety events monitoring unit. This unit monitors the reports of all events and then draws up a list, not only of the significant ones but also of minor ones which could be considered as precursors. It often recommends that the NSA look in greater detail into these precursors. The ANSP is then asked to provide a detailed analysis of the event. If the NSA is not satisfied with these analyses, it may even ask the ANSP to revisit the event and conduct a more in-depth examination. Analysis of precursors can, at times, be lengthy, but this is considered essential work. In order to reduce the number of requests, it is planned to hold quarterly bilateral meetings. It was mentioned that at times the reviewers might inject a particular bias into their analysis/reviews. Talks are underway on how to address this problem, although this independent review is still considered necessary, as it brings a different perspective on matters.

All reports are confidential, but this does not extend to judicial investigations. However this lack of confidentiality with respect to judicial investigations seems to have little impact because the ANSP considers that it has a good reporting culture. This was not always the case, and it was achieved through hard work, with various activities having been undertaken to promote safety culture and reporting. The ANSP Safety Management Unit has an action plan to promote more reporting and also to include Human Factors training.

## 2.6 Safety Assessment of Safety-related Changes

All states are applying Commission Regulation (EC) No 1315/2007, but there is a wide degree of interpretation on how to meet its requirements. ESARR 4 was often mentioned. The impression given was that it is in some cases mistakenly used as an acceptable means of compliance for the applicable EU regulations, instead of using an assessment methodology.

Safety assessment of changes was highlighted as a key area where the interface could be enhanced. It was reported that a difference of interpretation of the regulatory requirements between NSA and ANSP leads to significant debate. Another point of contention in this matter concerns when the ANSP needs to submit the safety assessment for NSA acceptance. This did not concern the severity requirement (as per Commission Regulation (EC) No 1315/2007) but rather at what stage the NSA needed the documentation in hand in order to be able to perform its evaluation of the change. Some ANSPs, on the other hand, reported that the NSAs are not clear about what documents are needed for their evaluation and also how long the evaluation takes.

The evidence requested by the NSA often depends on the expertise of their change assessment focal point. It was commented that this relationship depends very much on the NSA individual, and if this person is not available there can be problems. Some of the NSA personnel do not have sufficient expertise to look into content, and occasionally the ANSP has to describe the system to them in detail. Some ANSPs question whether it is really necessary for the NSA to understand every nut and bolt of the ATM system in order to supervise whether the risk assessment process complies with regulations.

The overall feeling regarding the current situation is that the NSAs appreciate the safety assessment process applied by the ANSPs, but they do not seem to be happy with how it is documented. On the other hand, the ANSPs would also appreciate some guidance material from the NSAs on how they can comply with the requirements.

Both parties agree that management of change is a point for debate, and both sides are looking into the matter to come up with solutions in order to improve the interface and resolve any points of discussion.

Many states are applying EUROCONTROL SAM. However, it seems that both the ANSPs and the NSAs are not entirely satisfied with this methodology as it is not applicable for every type of change. In addition, it requires a considerable length of time before safety specialists feel confident applying it.

### 2.6.1 Example 1

A large ANSP has a formal safety assessment process, which also includes document templates. In this process, there is the requirement to inform the NSA of all safety related changes, and notification must be right from the start of a project. The NSA then chooses which to check (by means of an audit), looking both at the process and the content. An auditor is nominated to follow the project. Depending on the size and complexity of the project, this auditor can request the support of other auditors/ad hoc experts to look into particular areas of the change. Once the project is ready to be put into operation, the NSA, on the basis of the on-going oversight, decides whether or not to accept the project. After implementation, the oversight (audit) continues, primarily to ensure that all promises made in the safety case are delivered when the change is in operation.

Although the smaller ANSPs may not have a template, they are still required to notify the NSA and present a safety case. The NSA then checks that all the required information has been conveyed, and is understandable and acceptable.

Organisational changes are also assessed for their safety impact, particularly to ensure that all safety accountabilities have been reassigned to the new posts/positions.

The on-going oversight of changes is considered to have both advantages and disadvantages. In the first place, it builds up the trust between the ANSPs and the NSA. At the same time, it protects the public from non-sustainable projects. On the other hand, the ANSP might substitute its own internal monitoring of the project by the regulatory oversight.

The NSA processes are designed so as to ensure that the ANSP owns the risk of the change. This ensures that the ANSP has the processes to manage these risks and the tools to fix them.

### 2.6.2 Example 2

The ANSP has a clear internal process for management of changes and a structured system for safety assessment and how it is documented. It is mandatory to use the structured system, because it contains all data and documentation related to change. The methodology for safety assessments is proposed by the ANSP and accepted by the NSA.

Notification and reporting of changes to the NSA is via a standard template based on Commission Regulation (EC) No 1315/2007 requirements. This template was drawn up after discussion between and with the agreement of both parties. The ANSP notifies the NSA of all changes, including non-safety-related ones. However, depending on the safety impact, if any, safety assessments in compliance with Commission Regulation (EC) No 2096/2005 are then carried out. If the NSA considers that a change requires a safety assessment, it can oblige the ANSP to carry it out even if the ANSP is not of the same opinion. It was commented that it took two years to refine this process, which now works seamlessly.

The notification is forwarded to the NSA via the electronic portal through the safety management focal point and contains information such as:

- the system affected;
- a high-level description;
- the name of project manager;
- contact details;
- the safety impact;
- the type of safety documentation;
- transition activities and the type of safety documentation for those activities.

After notification, the NSA nominates a project officer from its side, evaluates the information given, particularly as regards the severity of the risk, and informs the ANSP whether or not more information is required. Usually this process can take up to two weeks (the maximum time for a response is 30 days, in accordance with the administrative procedure).

Depending on the scope and size of the change, as it progresses, regular reports are sent to the NSA until the approval/acceptance stage is reached. The NSA then issues either:

- an acceptance;
- an acceptance subject to additional information provided;
- a non-acceptance.

A standard form for acceptance has also been developed. In cases of partial acceptance/non-acceptance, the form lists the negative findings. The ANSP is expected to submit a revised safety assessment documentation to address these findings.

Usually this phase lasts about two weeks before implementation, and acceptance is sometimes issued subject to fulfilment of all assumptions, pre-conditions and safety objectives. During the evaluation of the safety assessment documentation, the NSA looks into both the process used and the details of the evidence submitted.

In the case of big projects, there are regular meetings to check whether the NSA requires more information and to ensure that the information provided is satisfactory. These meetings are not documented (there are no formal minutes). In the case of small changes (which are reported to the NSA in monthly reports), it is planned to conduct occasional visits to the ANSP and audit/check a selection of these changes.

Safety assessments of organisational changes are not carried out, as they do not fall under the requirements of Commission Regulation (EC) No 2096/2005.

### 2.6.3 Example 3

Every change has to be notified to the NSA. A review is underway as to whether only major changes should be notified. This does not mean that minor changes would not be checked, but they would not be subject to the change acceptance process. Minor changes would fall within the scope of an ESARR 4 audit and samples of such changes would be checked.

The ANSP has its own methodology for assessing changes and this has been accepted by the NSA as AMC to ESARR 4. The methodology includes all the necessary steps, e.g. notification, processes for minor/major changes, timeframes and interaction

with the NSA. When the change is a big project, the NSA is involved throughout the whole life-cycle, and it nominates representatives to attend the various meetings. The early participation of the NSA in big projects has the added advantage of helping to build up its experience, and both parties can learn from the interchange.

There have been occasions when the status of a change has had to be downgraded by the NSA. However, on such occasions the change was still monitored. As the NSA expertise increases, it is expected that such cases will become rarer and the NSA will be in a position to understand how the system works and thus able to (technically) challenge the evidence provided. Changes are also subject to audits where evidence/products/results is/are expected to be seen, particularly after implementation and when the system is mature.

A limited number of NSA staff have unrestricted access to the ANSP's document management system. Time is saved in this way, as these people can check directly for the information needed for acceptance, without having to resort to formal requests. However, there needs to be absolute trust on the part of the ANSP that confidentiality will be respected by the NSA.

Interviewees remarked that, at times, there are discussions about the deadlines for the submission of information, and it was felt that this could be an area where there is scope for improvement.

#### 2.6.4 Example 4

Oversight is performed by several NSA personnel nominated as 'account-holders' (focal points) for different areas. They are ATM specialists who collect all the information related to their particular areas and forward it to the specialist NSA staff as necessary. Safety-assessment-related activities are performed by a specialised NSA team, which includes the focal point.

Six weeks prior notification is required, but there are times when this is not respected. Also, there have been occasions when the NSA felt that insufficient information was provided.

The NSA intends to formalise the procedure and change the present process. The ANSP will be asked to provide a list of changes planned for the coming three years. These will be assessed by a change implementation group, having representatives from the (civil) NSA, the ANSPs, the Ministry of Transport, the Ministry of Defence and the military NSA. The (civil) NSA will then indicate which changes it will review in more detail. Each change will then be reviewed at a meeting, to be held around once every six weeks.

Another part of this new process will involve the development of a matrix indicating to the ANSP what type of safety assessment will need to be carried out. However, this is still under discussion.

#### 2.6.5 Example 5

The NSA requires information on all changes to functional systems, before they are put into service. This is the first step in the oversight of safety assessments. The ANSP has its own checklist, based on Annex H of SAM v2, to allow it to make an initial judgement as to whether a change needs to be notified to the NSA. If a notification of change is seen as necessary then this is sent to the NSA. Subsequently, a report is sent to the NSA at the end of each safety assessment phase. The NSA chooses whether or not to accept these reports. If they are not accepted, the ANSP might need to carry additional safety assessment activities until the NSA is convinced. At the end of all safety assessment activities, the NSA issues a formal acceptance or non-acceptance.

A focal point for each change, particularly large ones, is nominated both at the ANSP and at the NSA. Normally, the project manager represents the ANSP, whilst the NSA nominates a project supervisor. These two are responsible for all coordination. However, all documentation for each phase is transmitted formally from the CEO of the ANSP to the DG of the NSA.

The information submitted is checked to ensure that the process is being correctly applied and also for its content. There can be cases where a change is highly technical (for example in matters related to ESARR 6) and where the NSA lacks in-house expertise. On such occasions, the NSA relies solely on the ANSP's declaration.

There are no templates for notification messages and acceptances, but standard text and procedures, particularly with respect to interoperability, are specified in the NSA's own oversight handbook.

The greatest constraint which the NSA faces with the

oversight of safety assessments is lack of sufficient time to analyse the information submitted by the ANSP owing to the volume of technical documentation provided. (It can take up to a year to analyse it.)

On the other hand, the ANSP feels that the NSA is too subjective in its interpretation of the safety assessments reports and that it also fails to supply proper justification for the rejection of these reports. A possible cause of this may be that the NSA staff are not sufficiently familiar with the technical matters in the reports.

### 2.6.6 Example 6

A local regulatory procedure describes the roles and responsibilities when more than one service provider (e.g. airport + ANSP on taxiway works) is involved. The most important point of this procedure is that the providers need to identify who is responsible for the change.

### 2.6.7 Example 7

All ATM changes are entered in the change database. Once a month, this database generates a report, which is forwarded to the NSA. Thus all changes are notified to the NSA. Once notification is received, the safety oversight of ATM changes consists of the following:

1. designation of a safety analyst;
2. safety plan and a coordination plan;
3. a review of the safety case;
4. a decision by the NSA;
5. safety assurance;
6. audits.

The answer from the NSA after notification of the changes is transmitted within 15 days.

ATM changes which do not require NSA acceptance can be subject to documentary reviews at a later stage (after implementation).

An NSA safety analyst:

- is designated for each change followed by the NSA;
- represents the NSA during the review of the change;
- must have followed an initial training on safety cases which is acknowledged by the NSA, and must maintain his/her competency.

The involvement of the analyst in all phases of the change is seen to have significant benefits. In particular:

- it avoids dead-end situations:
  - difficulties encountered are discovered early;
  - there is time to solve problems at the appropriate hierarchical level;
- it avoids implementation delays.

ATM changes subject to review require a detailed safety plan. This has to provide the following information:

- a description of the change, the scope of the studied system, a description of its interfaces;
- the roles of the various actors in the safety case;
- a description of the methods which are to be used to build the safety case:
  - identification of the safety objectives and requirements;
  - safety assessment and assurance.
- the envisaged operational and technical training principles;
- a schedule of the various phases of the safety activities.

The safety analyst then validates the safety plan. A safety plan can evolve without a new formal validation by the safety analyst, but the safety analyst must be informed of any significant evolution of the safety plan. The analyst then draws up a coordination plan, which is a kind of 'contract' between the safety analyst and the contact point on the review arrangements. It is used to formalise the framework of the review of the safety case. In addition, the coordination plan identifies the 'acceptance limit point' (ALP), which is the point at which it is necessary for the ANSP to have received acceptance from the NSA in order to continue the deployment of the change. The operational implementation date for the change is not necessarily the only ALP. The coordination plan could specify others, and this is often the case for major projects. The ALPs are considered crucial for the oversight process, and should be defined as soon as possible during the safety case review process.

The safety case review is based on periodic meetings, and a review of the documents on a continuous basis. The safety analyst has to check:

- the scope and description of the change;
- the assumptions made during the safety case (in particular the interfaces with external systems);
- the risks and hazards identification;
- the consequences of the hazards;
- the coherence of the severity classification of the hazards;
- how the safety objectives associated with the hazards were determined;
- the validity and feasibility of the safety requirements;
- how it will be demonstrated that safety objectives and safety requirements are met and will continue to be met;
- if the risk mitigation measures are effectively implemented;
- if the transition phases have been taken into account.

Once the ANSP completes the safety case:

- a formal mail is needed to notify the NSA that the safety case has been finalised and that the safety case has been sent to the safety analyst. (The safety case must be finished and sent to the safety analyst one month before the ALP.);
- the safety analyst report gives the NSA:
  - information about the essential characteristics of the considered change;
  - a critical analysis of the safety case;
  - the safety analyst's conclusions with regard to the safety acceptability of the change;
  - a proposal for an NSA decision.

The NSA then has one month to answer, and its decision can be:

- acceptance of the change;
- a request for additional information;
- non-acceptance of the change.

Conditions can be defined within the acceptance, for instance for safety actions to be undertaken after acceptance.

Safety assurance after the change is considered to be part of the safety case, and the safety analyst has to ensure that the ANSP has planned to implement means allowing verification, during the operational life of the system, that the safety objectives and requirements are met. Safety indicators might be defined by the ANSP before the implementation of the change. These indicators will be monitored afterwards.

Once the change had been accepted, the oversight continues via audits. There are two types of audits:

- regulatory audits, which verify that every change is covered by a safety case;
- documentary reviews, which verify the correctness of a safety case after the implementation of a change. They check the application of the ANSP's procedures and the relevance of risk-mitigation measures.

Since the details of a safety case are not within the scope of the audit, safety auditors are not safety analysts and they are not required to have safety assessment competence.

The NSA has three safety analysts based at its headquarters and another thirteen distributed regionally. They are considered to be competent enough to review all types of change. However, as part of the continuous improvement process, it is planned in the near future to set up a working group of active ATCOs to provide more operational knowledge for the review process. In addition, when an ATM change has an impact on aircraft or on-board procedures, assistance is requested from the NSA's flight operations department, whilst the help of the NSA's training and standards office is sought for ATM changes modifying the qualification and/or the training and qualification maintenance plans for ATS staff.

### 2.6.8 Example 8

ANSP units have to submit notification of each change and file safety cases or preliminary safety assessments with the centralised safety assessment unit. These documents give a brief description of the change, who is involved, the implementation process and a severity assessment if already available at this early stage. It was remarked that the latter is sometimes not included. There is some debate as to whether certain projects are changes or a continuation of previous changes. However, this matter has now almost been resolved.

The ANSP has a dedicated safety assessment team, which scrutinises the safety assessment/case performed/provided by the unit in order to ensure that the risk has not been under-evaluated. The safety assessment team may even visit the local units to review the risk. They may also support/advise local units on how to improve the quality of safety assessments. They are also in charge of the training dealing with safety assessment matters.

After notification, the NSA may decide to supervise the change in the framework of Regulation (EC) No 1315/2007. Such a decision is based on several criteria. When the NSA decides that a case warrants its acceptance, it will analyse identified hazards, safety assessment and risk mitigation measures amongst other things. It may accept a change subject to restrictions. In such cases, the matter is followed up either by the ANSP's HQ or its regional office.

The ANSP may delegate to the safety assessment team the supervision of a change. This is usually the case for major technical projects and for software assurance (ESARR 6 and Commission Regulation (EC) No 482/2008).

It was commented that in the past, some changes have been refused, which has led to controversy between the ANSP and the NSA. The NSA now attempts to find the right persons/expertise to avoid such situations. Often, there are lengthy detailed discussions, but this is considered to be healthy. If agreement is not reached, the matter may be referred to higher levels.

The ANSP pays great attention to the smaller changes in order to ensure that the system is not abused. It is felt that abuse would lead to more stringent oversight, thus requiring more assessment activities and documentation. This, in turn, would lead to additional cost.

**2.6.9 Example 9**

In view of the processes/procedures specified in the oversight framework, the NSA has a very good idea of how safety assessments are conducted and of any weaknesses (if any) in the system. All safety assessments, irrespective of the severity of the outcome, are subject to review by the NSA, although it is more interested in monitoring the implementation of safety recommendations than in the safety assessment.

The oversight framework specifies that the NSA gets a quarterly status report on all safety assessments, which consists of a summary of all new cases, ongoing ones, those which have been closed and those which have been classified as incomplete. It is actually the ANSP which labels an assessment as "Incomplete", and these are the ones where it is felt that the internal assessment could be improved. The initial internal oversight by the ANSP's own risk assessment team raises some concerns on these cases and refers them back to the units performing the safety assessment for clarification/additional work. At the same time an alert is sent to the NSA that an assessment has been flagged as Incomplete, and all relevant documents are forwarded to it. Incomplete cases are considered to be very serious, and it is considered essential that the NSA is alerted immediately, without waiting for the quarterly summary report.

Safety assessments are also conducted with respect to reorganisation, with emphasis on safety responsibilities of personnel and management functions.

The ANSP also provides services in another state. In this instance, the ANSP follows the second state's processes, and safety assessments are sent to the NSA of the second state. Consequently, the ANSP's manual specifies a slightly different process/procedure for safety assessments depending where the change is to be made. However, the internal change process is the same for both countries. In all cases, there is always an owner of the change. If the change is considered to have a significant safety impact, the ANSP's risk assessment team will assign a safety assessment specialist to take charge of the change assessment. This specialist is responsible for inviting the appropriate experts needed for the change assessment.

**2.6.10 Example 10**

Changes are notified by email to a group email address to ensure that all NSA staff are notified. This notification contains brief details of the proposed changes, including an assessment of their safety significance.

Where considered appropriate, in the case of complex significant changes, a pre-operational inspection is conducted using checklists specifically developed to review key items of interest. This inspection serves two purposes: it ensures that regulatory staff have the opportunity to familiarise themselves with the change

and it provides an opportunity to assess compliance against applicable regulatory requirements in advance of acceptance.

As part of the review, the NSA verifies both process- and product-related elements. The reviews aim to ensure that both the ANSP's SMS and its regulatory processes are being followed. In addition, the specific change details provided in the safety case are reviewed in order to ensure that adequate risk assessment and mitigation activities are being conducted to allow the NSA to accept the proposed change.

The decision to review will depend on a number of factors, including the complexity/scope/uniqueness of the change and the availability of appropriate NSA personnel. For example, a complex, multifaceted change requiring both technology and procedural changes may be subject to an acceptance process over several months (or years for a major new ATM centre re-equipment programme). For changes of more limited complexity or scale, an acceptance may be granted within three to four weeks. The NSA review generally results in comments being provided and/or requests for clarification on certain matters. The hazard analysis submitted with the safety case is also subject to review. As part of the review process, the NSA does cross checks on a sampling basis to ensure that no significant elements laid down in the provider's SMS are omitted from the safety case.

Once the NSA review has been completed and significant concerns have been resolved to the satisfaction of the NSA, a formal notification of acceptance is provided. Under agreed SMS processes, the ANSP provides the safety case in advance of the implementation date of the change.

In order to ensure that ANSPs clearly identify what constitutes a "safety-related change", the NSA imposes the additional requirement that organisations must have an internal procedure in their safety management manuals for notifying the NSA of all planned safety-related changes. It was felt that there may be some merit in providing (or making reference to) a consistent common definition for the term "safety-related change" (e.g. including reference to SAM, Part IV, Annex H What is a change?)

**2.6.11 Example 11**

All relevant NSA staff receive change notifications by email. One member of staff is assigned the task of ensuring that all such notifications are appropriately filed electronically. For changes subject to review, a lead contact person is assigned to ensure that the NSA reviews and provides comments in response to submitted safety cases.

The NSA accepts safety cases following a review of those submitted. A standard template is used to ensure that a consistent, formal acceptance is issued. The acceptance letter may include specific conditions and/or limits on use where this is considered necessary by the NSA.

The NSA intends to enhance its change oversight procedure in 2010 in order to include a set of guidance review checklists to assist in ensuring that a consistent and systematic review is conducted.

For specific major changes, the NSA endeavours to ensure that its staff obtains appropriate training prior to becoming engaged in the acceptance process. As an example, prior to the introduction of the A-SMGCS, one staff member received training which included the subject of multilateration systems. The NSA also endeavours to access certain equipment and in ATC procedures training courses which are specific to the selected changes. In general, a number of NSA staff with different skill sets review significant changes in order to ensure that a comprehensive review taking into account various considerations (e.g. ATC training and procedures, engineering training and procedures) is undertaken. It is accepted that it is not possible to be an expert in all areas, but the team-based approach has proven to be effective to date.

## 2.7 Competence assessment

Very little variation was noted in the states participating in this study on how competence assessments of ATCOs and ATSEPs are handled. In some states, where NSA is separated from the regulator, the licences/ratings/endorsements are issued/renewed by the regulator while the NSA concerns itself only with the oversight of the ANSPs' competency assessment process.

Most of the NSAs participate either directly or indirectly in ATCO competence assessment. In some states, the NSA has its own competence assessors, in others it nominates some of the ANSP's staff to act on its behalf as assessors. Some NSAs/NAAs ensure that one of their inspectors is always present at the final check of a new ATCO or when an ATCO gets a new rating/endorsement. In all states, the NSA/NAA then handles the formalities of reviewing assessment documentation and issuing the necessary licence/rating/endorsement.

NSA/NAA involvement in ATSEP competency differs from its involvement in ATCO competency. Perhaps this reflects the fact that whereas an ATCO licence is an ICAO Annex 1 requirement, no such requirement exists for ATSEPs. Often the NSA/NAA involvement in ATSEP competency is limited to ensuring that the ANSP has put in place a framework/process for ATSEP training (a programme/plan) and that these personnel are certified/authorised by the ANSP as being competent in accordance with a scheme which defines the necessary skills and competencies required on a given item of equipment, or how many engineers/technicians are needed, and ensures that sufficient competent staff are available. This certificate/authorisation is viewed as an acceptable means of compliance to Annex V to Regulation (EC) No 2096/2005. In some states, ANSPs ensure that ATSEPs also undergo a periodic medical check, either like the ATCOs or for some other period as specified in their ATSEP competency scheme.

In all states visited, the competency scheme is one of the areas most checked during oversight audits. Often, competency matters at the ANSP are dealt with by the respective operations and engineering divisions and the safety division is not involved. Within the operations and engineering divisions, it is line management which deals with competency matters, and they liaise directly with the NSA/NAA.

On the ANSP side, there are a variety of ATCO competence assessment methods. Some base their scheme on continuous assessment; others use a one-off competency check, while a few have a mixture of the two. The ATCO competency check may consist of a practical test (live traffic or a simulator) and/or a theoretical test (written or oral). All these schemes are accepted by the respective NSAs as being compliant with the European ATCO Directive[4] and ESARR 5. However, the application of different schemes could have an impact in a FAB context.

Exceptionally, in one state, both ATCOs and ATSEPs are licensed. Their competency schemes are different. ATCOs have ongoing evaluation together with a dedicated check once every two years. ATSEPs are examined every two years only. In the past, ATCO competency checks were carried out by the NSA. However, these are now carried out by ANSP assessors and examiners. The reports are then sent to the NSA. ATCO OJTIs and assessors are still examined by the NSA prior to having their endorsements issued and also to retaining them. ATSEPs, unlike ATCOs, are all still examined by the NSA.

4 Repealed by Regulation (EC) No 1108/2009 but transposed in all national legislation of EU member states.

## 2.8 Functional Airspace Blocks

Functional Airspace Blocks (FABs) have to be in place and operating by December 2012. However, lots of work still needs to be done. The states visited all had some political/legal agreement in place regarding the establishment of an FAB, but the progress on how to implement oversight varies from FAB to FAB.

Many organisations are citing lack of staff as their primary constraint in following up FAB matters. Another constraint mentioned was that in some states the NSA does not participate in FAB meetings because the state representative comes from the Ministry of Transport.

Observations on the oversight of Maastricht UAC were considered to be highly relevant to the matter.

### 2.8.1 Example 1 Maastricht UAC

Maastricht UAC provides en route services in the airspace of Belgium, Luxembourg, north-west Germany and the Netherlands. An NSA committee (NSAC) has been set up to conduct oversight. All the four states are represented and, in line with the SES regulations, the Netherlands chairs this committee. The NSAC has set up a dedicated Common Supervisory Team (CST), which specifies the audit process and draws up the audit/inspection programme. This programme is then approved by the NSAC. The CST is supported by the Audit Team and the Review Team, who are actually the persons who perform the audits.

The CST meets once every two months, mainly to:

- compose review teams;
- clarify problems/issues/constraints with the composition of these teams;
- monitor the progress of the review.

In addition, all changes (in terms of Regulation (EC) No 2096/2005) are notified to the CST Chairman.

In connection with the licensing of ATCOs, a Licensing Group has been established, and the Belgian NSA is responsible for licensing matters on behalf of all states. Since ATCO licensing was subject to a Directive and not a Regulation, the NSAC first conducted a gap analysis of the Directive as transposed into national legislation in the four states to ensure that there were no discrepancies.

The Four States have developed a dedicated oversight manual for MUAC.

### 2.8.2 Example 2

Regrettably, owing to shortage of staff, it is not possible for the NSA to attend all meetings, although they are all monitored. There are internal meetings on the matter, but the objective of such meetings is to ensure that everybody has the same level of knowledge about the project.

The interviewees were of the hope that many process and procedures would be streamlined across the members of the FAB.

### 2.8.3 Example 3

The ANSPs involved are working well and forging ahead. The respective regulators are also working well, but at a slower pace, particularly when it comes to updating/harmonising regulations. An example quoted was the ATCO Directive (reffer to footnote 4 above), where there are differences in its implementation in the different FAB countries.

Agreements at regulatory authority level have also been established, and now the work is focusing on reaching agreements at a lower level, particularly on common oversight and certification processes/procedures.

The NSA committee has been formed and is already putting things down on paper and getting some structure in place. At this stage, it is not possible to establish a common NSA, particularly owing to the number of small local ANSPs. It is planned to have joint audit teams to carry out FAB audits. It was felt that the FAB would be influenced significantly by the work done as part of a previous cooperation project between various ANSPs. The issue was raised of lack of resources, particularly of having persons dedicated solely to FAB work.

### 2.8.4 Example 4

Several standing committees have been established. The Safety Committee is active, holding regular meeting either physically or via WebEx. It has focused primarily on safety assessment and how to manage risk assessment of changes involving more than one (FAB) ANSP. The scope is now widening toward an FAB SMS. It has also proposed a notification process and the notion that if notification is acceptable to one

NSA, then it should be acceptable to all NSAs. Another proposal is for each ANSP to have only one focal point at the local NSA, which would then distribute to all other NSAs.

On a wider scale, the Safety Committee has regular contact and coordination with the NSA committee in order to ensure that targets meet the regulatory requirements.

In that connection, the NSA committee has, in conjunction with the Safety Committee, developed procedures for notification and review of changes in the FAB. There will be only one change leader, even if the change involves more than one ANSP. The leader will then notify his local NSA, which in turn will notify the other NSAs. The NSAs will then decide how the oversight tasks should be distributed amongst them.

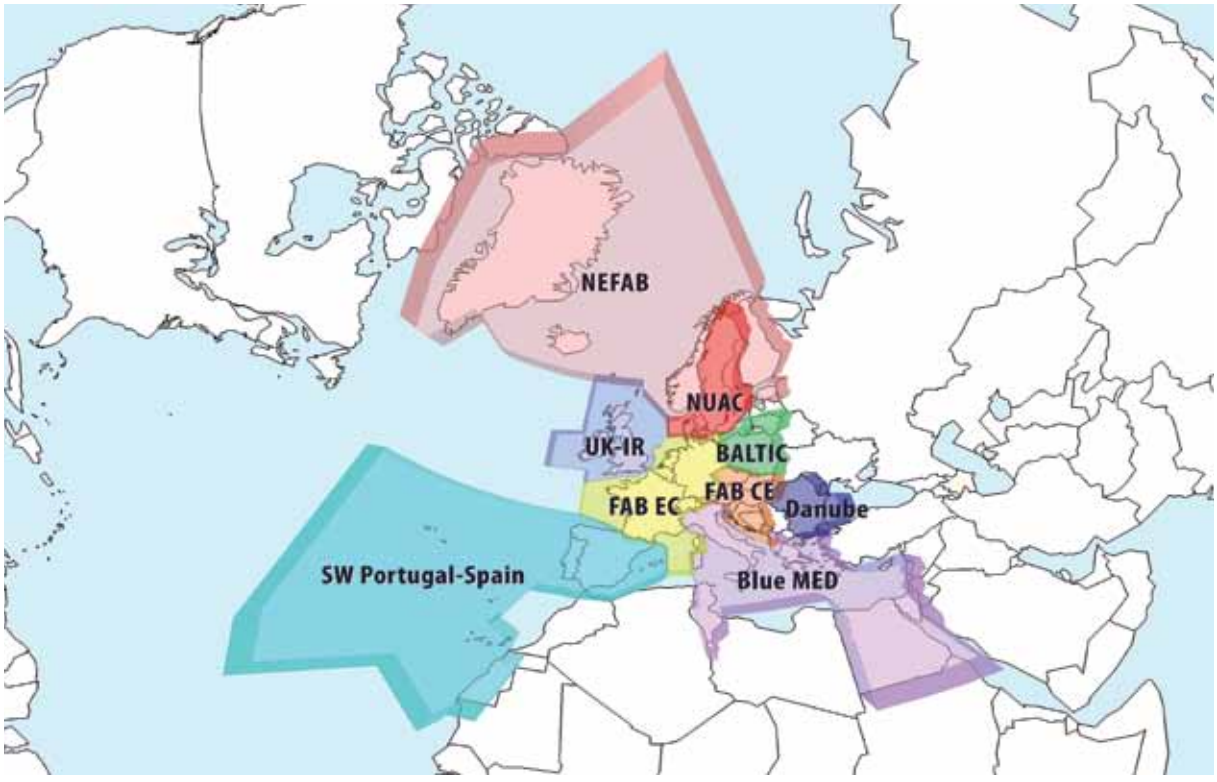
For the moment, severity is not to be included in the notification, as it has not been accepted by all ANSPs, but it is planned to review this process when more experience is gained with FAB assessments. Prior to this, there is still need to define a common method on how to assess severity.

**2.8.5 Example 5**

The FAB institutional structure has been defined and plans have been formulated. The planning phase is finished, but it is mostly run by ANSPs. Proposals have been put forward on how the regulators should organise themselves.

A FAB Agreement Drafting Group has been formed, and work started at the beginning of the year on how NSAs should handle the FAB matters. It has been proposed that first of all that the regulators should recognise one another's oversight process.

Three scenarios have been developed for this particular FAB. The first, the Static scenario, is for 2012, and is expected to bring early benefits from harmonised airspace classification. It was agreed that EUROCONTROL's Safety Assessment Methodology would form the basis of the FAB's harmonised safety assessment process.



# CHAPTER 3 – CONSIDERATIONS

During the course of the interviews, some of the participants raised several points where they felt that the interface could be enhanced. Implementing a national oversight programme is not something which can be done over night. It takes years of work, and along the way significant lessons are learned. One has to bear in mind that the interface implemented much depends on various factors, a notable one of which is local context.

A few of the organisations wished to share these lessons learned in order to avoid the difficulties encountered earlier. A number of considerations were directed either at the lack of regulatory guidance or at FAB questions.

The points mentioned in the interviews are summarised below. It should be noted that whilst most of these refer to observations on the interface between ANSP and NSA, there are some which fall outside the scope of this work. However, in the interests of completeness, the list contains all comments made by the interviewees:

- Greater harmonisation is necessary between NSAs to lead to better oversight of ANSPs. This was considered to be especially important for FAB matters. In time there would be also need for processes to be harmonised with adjacent FABs.
- The regulatory policy should be to ensure that regulation is effective rather than to check whether regulation exists. Over-regulation is actually less effective and often leads to just 'tick-in-the-box' exercises.
- Clear responsibilities and accountabilities within both the ANSP and the national regulatory authorities in the safety area is a key consideration. It was noted that in some cases, unclear responsibility for oversight, rulemaking and investigation, and the interrelation between these is a contributing factor towards a sub-optimal interface with the ANSP. This could also be affected by the ANSP's own safety culture.
- Given the difference in structure between NAA/NSA (state authority) and ANSP (corporatized), different view points exist on how safety can be addressed. Although safety is paramount and takes precedence over all other considerations, nobody welcomes unnecessary expense.
- There could be a risk of units being over-audited if there is a lack of coordination between the various audit plans (oversight, internal, ISO).
- Audits and evaluation of safety assessments can at times be subjective rather than objective. This situation is brought about by the background of the person conducting the check. Concern has been expressed on the effect which a change of personnel can have where no formal system has been established. A more uniform systematic approach is desired, although individual input is appreciated.
- Safety assessment of changes was highlighted as a key area where the interface could be enhanced. It was reported that a difference of interpretation between NSA and ANSP of the regulatory requirements led to significant debate.
- Another point regarding safety assessments was when the ANSP needs to submit the safety assessment for NSA acceptance. This did not question the severity requirement (as per Commission Regulation (EC) No 1315/2007) but rather at what stage the NSA needed the documentation in hand in order to be able to perform its evaluation of the change.
- Some ANSPs reported that the NSAs are not clear about what documents are needed for the review of safety-related changes and also how long their review takes.
- It was reported that in some cases, AAIB investigators either have a pilot background or are ex-ATCOs who left the service quite some time before. Consequently, AAIB safety recommendations at times either fail to address ATM questions or are based on old practices.
- Functional separation is viewed that it might present difficulties for the NSA in exercising its full authority vis-à-vis a sister unit of the same parent entity. Up to now, however, there has not yet been a case in which the NSA has needed to use its authority to sanction.
- Many organisations are continuing to cite lack of staff as their primary constraint in following up FAB matters.
- Another constraint mentioned is that in some states the NSA does not participate in FAB meetings because the state representative comes from the Ministry of Transport.

# PART II

# SELECTION OF GOOD PRACTICES IN INTERFACE BETWEEN ANSP AND NAA/NSA

# CHAPTER 1 – INTRODUCTION

## 1.1 Background

Part I of this report lists a large number of local practices on the interface between ANSPs and NSAs, reported by these organisations when they were interviewed on the matter in the period January to April 2010.

This work was strongly supported by the corresponding stakeholder advisory bodies in EUROCONTROL, i.e. the Safety Team (for the ANSPs), the Safety Regulation Commission (for the Regulators and NSAs) and at their joint meetings.

A number of these practices are expected to enhance considerably the maturity of the interface when shared and if applied at a Pan-European level.

A group of subject matter experts (SME) from both ANSPs and NSAs[5] met during two Workshops to define which of the collected practices described in Part I could be considered as valuable and worth sharing. They carried out an analysis based on a set of objective criteria and decided what constitutes good practices. The work done during the workshops was preceded and then followed by bilateral consultations.

Part II of this report is therefore a description of the work they have undertaken, resulting in a classification of the selected practices according to their significance and ease of application. A number of these practices can therefore be considered as best in class and are suitable for wider application in the ATM community.

## 1.2 Analyses of existing practices

### 1.2.1 Workshop I

The first workshop was held in October 2010 after the draft Report on Collection of Practices in Interface between ANSP and NSA (Part I of the report) had been reviewed by the Safety Team and Safety Regulation Commission.

The participating SMEs were from both ANSPs as well as NSAs and came from different sized organisations (large and small) while representing various business cultures across Europe.

The objectives of the workshop were:

- to draw a set of criteria to define what constitutes best practices;
- to analyse various existing practices described in the Part I of the Report; and
- to identify those practices which would improve the interface and promote a more mature relationship between NSAs and ANSPs[6], for dissemination and possible application to the European wide ANSP and NSA community.

The outcome of this workshop was that the SMEs, using expert judgement, made a first selection with the help of a web-based software application of those practices which looked as the most promising to be selected and/or further refined.

As the list of collected practices was quite lengthy it was decided that further review will be conducted remotely and then each area would be discussed through email exchange. Additionally it was deemed necessary to hold another workshop to go through the shortlisted practices.

It is worth mentioning that from both the ANSP as well as the NSA side, the SMEs showed a very high degree of commitment to sit together around the table and come forward with converging views.

Appendix 2 shows the documents used for initial selection.

The area ATCO/ATSEP competence was considered as not being a priority at this stage.

5 Appendix 1 shows a list of the experts involved in this activity.

6 During the Workshop, the UK CAA informed the participants about the work carried out in the UK to develop a maturity model to measure and improve the relationship between NSA and ANSP.

### 1.2.2 Workshop II

After the first Workshop and bilateral consultations, the input from the SMEs was analysed further, was consolidated, and a revised list of practices was drawn up for their' consideration. This revised list took into account the requests for clarifications, comments, recommendations and amendments which they had previously suggested.

The outcome of the second workshop, held in January 2011, was as follows:

- Several of the practices identified were revised in view of the experts' judgement to make them more suitable for wider application.
- The SMEs analysed the final selection and agreed to classify the revised practices according to a matrix with two elements: Significance and Ease of Application.
- Proposed dissemination of these good practices and their ranking, as described in detail in the following Chapter 2, to ST and SRC.

The subject matter experts wish to emphasise that the main issue remains the lack of staff, particularly at NSAs, their training and competence and adequate funds to address these shortcomings. Some of the good practices that were selected could provide a degree of mitigation for these shortcomings.

# CHAPTER 2 – SELECTED PRACTICES

## 2.1 Structure

The list of selected good practices has been divided into six areas[7]:

- Institutional arrangements (Organisation & NSA Staffing);
- Roles and responsibilities;
- Relationship ANSP/NSA;
- Safety Oversight Audits;
- Management of occurrence reporting and investigations;
- Safety Assessment of Safety-Related Changes.

The practices are shown in Tables 1 – 6 at the end of this Chapter. For clarity of purpose, the expected outcomes of each of these practices are explained at the beginning of the table. Each table consist of four columns:

- Ranking – indicating the significance of the practice and how easy is to implement it
- Practice – detailed word-picture of what to implement. These practices are derived from those described in the Part I. A number of them were revised by the experts to make them more suitable for wider application.
- Experts comments – hints and tips to take into account when implementing this practice
- Source – refers to the reported practice (as in Part I) from which the recommended practice has been derived.[8]

## 2.2 How to use selected practices

Prior to reading more about the selected practices, the reader of this report should carefully reflect on the following considerations:

- The identified existing practices may in some cases be appropriate for wider application while others work well only within a particular organisation, given its specific business culture, size etc. This means that a practice which works well within one organisation might be less successful in another, especially if the latter has a significantly different environment. Consequently these practices may require modification to fit other organisations.
- Based on a critical evaluation of the initial practice, the subject matter experts, using their knowledge, proposed amendments to render these local practices more suitable for wider application. The selection of practices in the tables below lists the modified practices.
- Additionally the experts provided hints that may help with the implementation of such practices (see Experts Comments column). Still one size may not fit all and, therefore, the decision to adopt any of these good practices should be subject to careful consideration and evaluation.
- Several of the identified practices stem from regulatory requirements while other are improvements which make it easier to meet regulations. To facilitate implementation the experts used two criteria: significance and ease of application.
- Some of the advanced practices may seem daunting at first. This is due the fact that they require the prior implementation of basic practices.
- Furthermore, several of these practices cannot be applied in isolation because they need a solid foundation of other simpler/basic practices. Implementation of these basic practices is one of the preconditions which are necessary to implement practices which are giving outstanding results in more advanced organisations.
- Finally, it should be noted that there is no guarantee that implementation of any given practice will lead to good or improved interfaces between ANSP and NSA in a certain environment. It is the shared opinion of the experts that the listed practices have the potential to be effective and there is a good chance that implementing them may well show improvements.

---

7 Competency was not considered as priority area and FAB issues are taken into account when analysing individual practices.

8 When summarising practices to facilitate the discussion at the Workshop the aim was to capture the salient points from the examples gathered during the interviews, thus not every paragraph has a practice associated with it. Also this avoided repetition of similar observations. The review of the practices further reduced the inventory, and a number of selected practices have only a trace of the original (see second bullet of 2.2).

## 2.3 Ranking

Practices are classed according to two criteria - Significance and Ease of Application with each criterion split into three levels.

**Significance**
The first level of Significance has been defined as '**Important**'. Such practices are considered as elementary and essential and have significant effect on the quality of day-to-day performance leading to a proper interface between ANSP and NSA. They could be essential in the context of FABs.

All practices that reflect a regulatory requirement[9] have been automatically ranked as 'Important'.

'**Relevant**' practices are outstanding ones that are highly effective in enhancing maturity. They assist in driving forward to real progress and achieving targets which in the beginning may seem to be daunting. They also could be a great asset in the context of FABs.

The third level is the '**Limited**' practice. Often these are practices that have evolved to address a particular situation in an individual state. Although this practice might be an outstanding solution for this state, attempts to transpose it more widely would need to take into account a considerable number of conditions amongst which are size, culture, safety maturity and availability of resources.

**Ease of Application**
'**Easy**' practices could be relatively straightforward to apply and could be used by all organisations, irrespective of their size, structure, available resources, expertise, culture and/or level of safety maturity, and these are also applicable in a FAB context. Such practices have the potential for quick and timely results often leading to a 'Quick Win'.

A '**Viable**' practice while relatively straightforward in its application may require a few resources for implementation and/or its application may need more discussion between the various parties. It may take some time for the results to become apparent but the benefits should be reaped in due course. Viable practices can still have broad application and could ease implementation in FABs.

Practices are classed as '**Challenging**' when a number of preconditions need to be fulfilled such as maturity and coordination/discussion at various levels both internally and externally. Implementation can take time because it depends on the commitment, availability of funds and adequately trained and competent staff.

The criteria explained above, i.e. "Significance" and "Ease of Application", can be put into a classification matrix as follows.

| | | Easy | Viable | Challenging |
|---|---|---|---|---|
| 1 | Important | A1 | B1 | C1 |
| 2 | Relevant | A2 | B2 | C2 |
| 3 | Limited | A3 | B3 | C3 |
| | | A | B | C |

Practices ranked in the green area are, in the opinion of the experts' panel, those to be considered first, due to their significance and potential ease of application[10], then progressively moving through the yellow and orange areas.

The practices listed in Tables 1 - 6 in chapter 2.4 use the above classification.

9 ICAO, ESARRs and/or EU Regulation, as appropriate.

10 Rank C1 is colored green to reflect its importance even though it may be challenging to apply.

## 2.4 Selection of Good Practices

### INSTITUTIONAL ARRANGEMENTS (ORGANISATION & NSA STAFFING)

Expected outcome of implementing these practices would be to achieve proportionality i.e. to have sufficient and necessary resources to realize the required safety outcomes andor benefits. These practices reinforce NAA/NSA independency and its mandate to enforce the required actions in the interest of public safety.

The key attributes arising from the following practices could be summarised as:

- proportionality;
- independency;
- mandate to enforce;
- adequate resources;
- training and competence of staff;
- processes and procedures.

Note: These attributes arise not only from implementing the practices listed below, but are main criteria for all the practices listed.

**Table 1: Institutional Arrangements (Organisation & NSA Staffing)**

| | | Easy | Viable | Challenging |
|---|---|---|---|---|
| 1 | Important | A1 | B1 | C1 |
| 2 | Relevant | A2 | B2 | C2 |
| 3 | Limited | A3 | B3 | C3 |
| | | A | B | C |

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **1.1** | B1 | NSA formulates and implements mandatory training requirements (initial and recurrent) for its staff. | Required to comply with ESARR 1/ Commission regulation (EC) No 1315/2007. | Part I, Chapter 2.1.2, Para 5 |
| **1.2** | B1 | NSA organises for its staff, on a systematic basis and as part of their training, mandatory periodical workshops/courses on new rules, new approaches, good practices and sharing of lessons learned. | | Part I, Chapter 2.1.2, Para 6 |
| **1.3** | C1 | NSA able to generate additional funds to finance the increase of staffing levels, or other operational costs, either through CRCO charges, special levies, cost recovery or a combination of any of these measures to enable independent financing/staffing. | | Part I, Chapter 2.1.1, Para 3 |
| **1.4** | C1 | Sharing auditors/specialists between NSAs on a local or regional basis, e.g. in a FAB context. | In addition to the sharing of individual auditors/specialists, this practice could also be used to set up a pool of experts as mentioned in EC Regulation 2096/2005, Article 9.2.<br>This practice may assist to address:<br>❍ staff shortage at NSA, and/or<br>❍ lack of competent NSA staff in particular specialised field. | Part I, Chapter 2.1.2, Para 7 |

**Table 1: Institutional Arrangements (Organisation & NSA Staffing) (cont'd)**

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **1.5** | C2 | Secondment of ANSP staff to NSA for a short period to do projects on regulatory tasks. | Formal arrangements are necessary to:<br>❍ avoid conflict of interest,<br>❍ protect the interest of all parties,<br>❍ maintain confidentiality. | Part I, Chapter 2.1.2, Para 3 |
| **1.6** | C2 | Secondment of ANSP staff to NSA to assist them temporarily until NSA has recruited appropriate staff themselves. | Formal arrangements are necessary to:<br>❍ avoid conflict of interest,<br>❍ protect the interest of all parties,<br>❍ maintain confidentiality. | Part I, Chapter 2.1.2, Para 3 |
| **1.7** | B3 | ANSP trains/coaches NSA staff either by having NSA staff working for a limited period at the ANSP or ANSP trainers work as OJTIs at NSA. | This practice may assist to:<br>❍ address staff shortage at NSA, and/or<br>❍ improve ATM competence of NSA staff.<br><br>Formal arrangements are necessary to:<br>❍ avoid conflict of interest,<br>❍ protect the interest of all parties,<br>❍ maintain confidentiality. | Part I Chapter 2.1.2, Para 4 |

## ROLES AND RESPONSIBILITIES

Purpose is to reinforce the attributes arising from those as per area "Institutional arrangements" and have clear idea of what needs to be done, by whom and when.

The key outcome arising from the following practices could be summarised as:

- smooth and timely set-up;
- clear distinction between the respective safety roles of the ANSP and NSA;
- avoiding ambiguity.

### Table 2: Roles and Responsibilities

| | | Easy | Viable | Challenging |
|---|---|---|---|---|
| 1 | Important | A1 | B1 | C1 |
| 2 | Relevant | A2 | B2 | C2 |
| 3 | Limited | A3 | B3 | C3 |
| | | A | B | C |

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **2.1** | A1 | Explicit and systematic application of ANSP/NSA interface processes and procedures. | The application of the processes requires clearly defined processes/procedures. Therefore, this practice can be considered as "compliance" or "implementation" of the "framework" from Practice 2.3. | General comment |
| **2.2** | B1 | Clearly defined safety accountabilities and responsibilities where appropriate of each individual in NSA and ANSP. | Just defining safety accountabilities and responsibilities does not ensure results, these have to be exercised and put into everyday use. | Part I, Chapter 2.2, Para 8 |
| **2.3** | C1 | Manual/regulatory framework describes the deliverables expected and timing, where required, from the ANSPs and NSAs, and includes processes showing the information flow between the two parties. Such a manual/framework will be understandable, agreed and implemented by both sides. | Although such a manual/framework should make the process/procedures/flows clearer, care is needed to ensure not to add to the administrative burden and not to slow down the work.<br>Implementation is essential because such a document is not only for show. | Part I Chapter 2.2, Para 4,5,6 |
| **2.4** | C1 | Explicit internal distribution of the responsibilities and clear communication procedures within National Aviation Authorities, not only NSA, but also links to other bodies e.g. Rulemaking, AAIB, Economic Regulator and Military. | Just distributing responsibilities does not ensure results, these have to be exercised and put in everyday use.<br>While it is easy to develop the agreement, it might take some time. The diverse local arrangements in place may render it hard to reach the necessary agreement. | Part I Chapter 2.3, Para 1 |

## RELATIONSHIP ANSP/NSA

The purpose adopting these practices is to have greater trust, more respect and better understanding between ANSP and NSA.

The key attributes could be summarised as:

- mutual trust;
- both parties know what is happening;
- both parties know what is going to happen;
- clear view of respective roles and responsibilities.

**Table 3: Relationship ANSP/NSA**

| | | Easy | Viable | Challenging |
|---|---|---|---|---|
| 1 | Important | A1 | B1 | C1 |
| 2 | Relevant | A2 | B2 | C2 |
| 3 | Limited | A3 | B3 | C3 |
| | | A | B | C |

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **3.1** | B1 | Plan and implement regular meetings at various hierarchical levels between NSA and ANSP at strategic and technical level, with commonly agreed agenda and purpose. | | Part I, Chapter 2.3.1, Para 1 |
| **3.2** | B1 | Joint NSA-ANSP interface (person-to-person, working groups as appropriate) when required to deal with specific safety issues (arising from safety audits, safety occurrences, safety assessment of change etc.). | | General comment |
| **3.3** | B1 | Manual/Processes/Procedures of oversight communicated to ANSP(s) by NSA. | | General comment |
| **3.4** | C1 | Detailed and agreed National Regulatory Framework or Manual which clearly specifies links with external Agencies, e.g. ANSP, Military units, other national aviation bodies. | While easy to develop, achieving full agreement might take some time. | Part I, Chapter 2.3, Para 2 |
| **3.5** | C1 | Implement Safety Programme at the state level as required by ICAO, as well as by EU Regulation for EU member states. | | General comment |
| **3.6** | C1 | Impact assessment is performed on proposed regulation and reviewed, subject to national institutional arrangements, by rulemaking/ oversight functions and ANSP(s). | This is very important so as to present a balanced view to the rule-making body. If not done sufficiently and effectively at the early stages, it might result in inefficiency when implemented later. | Part I, Chapter 2.3.1, Para 11 |
| **3.7** | C1 | NSA should have a quality management system in place to ensure proper application and understanding of processes and lead to continuous improvement. | | Part I, Chapter 2.3, Para 3 |

**Table 3: Relationship ANSP/NSA (cont'd)**

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **3.8** | C1 | The national law mandates that all the information obtained from the ANSPs is confidential and cannot be divulged to other parties without prior ANSP agreement. | | Part I, Chapter 2.3.2, Para 8 |
| **3.9** | B2 | Formal interface for regulatory requirements of ANS provision. Identified specialist/single point of contact should be nominated by each side. | Both parties could exchange a list of experts clearly indicating their respective responsibilities. | Part I, Chapter 2.3.2, Para 1 |
| **3.10** | B2 | Oversight accountabilities and competencies distributed between NSA personnel to ensure that each area is covered in the necessary detail and to identify substitutes when the main focal person is not available. | This would be the outcome of a QMS for NSA as well. | General comment |
| **3.11** | B2 | NSA has its own confidentiality regulations (Code of conduct) and its staff are fully aware of them. | | Part I, Chapter 2.3.2, Para 8 |
| **3.12** | B2 | NSA organises workshops/awareness sessions to assist ANSP(s) in implementation of requirements and to share experience. | It is particular importance where in a state there are number of ANSPs, particularly small ones. | Part I, Chapter 2.3, Para 10 |
| **3.13** | B2 | Informal contact between ANSP and NSA staff, in particular at technical level, may be helpful. | Does not replace formal processes and contact but eases communication to improve understanding and trust. However it should not undermine individual accountabilities on both sides. | General comment |
| **3.14** | C2 | Coordinated policies/requirements between the various NAAs/NSAs/Ministries to avoid contradictory instructions to ANSP(s). | | General comment |
| **3.15** | C2 | Regulatory appeal process is available in case that ANSP does not agree with NSA interpretations/ instructions. | | Part I, Chapter 2.3.1, Para 9 |
| **3.16** | C2 | NSA, as the authority responsible for safety, supports and facilitates coordination between ANSP and other government authorities, when required or requested by the ANSP. | This is a good support function that the NSA can provide to ANSPs. | General comment |
| **3.17** | B3 | A limited number of NSA staff have controlled access to ANSP's document management system. Time is saved in this way as these persons could check directly for information needed without resorting to formal requests. | The NSA has to exercise this privilege with care because it has direct access to third party documents.<br>Can have serious implications (Intellectual property rights/ commercial). Hence there needs to be absolute trust from ANSP that confidentiality will be respected by the NSA.<br>May result in the NSA assuming part of the ANSP's responsibility to manage safety. | Part I, Chapter 2.6.3, Para 4 |

## SAFETY OVERSIGHT AUDITS

The purpose of adopting these practices is to have effective and relevant audits while avoiding duplication of work to reduce unnecessary burden on service provider(s) as well as the NSA.

The key attributes could be summarised as:

- consistent;
- open;
- risk based;
- documented;
- planned.

### Table 4: Safety Oversight Audits

| | | Easy | Viable | Challenging |
|---|---|---|---|---|
| 1 | Important | A1 | B1 | C1 |
| 2 | Relevant | A2 | B2 | C2 |
| 3 | Limited | A3 | B3 | C3 |
| | | A | B | C |

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **4.1** | A1 | NSA coordinates timing and content of audit plan with ANSP. | | General comment |
| **4.2** | A1 | NSA Annual audit plan distributed beforehand. | | Part I, Chapter 2.4, Para 2; Chapter 2.4.2, Para 1 |
| **4.3** | A1 | Audit planning process specifies deliverables (audit plan) and timeframes for submission of the required information which is then communicated to the ANSP. | | Part I, Chapter 2.4.7, Para 1 |
| **4.4** | A1 | It is the responsibility of the NSA to confirm every corrective action and its ultimate implementation date and to enforce if the date is not met, but the setting of the corrective action/date should be achieved in mutual agreement with the ANSP. | | Part I, Chapter 2.4.3, Para 2 |
| **4.5** | B1 | Audit planning (periodical, annual) follows a risk-based approach taking into account factors such as size, criticality, level and complexity of traffic handled, culture, history of non compliance and NSA's confidence in the unit's/organisation's safety maturity. | The results of the safety culture survey and the safety maturity survey can be used as well. | Part I, Chapter 2.4, Para 6 |
| **4.6** | B1 | Audit Plan should be flexible enough to permit amendments (e.g. time, availability of personnel, etc.) to accommodate the needs/constraints of both the NSA and the ANSP(s). | | Part I, Chapter 2.4, Para 3 |

| Table 4: Safety Oversight Audits (cont'd) | | | | |
|---|---|---|---|---|
| **No** | **Rank** | **Practices** | **Experts Comments** | **Source** |
| **4.7** | B1 | Categorising non-conformities by urgency, to identify the main areas of concerns, i.e. safety risks that need to be solved first. | This does not mean that non-conformities/observations such as document editions, updates, typos, etc. should/could be ignored; it is just that they are not highest priority. | Part I, Chapter 2.4, Para 1 |
| **4.8** | C1 | Audits should look at the steady state and at changes, whilst at the same time, looking for continuous improvement. | | Part I, Chapter 2.4, Para 5 |
| **4.9** | B2 | Proper application of the safety management processes by the ANSP leads to improved internal monitoring at the ANSP and may result in increased confidence by NSA and less frequent oversight interventions. | NSA might reduce its oversight interventions if it has high confidence and strong assurance that the ANSP internal monitoring ensures that robust SMS processes are in use. | General comment |
| **4.10** | B2 | NSA ensures that ANSP has planned to implement means to allow verification during the operational life of the system that the safety objectives and requirements are met. | Safety assurance after the safety-related change is considered to be part of the safety case. Safety indicators might be defined by ANSP before the implementation of the change. These indicators will be monitored afterwards. This could be part of ANSP Safety Management Manual. | Part I, Chapter 2.6.7, Para 6 |
| **4.11** | C2 | Oversight is the responsibility of several NSA personnel nominated as 'account-holders' (focal points) for different areas. They are ATM specialists, who collect all the information related to their particular areas and forward it to the specialist NSA staff as necessary. | This practice:<br>❍ could be related to the NSA internal organisation (e.g. distribution of accountabilities/responsibilities) and availability of staff;<br>❍ is particularly relevant for FABs. | Part I, Chapter 2.4.1, Para 1 |
| **4.12** | C2 | Joint auditing teams having ATS, CNS and Airports background, leading to audits that are wider in scope but at less frequent intervals (resulting in less disruption). | It is important to undertake oversight at minimum inconvenience to ANSP.<br><br>This practice could be related to the NSA internal organisation (e.g. distribution of accountabilities/ responsibilities) and availability of staff. | Part I, Chapter 2.4.4, Para 1 |

## MANAGEMENT OF OCCURRENCE REPORTING AND INVESTIGATIONS

The purpose of adopting these practices is to have robust reporting system with timely investigations, as necessary, based on just culture principles and clear responsibilities for the implementation and verification of safety recommendations.

The key attributes could be summarised as:

- clarity;
- harmonised (FABs, states where there is more than one ANSP, NAA/NSA/AAIB);
- consistent;
- open (just culture);
- timely;
- completeness;
- feedback.

Note: Some of the comments received were with respect to the interface between AAIB/ANSP/NSA. Consequently some of these practices are addressed to the AAIB.

**Table 5: Management of Occurrence Reporting and Investigations**

| | | Easy | Viable | Challenging |
|---|---|---|---|---|
| 1 | Important | A1 | B1 | C1 |
| 2 | Relevant | A2 | B2 | C2 |
| 3 | Limited | A3 | B3 | C3 |
| | | A | B | C |

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **5.1** | A1 | Clearly defined list of reportable occurrences based on existing regulation and agreed between all relevant parties. | This is essential to be formalised in a FAB context. | Part I, Chapter 2.5, Para 2 |
| **5.2** | A1 | Direct feedback as appropriate from AAIB to NSA and ANSP on investigation reports. | ANSP and NSA need to know of unsafe situation as soon as possible. For EU states this is now a requirementprescribed in Commission Regulation (EC) No 996/2010. | Part I, Chapter 2.5, Para 3 |
| **5.3** | A1 | All reportable occurrences from ANSPs, aircraft and airport operators are sent to a dedicated address. | Several methods are available e.g. email, automatic reception/action process. | Part I, Chapter 2.5.1, Para 1 |
| **5.4** | A1 | Use of RAT (Risk Analyses Tool). | Training is necessary to ensure consistency of application of RAT.<br><br>For EU States RAT is part of the IR on Performance (Commission Regulation (EU) No 691/2010). | Part I, Chapter 2.5 |
| **5.5** | B1 | Clear notification procedure for reportable occurrences is agreed between relevant parties (e.g. ANSP/NSA/AAIB) and formalised in appropriate manual/procedures. | | General comment |

**Table 5: Management of Occurrence Reporting and Investigations (cont'd)**

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **5.6** | B1 | It is defined which authority (i.e. AAIB, NSA) is responsible for following-up on the implementation of AAIB safety recommendations. | For EU states it is prescribed in Commission Regulation (EC) No 996/2010. | Part I, Chapter 2.5, Para 3. |
| **5.7** | B1 | AAIB invites discussion on draft report from all parties addressed in this report to ensure factual accuracy. | For EU states it is prescribed in Commission Regulation (EC) No 996/2010. | General comment |
| **5.8** | B1 | Agreement between ANSP/NSA for ANSP to achieve effective report classification according to a pre-defined methodology. | RAT can be used to solve any issues on classification of severity, and this is very important in the FAB context. For EU States RAT is part of the IR on Performance (Commission Regulation (EU) No 691/2010). | Part I, Chapter 2.5.7, Para 2 |
| **5.9** | B1 | The AAIB safety recommendations are sent to NSA who in turn forwards them to ANSP to formulate an appropriate answer. The ANSP and NSA then discuss the proposed answer between them. | Care is necessary not to render the practice too complex as this could lead to a lack of transparency and could also impact on the speed of processing. In view that the shortest communication paths are the best, it is recommended that the AAIB safety recommendations addressed towards the ANSP are sent directly to the ANSP but the NSA should be informed of them. | Part I, Chapter 2.5.7, Para 3 |
| **5.10** | C1 | AAIB and NSA have issued to the ANSPs a joint statement guaranteeing the confidentiality of occurrence reporting. | | Part I, Chapter 2.5.6, Para 5 |
| **5.11** | A2 | Occurrence reports are sent to the NSA though accidents and serious incidents need to be reported in parallel to the AAIB. | | Part I, Chapter 2.5.3, Para 1 |
| **5.12** | B2 | All reportable occurrences from ANSPs are automatically forwarded to the appropriate oversight personnel. | Oversight personnel may not be involved in investigation and can use this information only to have better knowledge of the current state of ANSP.<br>Such reporting is to be in line with Just Culture principles. | Part I, Chapter 2.5.1, Para 1 |
| **5.13** | C2 | To avoid duplication of work the ANSP's database is linked to the NSA's database (e.g. ECCAIRS). AAIB/EASA could also have controlled access to the NSA database to further reduce duplication. | | Part I, Chapter 2.5.7, Para 3 |
| **5.14** | C3 | NSA has its own ATS investigators to look into those incidents which do not attract the attention of the AAIB. | This practice could be related to the NSA internal organisation and requires resources to have independent investigator(s). | Part I, Chapter 2.5, Para 4<br>Chapter 2.5.2, Para 5 |

**Table 5: Management of Occurrence Reporting and Investigations (cont'd)**

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **5.15** | C3 | During analyses NSA investigators not only look at the occurrences themselves but also at the NSA processes to identify effectiveness of the oversight process. | This practice is a natural follow-up from the previous one (No. 5.14).<br>A systematic approach to look into the effect of oversight would be of help. | Chapter 2.5.2, Para 5 |
| **5.16** | C3 | NSA mandate that the ANSP investigates in more detail if it is felt that the initial internal investigation did not go into sufficient depth. | Mandate is contrary to a robust NSA/ANSP relationship. However, the intent behind this practice has some validity although it is more appropriate for the NSA to request or to ask for such an investigation providing adequate justification for its doubt on the initial report.<br>The NSA has to ensure that an ANSP investigates adequately to identify fully all causal factors and put in place effective corrective measures to minimise the risk of a repeat occurrence.<br>In case that the NSA remains unsatisfied with the effectiveness of the internal investigation it should organise an independent investigation. | Part I, Chapter 2.5, Para 4 |

## SAFETY ASSESSMENT OF SAFETY-RELATED CHANGES

The purpose of adopting these practices is to have better understanding of each other roles and to have appropriate resources consistent with level (risk) of change.

The key attributes relevant for this area could be summarised as:

- timely;
- both parties aware of risk;
- consistency;
- independence (separation);
- efficiency.

Note: When we speak of changes we are referring of changes as defined in ESARR 4 and Commission Regulation (EC) No 2096/2005.

**Table 6: Safety Assessment of Safety-related Changes**

| | | Easy | Viable | Challenging |
|---|---|---|---|---|
| 1 | Important | A1 | B1 | C1 |
| 2 | Relevant | A2 | B2 | C2 |
| 3 | Limited | A3 | B3 | C3 |
| | | A | B | C |

| No | Rank | Practices | Experts Comments | Source |
|---|---|---|---|---|
| **6.1** | A1 | Changes are subject to safety planning appropriate to the level and complexity of the change. | This safety plan should be part of the overall project plan for the change and part of the safety assessment process anyway, and not solely for NSA purposes.<br>It has to be clear that it is not because the changes are to be reviewed that they require safety plans, but because the review will be easier if there is a safety plan. | Part I, Chapter 2.6.7, Para 6 |
| **6.2** | A1 | A focal point for changes subject to review is nominated both at the ANSP as well as at the NSA. | | Part I, Chapter 2.6.5, Para 2 |
| **6.3** | A1 | NSA and ANSP agree on a coordination plan based on an ANSP project plan to formalise the framework of the review of the safety case/ assessment. | | Part I, Chapter 2.6.7, Para 7 |
| **6.4** | A1 | The NSA/ANSP coordination plan for the review of the safety case/assessment identifies deliverable dates ('acceptance limit point'). | | Part I, Chapter 2.6.7 |
| **6.5** | A1 | A standard form for acceptance has been developed. In cases of conditional acceptance/ non-acceptance the form would list the findings. | In the case of a conditional acceptance it is essential that the form also lists the positive findings in order that the ANSP avoids repeating what has already been done correctly. | Part I, Chapter 2.6.2, Para 3 |

| Table 6: Safety Assessment of Safety-related Changes (cont'd) | | | | |
|---|---|---|---|---|
| **6.6** | A1 | NSA provides to ANSP written and detailed justification for the non-acceptance of safety assessment reports. | In a well-established relationship, things should not reach this stage. | Part I, Chapter 2.6.2, Para 3<br>Chapter 2.6.5, Para 6 |
| **6.7** | A1 | Change can be accepted subject to safety actions being undertaken after acceptance. | These safety actions could afterwards be overseen by the NSA through the continuous safety oversight. | Part I, Chapter 2.6.7, Para 5 |
| **6.8** | B1 | NSA has formal procedures, agreed with the ANSP, describing the process for notification and acceptance of safety-related changes. On the other hand ANSP has a formal safety assessment process in its SMS that includes the requirement, when applicable, to inform the NSA of all relevant safety-related changes.<br>These procedures/processes are to be harmonised. (e.g. scope, timing of notification, timing of review, content, level of assurance, interaction between both parties). | | Generic comment |
| **6.9** | B1 | Changes are subject to audit after implementation and when the system is mature to see evidence/products/results. | | Part I, Chapter 2.6.3, Para 3 |
| **6.10** | B1 | NSA carries out on-going oversight of changes (audit). | Such a check could look into conditions of acceptance, safety assurance activities. | Part I, Chapter 2.6.1, Para 1<br>Chapter 2.6.3, Para 3 |
| **6.11** | C1 | Methodology for safety assessments is proposed by ANSP and accepted by NSA. | Might be difficult in FAB context;<br>Ideally in a FAB the methodology for safety assessment is proposed and agreed by all ANSPs in the FAB and accepted jointly by all the NSAs in this FAB. | Part I, Chapter 2.6.2, Para 1 |
| **6.12** | C1 | NSA staff with appropriate skill sets will review significant changes to ensure a comprehensive review taking into account different considerations. | Requires the NSA to have sufficient resources because there are constraints on resources/ competences.<br>NSAs need to respect that ANSPs are in a far better position to manage safety than the NSAs. Appropriate balance is needed regarding NSA trust in ANSP because there might be a danger of NSAs going into too much detail and assuming part of the ANSP's responsibility to manage the safety of the service provided. | Part I, Chapter 2.6.11, Para 3 |

| Table 6: Safety Assessment of Safety-related Changes (cont'd) | | | | |
|---|---|---|---|---|
| **6.13** | A2 | The notification and reporting of changes to the NSA is achieved via a standard template based on drawn up after discussion and agreement of both parties. | | Part I, Chapter 2.6.2, Para 2 |
| **6.14** | A2 | ANSP notification, containing brief details of the proposed changes and including an assessment of their safety significance, is distributed internally by NSA to ensure all appropriate NSA staff is notified. | Internal distribution could be via a group email address. | Part I, Chapter 2.6.10, Para 1 |
| **6.15** | A2 | For complex or significant changes, a pre-operational check is conducted using checklists specifically developed to review key items of interest. | It is important that a check is done but different methods may be used i.e. not limited to checklists, but could also include e.g. ad hoc meetings, audit, targeted inspections. | Part I, Chapter 2.6.10, Para 2 |
| **6.16** | B2 | NSA has a set of guidance review criteria to assist in ensuring a consistent and systematic review is conducted. | Checklist(s) could be one of the methods used. | Part I, Chapter 2.6.11, Para 3 |
| **6.17** | B2 | Organisational changes are also assessed for their safety impact, particularly to ensure that all safety accountabilities have been allocated appropriately. | This is actually not a regulatory requirement, but it is an excellent idea to do so and should be in the ANSP SMM. | Part I, Chapter 2.6.1, Para 3 |
| **6.18** | B2 | For specific changes subject to review, the NSA endeavours to ensure that its staff obtains appropriate knowledge prior to becoming engaged in the acceptance process. | NSA should not be an expert but needs enough knowledge to assess the change.<br><br>Training is not always possible/ available (e.g. new technology, operational procedures, human performance) although this training might be necessary from the NSA's side to meet Art 9 of EC1315/2007.<br><br>Such training should not be a limiting factor on the implementation of the change.<br><br>Where ANSP is introducing bespoke change(s)(e.g. airspace) it should allow NSA access to simulations, trials, etc. | Part I, Chapter 2.6.11, Para 3 |
| **6.19** | B2 | When the change is a complex project, the NSA is involved throughout the whole life-cycle and it nominates representatives to attend the various meetings. | This is one of the aspects of the review coordination plan. | Part I, Chapter 2.6.3 Para 2 |
| **6.20** | B2 | For complex projects there are regular meetings to check if the NSA requires more information and to ensure that the information provided is satisfactory. | | Part I, Chapter 2.6.2, Para 5 |

| Table 6: Safety Assessment of Safety-Related Changes (cont'd) | | | | |
|---|---|---|---|---|
| **6.21** | B2 | For complex projects a report is sent to the NSA at the end of each safety assessment phase. The NSA should comment appropriately or these reports. | This is one of the aspects of the review coordination plan.<br>After reviewing the report NSA could issue letter of no objection. | Part I, Chapter 2.6.5, Para 1 |
| **6.22** | B2 | Low-risk changes do not have to be subject to the change acceptance process. However NSA should periodically audit/check a selection of changes. | Oversight should be proportionate to risk and available resources. | Part I, Chapter 2.6.3, Para 1 |
| **6.23** | C2 | Safety assessment related activities are performed by a specialised NSA team, which includes the NSA focal point/account holder for this area. | This practice could be related to the NSA internal organisation (e.g. distribution of accountabilities/ responsibilities) and requires the NSA to have sufficient resources. | Part I, Chapter 2.6.4, Para 1 |
| **6.24** | A3 | Low-risk changes may be notified to the NSA by using periodic reports. | The notification process is to be agreed between ANSP and NSA. | Part I, Chapter 2.6.2, Para 5 |
| **6.25** | C3 | ANSP provides a list of future changes, say those planned for the coming three years. This is assessed by a change implementation group having representatives of e.g. civil/military NSA, ANSP(s), Ministry of Transport, and Ministry of Defence. | This might be a good practice on a local level for the NSA to calibrate its resources, particularly if ANSP is implementing innovative measures that might require changes to present regulation. | Part I, Chapter 2.6.4 Para 3 |
| **6.26** | C3 | The oversight framework specifies that the NSA get a quarterly status report on all safety assessments which consist of a summary of all new cases, ongoing ones, those closed and those that had been classified by ANSP as Incomplete (i.e. where the internal assessment could be improved). | This practice has its valid point but may result in increased workload both for ANSP and NSA, particularly in those cases where these are small organisations. | Part I, Chapter 2.5.9, Para 2 |
| **6.27** | C3 | Local regulatory procedure describes roles and responsibilities when more than one service provider (e.g. Airport + ANSP on taxiway works), is involved and service providers need to identify who is responsible for the change. | Care is necessary to ensure that the involved service providers assess the impact of the change on their part of the service provision. Communication is essential between two providers to ensure that they reach similar conclusions with respect to the overall safety objectives of the change. | Part I, Chapter 2.6.6, Para 1 |

# APPENDICES

# APPENDIX 1
# CONTRIBUTORS - DATA COLLECTION (PART I)

Note: Contributors are listed in alphabetical order by state. This does not reflect any order of hierarchy. Designations and job titles are as on the date of contribution.

**Austria**

**AUSTROCONTROL**
Mr Artner Werner, Head of Safety and Quality Management Department

**CAA-Federal Ministry for Transport, Innovation and Technology**
Mr Franz Nirschl, Deputy Director Air Navigation Services

**Cyprus**

**Department of Civil Aviation – ANSP**
Mr Nicos Nicolaou, Chief Operations Officer
Mr Haris Antoniades, Senior Air Traffic Control Officer - ACC
Mr Evangelos Antonopoulos, Air Traffic Control Officer - Safety Office

**Department of Civil Aviation – NSA**
Ms Panayiota Georgiou-Demetriou, Senior Air Traffic Control Officer

**Denmark**

**NAVIAR**
Mr Lars Bech Madse, Deputy Director
Mr Steen Halvorsen, Director Safety & Quality
Mr Dan Dreijer Andersen, Head of Investigation
Mr Robert Strauss, Risk Manager

**CAA-Aerodromes and Air Navigation Services Department**
Mr Ryan Sorensen, Safety Inspection Department
Ms Kirsten Sonderby, Chief Inspector
Mr Knud Rosing, Chief Inspector

**France**

**DSNA**
Mr Nicolas Dubois, Head of Safety, Quality and Security Management
Mr Stephane Deharvengt, Deputy Head of Safety, Quality and Security Management

**DSAC/ANA**
Mr Thomas Levecque, Head of Air Navigation Service Provider Certification Office
Mrs Louise-Yvette Buard, Head of ATM Safety and Interoperability Unit

**Germany**

**DFS**
Mr Hans-Juergen Morscheck, Director Corporate Safety & Security Management
Dr Franz Kern, Head of Safety Assessment and Risk Management
Mr Heino Kuester, Head of Safety & Security Monitoring
Mr Volker True, Senior Expert Corporate Safety & Security Management

**National Air Traffic Services Supervisory Authority**
Mr Juergen Luhmann, National Air Traffic Services Supervisory Authority

**Greece**

**Hellenic Civil Aviation Authority**
Ms Anna Kouvaritaki, Safety Expert, Safety Management Office - Area Air Navigation Department

**Ireland**

**Irish Aviation Authority**
Mr Thomas V. Regan, Assistant Director Regulatory Performance and Personnel Licensing

**Portugal**

**NAV Portugal**
Mr Antonio Guerra, DSEGOP/SEGNA

**INAC**
Mr Francisco Balaco, Director of Aerodromes and Air Navigation
Mr Carlos Abreu, Head of Air Navigation Department
Mr Jose Salgueiro, Head of Flight Safety Department
Mrs Ines Salgueiro, Analyst, Flight Safety Department

**Romania**

**ROMATSA**
Mr Voinea Florin Gunta, Acting Director Safety & Quality

**Romanian Civil Aeronautical Authority**
Ms Claudia Virlan, Director General
Mr Liviu Bunescu, Director ANS Supervision Directorate
Ms Cristina Caliga, ANS Supervision Directorate, Standards and Regulations for ANS Office

**Spain**

**DGAC**
Mr Juan Manuel Gallardo Gonzalez, Director of GNSS Programme

**Switzerland**

**Skyguide**
Mr Simon Maurer, Chief Safety Officer

**Federal Office of Civil Aviation**
Mr Christoph Regli, Head of Section
Ms Laure Noelle Maret, Expert Oversight ANS

**The Netherlands**

**LVNL**
Mr Job Bruggen, Safety Director

**Inspectorate for Transport, Public Works and Water Management (IVW)**
Mr Robert Van Dorp, Civil Aviation Administration
Mr Jos Nollet, Civil Aviation Administration

**Ukraine**

**State Aviation Administration**

Mr Dmytro Babeichuk, Deputy Chairman of SAA
Mr Sergey Borzenets, Head ATM Safety Regulation Division
Mr Andrii Fediakov, Chief Expert ATM Division, Acting Head of Division

**UkSATSE**

Mr Olexandr Katrych, Head of Internal Control and Audit Inspectorate
Mr Vitaliy Bezmal, Head of Safety Assessment Division
Mr Konstantin Shvets, Head of Information & Safety Performances Analysis Division
Mr Ivan Butsyk, Head of ATS Control Division
Mr Volodymyr Holnyii, Head of CNS Control Division

**United Kingdom**

**NATS**

Mr Robert Granville, Head of Safety Management
Ms Hazel Courteney, Head of Safety Strategy & Performance
Mr John Holmes, Head of System Safety
Mr Giles Pateman, Head of Quality
Mr Steve Tafe, Safety Manager Swanwick and Head of System Safety

**Safety Regulation Group**

Mr Harry Daly, Head of Strategy and Standards, Air Traffic Standards Division

**EUROCONTROL**

**Maastricht Upper Area Center**

Mr Keith Cartmale, Safety Manager MUAC

# APPENDIX 2
# CONTRIBUTORS - SELECTION OF PRACTICES (PART II)

Note: Contributors are listed in alphabetical order by state. This does not reflect any order of hierarchy. Designations and job titles are as on the date of contribution.

**Austria**

**AUSTROCONTROL**
Mr Artner Werner, Head of Safety and Quality Management Department

**CAA-Federal Ministry for Transport, Innovation and Technology**
Mr Franz Nirschl, Deputy Director Air Navigation Services

**Czech Republic**

**Air Navigation Services**
Mr Svatopluk Halen, Head of Safety and Quality Department

**France**

**DSAC/ANA**
Mr Frank Giraud, Air Navigation Service Provider Certification Office
Mr Laurent Chapeau, Deputy Head of Office, ATM Safety Assessment and Interoperability Unit

**Germany**

**DFS**
Mr Hans-Jürgen Morscheck, Director Corporate Safety and Security Management

**Greece**

**Hellenic Civil Aviation Authority**
Ms Anna Kouvaritaki, Safety Expert, Safety Management Office - Area Air Navigation Department

**Italy**

**ENAV S.p.A.**
Mr Alberto Iovino, Operational Safety, Report and Communication

**Ireland**

**Irish Aviation Authority**
Mr Adrian Mahony, Manager ANSD/ASD

**Lithuania**

**Oro Navigacija**
Mr Pavel Petrov, ATS Safety Manager, ATM Safety & Quality Management Division

**The Netherlands**

**Inspectorate for Transport, Public Works and Water Management (IVW)**
Mr Jos Wilbrink, Senior officer International Affairs, Civil Aviation Authority
Mr Robert Van Dorp, Civil Aviation Authority

**Ukraine**

**State Aviation Administration**
Mr Dmytro Babeichuk, Deputy Chairman of SAA

**UkSATSE**
Mr Vitaliy Bezmal, Head of Safety Assessment Division
Mr Konstantin Shvets, Head of Information & Safety Performances Analysis Division

**United Kingdom**

**NATS**
Mr Robert Granville, Head of Safety Management

**Safety Regulation Group**
Mr Chris Peart, Head ATS Operations

**EUROCONTROL**

**Maastricht Upper Area Center**
Mr Keith Cartmale, Safety Manager MUAC

# APPENDIX 3
# WORKING PAPERS WORKSHOP I

## A3.1 Scoring Guidance

**CRITERIA**

- Achieving effective&quick results/speed of processing - refers to achieving expeditiously effective results relative to the complexity of the action;
- Proactive involvement of both parties – refers to coordination and consensus on actions to be done, including common position in international representation/meetings/initiatives;
- Improved level of communication - refers to ease communication in day to day activities leading to better understanding between two parties;
- Transparency of procedures & safety documentation - refers to dissemination and accessibility of key procedures on safety oversight and frank discussion of areas requiring improvement leading to increased trust and confidence;
- Balance of frequency of meetings - means meetings to the depth as necessary and when required for better utilisation of time and effort;
- Consistency in working practices-sustainability - refers to systematic and objective application of practices/processes/procedures;
- Ease for pan-European application – refers to the potentiality of immediate dissemination and usage of practice for pan-European application (particular relevance to the FAB activities).

**SCORING**

**Perfect fit**
Outstanding practice, meets perfectly all relevant criteria, ready for immediate pan-European dissemination. (100%)

**Very relevant**
Very Good practice, but there are some small preconditions or some small comments to be taken into consideration for its implementation and/or this practice should be, and can easily be optimised further with assistance of EUROCONTROL into a best practice (please explain what you want to be optimised, using 'comment' box). (75%)

**Relevant**
Not a bad practice, but there are quite some preconditions or constraints to be taken into consideration before it can be implemented more widely; if requested by the participants however, this practice might be developed further into a best practice (please explain what you want to be developed and/or optimised, using 'comment' box). (50%)

**Limited effect**
There are a lot of preconditions to be fulfilled for this practice to be implemented by others; not considered to be worked any further. (25%)

**Almost no effect**
Local practice which is not considered to be disseminated further. (10%)

**HINTS FOR SCORING**

Look at these hints when scoring the practice against the criteria.

### Effect

- the effect on compliance of the ANSP (do you think this best practise will help to ensure long term compliance by the ANSP with the applicable rules); and/or
- the effect on safety (do you think this best practise will contribute to a safer sky).

### Efficiency

Do you think this best practise will:

- reduce the workload of the NSA; and/or
- reduce the burden on the ANSP of proving compliance (administrative and during the audit), all without reducing the risk of non compliance; and/or
- reduce the costs for the airlines.

### Quality

Do you think this best practise will contribute to a better quality of:

- The oversight activity (audit/inspection): Will the ANSP be satisfied with the quality/professionalism of the activity performed;
- The report to the ANSP: Will the ANSP be satisfied with the quality/professionalism of the report sent to him (quality of the finding: Is it really important, do I know as a ANSP why it is a non conformity, does the ANSP know what is expected of him).

## A3.2 Initial list of practices

The tables below show the summary of the practices as initially ranked via web-based software application. This initial ranking was reviewed by the subject matter expert to achieve the final list shown in Part II of the report. Rank is expressed as normalised account of the results from individual reviewers.

N. B. These tables are only for illustration purposes because after the further review the criteria of selection was upgraded. Additionally some of the practices shown below were amended to ease the application.

| Synthesis of the total results – Institutional arrangements | |
|---|---|
| Clear definition of processes and procedures, training programs, understanding and awareness. | 1,000 |
| NSA organise for its staff mandatory periodical workshops/short courses dealing with new rules, new approaches, good practices and sharing lessons. | 0,841 |
| NSA put in place mandatory training requirements (initial and recurrent) for its staff, including training programme. | 0,782 |
| Training/coaching of NSA staff by ANSP by having NSA staff working for a limited period at the ANSP, or ANSP trainers working as OJTI at NSA. | 0,752 |
| Secondment of ANSP staff to NSA to perform regulatory tasks. | 0,679 |
| Sharing auditors/specialists between NSAs on local or regional basis. | 0,628 |
| NSA ability to generate their own funds either through CRCO charges, special levies, cost recovery or a combination of any of these measures to enable independent financing/staffing. | 0,559 |

| Synthesis of the total results – Roles and responsibilities | |
|---|---|
| Explicit and systematic application of interface processes and procedures. | 1,000 |
| Specified deliverables expected from ANSP and processes that show the information flow between two parties described in manual/regulatory framework, understood and agreed by both parties. | 0,972 |
| Clearly defined safety roles and responsibilities of each individual in NSA and ANSP. | 0,971 |
| Clear internal distribution of the responsibilities within National Aviation Authorities, not only NSA, but also links to Rulemaking, AAIB, Economic Regulator and Military, and their internal communication. | 0,894 |
| Proper application of the safety management processes by the ANSP leading to increased confidence by NSA and less frequent oversight interventions. | 0,875 |

| Synthesis of the total results – Relationship ANSP/NSA | |
|---|---|
| Regular meetings at strategic and technical level. | 1,000 |
| Detailed National Regulatory Framework or manual which clearly specifies links with external Agencies, e.g. ANSP, Military units other national aviation bodies. | 0,960 |
| Informal contacts as necessary, in particular at technical level. | 0,969 |
| Manual of oversight communicated to ANSPs. | 0,882 |
| Joint NSA ANSP working group dealing with specific safety issues. | 0,885 |
| Coordinated policies/requirements between the various NAAs/Ministries. | 0,788 |
| Impact assessment of new /amended regulation (review by both rulemaking and oversight side as well as ANSP). | 0,832 |
| Safety Programme at the state level. | 0,750 |
| NSA organise workshops/awareness sessions for small organisations to assist in implementation of requirements and sharing experience. | 0,732 |
| Formal interface at all regulatory requirements. Single point of contact. | 0,748 |
| NSA facilitate/coordinate between ANSP and other government authorities (Military, Communication, Economic, etc.). | 0,613 |
| Escalation process in case that ANSP does not agree with NSA interpretations / instructions. | 0,581 |
| Distribution of oversight tasks split between NSA personnel to ensure that each area is covered in the necessary detail. | 0,568 |
| QMS at NSA. | 0,496 |
| NSA has its own confidentiality regulations (Code of conduct) and their staff is made aware of them. | 0,467 |
| The national law mandates that all the information obtained from the ANSPs is confidential and cannot be divulged to other parties. | 0,394 |

| Synthesis of the total results - Safety oversight audit | |
|---|---|
| NSA coordinate audit plan with ANSP. | 1,000 |
| Annual audit plan distributed beforehand. | 0,903 |
| Audit planning process specifies deliverables (audit plan) and timeframes for submission of the required information. | 0,881 |
| Plan flexible enough to permit amendments to accommodate the needs/constraints of both the NSA and ANSP(s). (Time, availability of personnel, etc.). | 0,881 |
| Audits are based on criticality and confidence in the unit's safety maturity. | 0,809 |
| Audit plan based on history of non compliance and compliance culture of the ANSP. | 0,779 |

| Synthesis of the total results - Safety oversight audit (cont'd) | |
|---|---|
| Categorising non conformities by importance to identify the main areas of concerns (without effort being used to address minor issues, e.g. document editions, updates, typos, etc.). | 0,768 |
| Audits planned based on size, level and complexity of traffic (periodical, annual). | 0,734 |
| Joint auditing teams having ATS, CNS and Airports background, wider in scope but less frequent audits conducted at units (leading to less disruption). | 0,645 |
| Oversight is performed by several NSA personnel nominated as 'account-holders' (focal points) for different areas. They are ATM specialists who collect all the information related to their particular areas and forward to the specialist NSA staff as necessary. | 0,636 |
| Availability and use of standardised checklists/tools to meet increasing number of regulatory requirements. | 0,606 |
| Audits look at the steady state as well as changes while, at the same time, looking for continuous improvement. | 0,580 |
| NSA delegate some of the oversight activities to an independent audit unit within an ANSP. | 0,559 |
| NSA set target dates for the completion of corrective actions. | 0,557 |
| Targeted inspections are undertaken prior to the NSA acceptance of specific changes. | 0,539 |
| NSA "joint venture" with the body that ISO certified the ANSP. | 0,515 |
| Conducting ad-hoc inspections. | 0,374 |

| Synthesis of the total results – Management of occurrence reporting and investigation | |
|---|---|
| Clear notification procedure for reportable occurrences agreed between relevant parties (ANSP/NSA/AAIB) and formalised in appropriate manual/procedures. | 1,000 |
| Clearly defined list of reportable occurrences. | 0,973 |
| It is defined which authority is (i.e. AAIB, NSA) is responsible for follow-up on the implementation of AAIB safety recommendations. | 0,957 |
| Direct feedback from AAIB to NSA and ANSP on investigation reports. | 0,915 |
| Common database AAIB, NSA. | 0,909 |
| To avoid duplication of work the ANSP's database is linked to the NSA's ECCAIRS. | 0,904 |
| All occurrence reports from ANSPs, aircraft and airport operators are sent to a dedicated email address and are automatically forwarded to the appropriate oversight personnel. | 0,894 |
| Agreement with ANSP to do the classification according to a pre-defined methodology. | 0,892 |
| ANSP staff has facility to file a report and send this direct and confidentially to the NSA. | 0,868 |
| The AAIB safety recommendations sent to NSA who in turn forwards them to ANSP to formulate an appropriate answer. The ANSP and NSA then discuss the proposed answer between them. | 0,867 |
| Occurrence reports are sent to the NSA though accidents and serious incidents need to be reported in parallel to the AAIB. | 0,858 |

| Synthesis of the total results – Management of occurrence reporting and investigation (cont'd) | |
|---|---|
| AAIB and NSA have issued to the ANSPs a joint statement guaranteeing the confidentiality of occurrence reporting. | 0,827 |
| NSA has its own ATS investigators to look into those incidents which do not attract the attention of the AAIB. | 0,663 |
| NSA mandate that the ANSP investigates in more detail if it is felt that the initial internal investigation did not go into sufficient depth. | 0,623 |
| Use of RAT (Risk Analyses Tool). | 0,593 |
| NSA may select events of significant interest and ask for ANSP analysis and actions. If the situation so warrants, the NSA may impose on ANSP to conduct further analysis of a particular incident(s). | 0,591 |
| Under national Law the ANSP is obliged to provide technical support/expertise to the AAIB. The ANSP and AAIB have a bilateral formal agreement on the use of these ANSP personnel. | 0,475 |
| During analyses ATS investigators not only look at the occurrences themselves but also at the NSA processes to identify any possible shortcomings in the oversight. | 0,472 |
| AAIB could ask for copies of ANSP investigation reports and has the authority to change the severities assigned by ANSPs in view that the AAIB has more sources of data, including military, available to them. | 0,323 |

| Synthesis of the total results – Safety assessment of safety-related changes | |
|---|---|
| ANSP has a formal safety assessment process in its SMS, including the requirement to inform the NSA of all changes and notification right from project start. | 1,000 |
| NSA has formal procedure describing the process for notification and acceptance of changes. | 0,955 |
| ANSP methodology includes all the necessary steps e.g. notification, processes for Minor/Major Changes, timeframes and interaction with the NSA (subject of acceptance by NSA). | 0,936 |
| Methodology for safety assessments is proposed by ANSP and accepted by NSA | 0,892 |
| When the change is a big project, the NSA is involved throughout the whole life-cycle and it nominates representatives to attend the various meetings. | 0,880 |
| The notification and reporting about changes to the NSA is done via a standard template based on drawn up after discussion and agreement of both parties. | 0,805 |
| NSA provides to ANSP proper justification for the rejection of safety assessment reports. | 0,805 |
| For big projects there are regular meetings to check if the NSA requires more information and to ensure that the information provided is satisfactory. | 0,804 |
| NSA has a set of guidance review checklists to assist in ensuring a consistent and systematic review is conducted. | 0,802 |
| A focal point for each change, particularly large ones, is nominated both at the ANSP as well as at the NSA. | 0,770 |
| NSA draws coordination plan to formalise the framework of the review of the safety case. In addition the coordination plan identifies deliverable dates ('acceptance limit point'); | 0,729 |
| Local regulatory procedure describes roles and responsibilities when more than one service provider (e.g. Airport + ANSP on taxiway works), is involved and service providers need to identify who is responsible for the change. | 0,723 |
| A standard form for acceptance has been developed. In cases of partial acceptance /non-acceptance the form would list the negative findings. | 0,716 |
| ANSP provide a list of changes planned for the coming three years. This is assessed by a change implementation group having representatives of e.g. civil/military NSA, ANSPs, MoT, Ministry of Defence. | 0,667 |

| Synthesis of the total results – Safety assessment of safety-related changes (cont'd) | |
|---|---|
| ATM changes subject to review require a detailed Safety Plan. | 0,664 |
| For major changes a report is sent to the NSA at the end of each safety assessment phase. The NSA can accept or otherwise these reports. | 0,662 |
| The oversight framework specifies that the NSA get a quarterly status report on all safety assessments which consist of a summary of all new cases, ongoing ones, those closed and those that had been classified by ANSP as Incomplete (i.e. where the internal assessment could be improved). | 0,637 |
| Notification, containing brief details of the proposed changes including an assessment of their safety significance, is sent by email to a group email address to ensure all NSA staff is notified. | 0,635 |
| Safety assessment related activities are performed by a specialised NSA team, which includes the NSA focal point/ account holder for this area. | 0,617 |
| Organisational changes are also assessed for their safety impact, particularly to ensure that all safety accountabilities had been reassigned to the new posts/positions | 0,599 |
| A limited number of NSA staff has unrestricted access to ANSP's document management system. Time is saved in this way as these persons could check directly for information needed for acceptance without resorting to formal requests. | 0,594 |
| NSA carries out on-going oversight of changes (audit) | 0,592 |
| NSA ensures that ANSP has the processes to manage the risks and the tools to fix them. | 0,589 |
| NSA staff with different skill sets will review significant changes to ensure a comprehensive review taking into account different considerations | 0,579 |
| Change can be accepted subject to safety actions being undertaken after acceptance | 0,572 |
| For complex significant changes, a pre-operational inspection is conducted using checklists specifically developed to review key items of interest. | 0,551 |
| Small changes are reported to the NSA by using monthly reports. | 0,549 |
| Safety assurance after the change is considered to be part of the safety case. NSA ensures that ANSP has planned to implement means allowing verification during the operational life of the system that the safety objectives and requirements are met. Safety indicators might be defined by ANSP before the implementation of the change. These indicators will be monitored afterwards. | 0,542 |
| Changes are also subject to audits after implementation and when the system is mature to see evidence/products/ results | 0,533 |
| NSA conducts occasional visits to the ANSP and audit/check a selection of small changes. | 0,527 |
| For specific major changes the NSA endeavours to ensure that its staff obtains appropriate training prior to becoming engaged in the acceptance process. | 0,501 |
| NSA has a working group of active ATCOs to provide more operational knowledge to the review process. | 0,495 |
| NSA also endeavours to access certain equipment and ATC procedures training courses specific to selected changes. | 0,481 |
| NSA relies solely on the ANSP's declaration where the change is highly technical (e.g. software issues) and the NSA lacks in-house expertise in this matter. | 0,425 |
| Small changes are not subject to the change acceptance process. | 0,417 |

# ABBREVIATIONS

| | |
|---|---|
| **AAIB** | Aircraft Accident Investigation Bureau |
| **ACC** | Areal Control Centre |
| **ALP** | Acceptance Limit Point |
| **AMC** | Acceptable Means of Compliance |
| **ANS** | Air Navigation Service |
| **ANSP** | Air Navigation Service Provider |
| **AOB** | Any Other Business |
| **APP** | Approach Control Service |
| **A-SMGCS** | Advanced Surface Movement Guidance and Control System |
| **AST** | Annual Summary Template |
| **ATC** | Air Traffic Control |
| **ATCO** | Air Traffic Controller |
| **ATM** | Air Traffic Management |
| **ATS** | Air Traffic Services |
| **ATSEP** | Air Traffic Safety Electronics Personnel |
| **ATSU** | Air Traffic Services Unit |
| **CA** | Corrective Action |
| **CANSO** | Civil Air Navigation Services Organisation |
| **CEO** | Chief Executive Officer |
| **CNS** | Communication, Navigation, Surveillance |
| **CRCO** | Central Route Charges Office |
| **CST** | Common Supervisory Team |
| **DG** | Director General |
| **DGCA** | Directorate General of Civil Aviation |
| **EAPPRI** | European Action Plan for the Prevention of Runway Incursions |
| **EASA** | European Aviation Safety Agency |
| **EC** | European Commission |
| **ECCAIRS** | (EC) European Coordination Centre for Aircraft Incident Reporting Systems |
| **ESARR** | EUROCONTROL Safety Regulatory Requirement |
| **FAB** | Functional Airspace Block |
| **IANS** | (EUROCONTROL) Institute of Air Navigation Services |
| **ICAO** | International Civil Aviation Organisation |
| **ISO** | International Standards Organisation |
| **IT** | Information Technology |
| **MET** | Meteorological Service |
| **MOR** | Mandatory Occurrence Reporting (Scheme) |
| **MoT** | Ministry of Transport |
| **MUAC** | Maastricht Upper Area Centre |
| **NAA** | National Aviation Authority |
| **NSA** | National Supervisory Authority |
| **NSAC** | NSA Committee |
| **OPS** | Operations Room/Division |
| **QMS** | Quality Management System |
| **RAT** | Risk Analysis Tool |
| **SAM** | (EUROCONTROL) Safety Assessment Methodology |
| **SES** | (EC) Single European Sky (legislation) |
| **SESIS** | (EUROCONTROL) SES Implementation Support |
| **SME** | Subject Matter Expert |
| **SMS** | Safety Management System |
| **SR** | Safety Recommendation |
| **SSC** | (EC) Single Sky Committee |
| **SSP** | (ICAO) State Safety Programme |
| **TWR** | Aerodrome Control Service (Tower) |
| **UAC** | Upper Area Control Centre |