

FINAL STAKEHOLDER WORKSHOP

Study on Common Requirements for the Provision of Air Navigation Services

Brussels
15th October 2003

*This document is confidential and is intended solely for the use and
information of the client to whom it is addressed.*



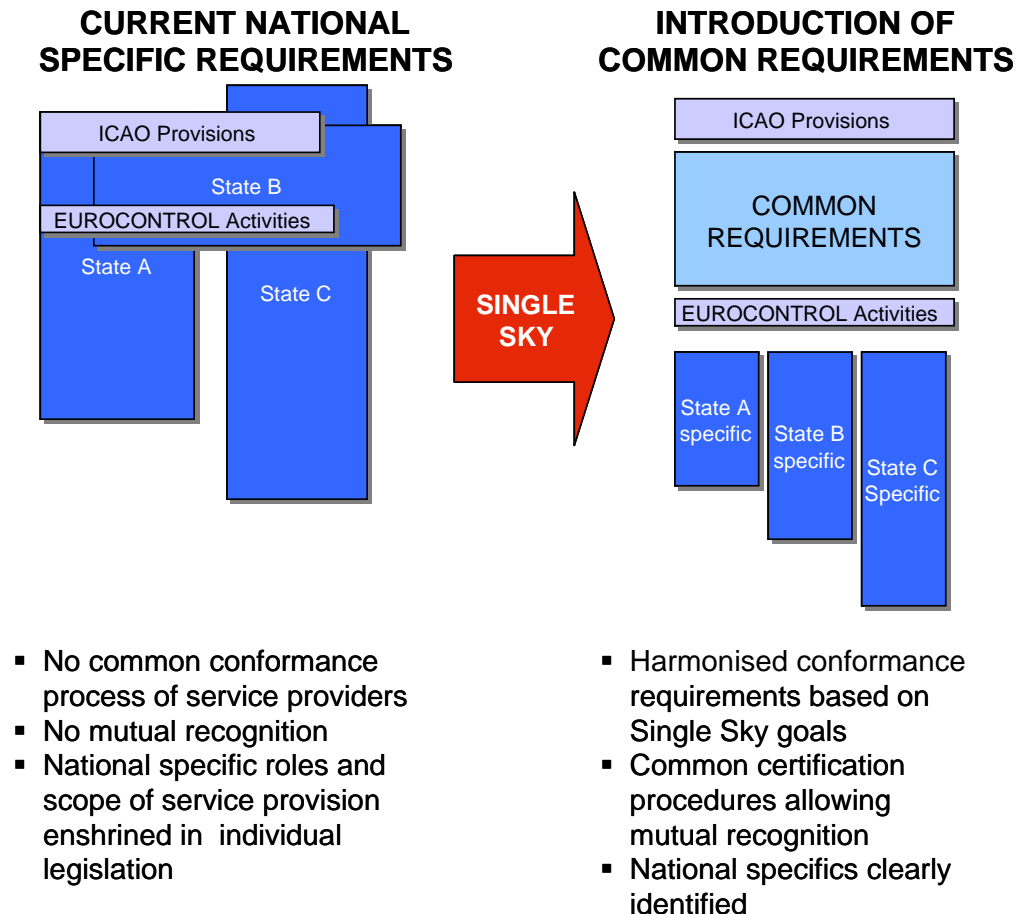
Booz | Allen | Hamilton

Table Of Contents

- ▶ Overview of Study
- ▶ Definition and Application of Common Requirements
- ▶ Overview of Common Requirements
- ▶ Recommendations for Operational Data



The overall purpose of the study has been to define Common Requirements to assist in creating a 'level playing field' ...a common certification system for ANS provision



- ▶ Common Requirements should:
 - allow the uniform application of service provision
 - enable mutual recognition of ANSPs across Member States
 - allow providers of services to be chosen to best meet the requirements of any given airspace, irrespective of national boundaries
- ▶ Common Requirements are to be **generic** with Community-wide applicability...
- ▶ ...to be clearly distinguished from any local specific conditions required of an ANSP by a Member State for designation



To achieve this the study was conducted across 3 phases of activity, over period of eight months

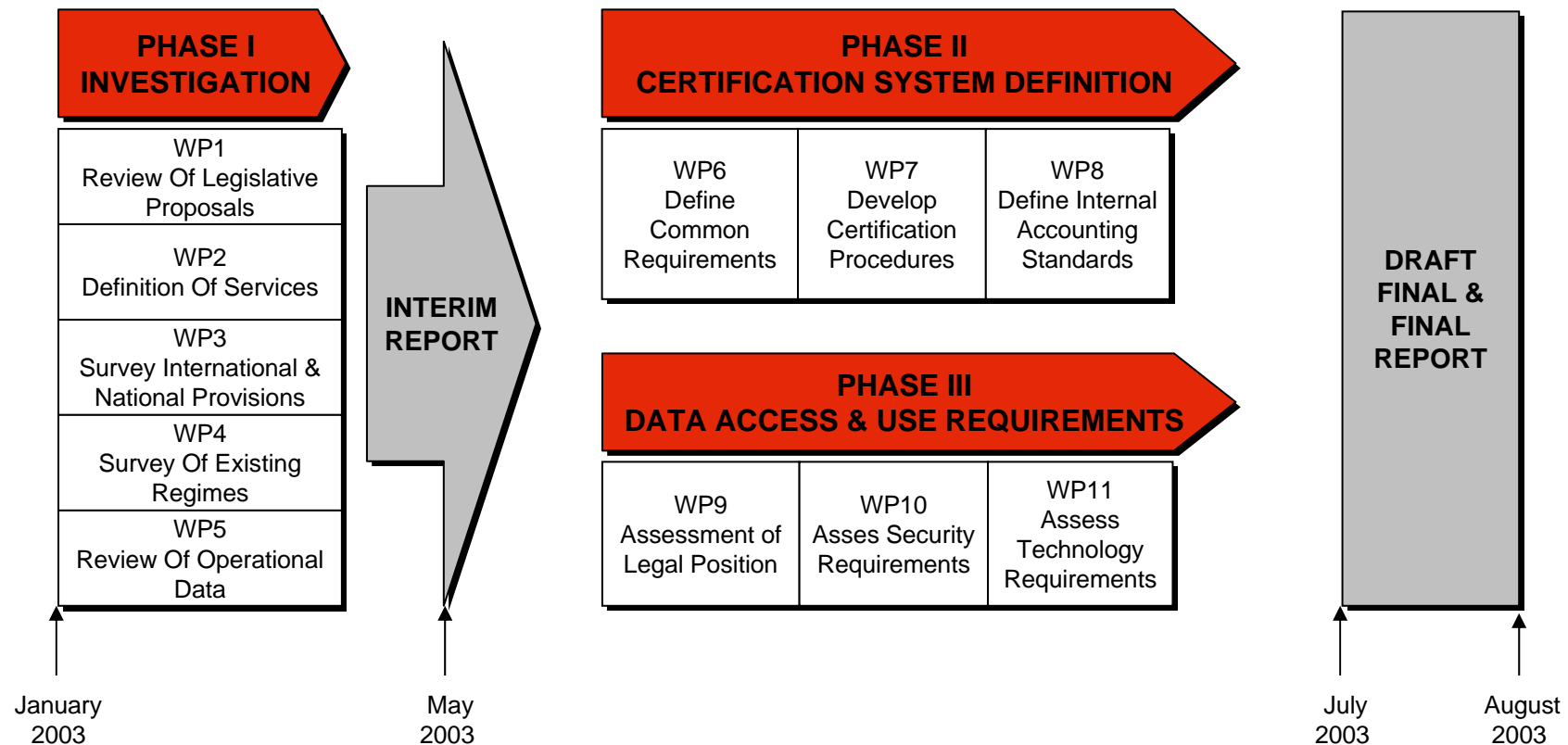
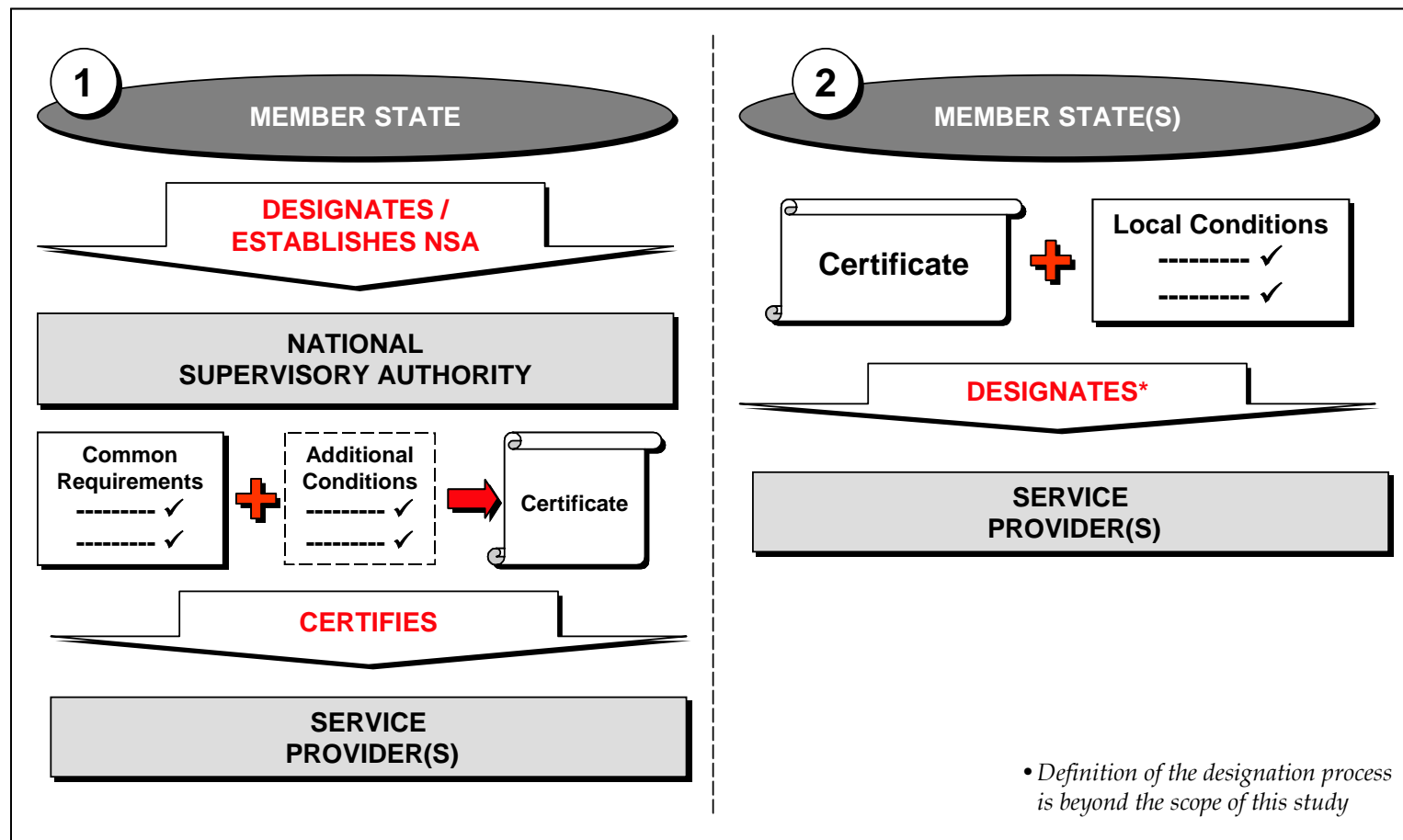


Table Of Contents

- ▶ Overview of Study
- ▶ Definition and Application of Common Requirements
- ▶ Overview of Common Requirements
- ▶ Recommendations for Operational Data



The Common Requirements form a set of generic requirements which a service provider must meet in order to be *designated* by a Member State



There are a series of underlying principles that require clarification...

- ▶ The proposed Common Requirements are Community-wide requirements which are applicable to any service provider engaging in the provision of air navigation services
 - ATS, MET, AIS or CNS
- ▶ They are applicable for service provision for all phases of flight
 - En route, approach and aerodrome
- ▶ They are distinct from Local Conditions which may also be required by a Member State to meet local specificities, where justifiable
 - National security / operational requirements
- ▶ There is no expiry date for the Common Requirements
 - Their compliance is required to maintain currency of the certificate awarded

Compliance with the Common Requirements is designed to be the instrument of 'access' to service provision across the Community



The form and scope of the Common Requirements has been chosen to facilitate the ongoing supervision and designation process

- ▶ The compliance of General and Specific requirements are supported by ongoing reporting provisions of the Business Plan, Annual Plan and Annual Report
- ▶ Based on Stakeholder feedback, the structure of the Common Requirements has been amended to allow a more logical flow and increase commonality during their implementation
 - All Common Requirements for quality management, safety management, safety reporting, security and contingency planning are grouped together recognising that operational practice may allow them to be part of the same overall system
- ▶ At this stage, and in order to maintain a complete picture, Common Requirements include areas also addressed by the ESARRs
 - The relationship between these elements may evolve as the Commission fulfils its obligations under Article 4 of the Service Provision Regulation

The Requirements apply equally for the provision of national services and trans-national services, thus facilitating the creation of FABs



The choice of depth of the Common Requirements is important towards facilitating the creation of a 'level playing field'

- ▶ The Common Requirements have been determined by the need to identify or develop common minimum criteria for the provision of ANS to the maximum extent possible
 - The overall aim being to minimise ambiguity on interpretation and drive 'upwards' a level playing field
 - Due to the varying institutional and operational models, it is not possible to specify every detail of information 'desired' from an NSA's perspective
 - It is foreseen that the application of the Common Requirements as they stand will have a large spread of impact across service providers and there may be justifiable reasons for a phased approach of implementation in some cases
- ▶ Although the obligations of the draft SES proposals are directed towards the Member State, the Common Requirements extend obligations directly to the service provider
 - This is designed to make the supervisory process more cooperative and transparent
 - Some may appear to be more appropriately specified as part of '*additional conditions attached to certificates*' – Annex II of Service Provision Regulation

The depth is chosen to maximise the definition of requirements through common application, as apposed to national specificity

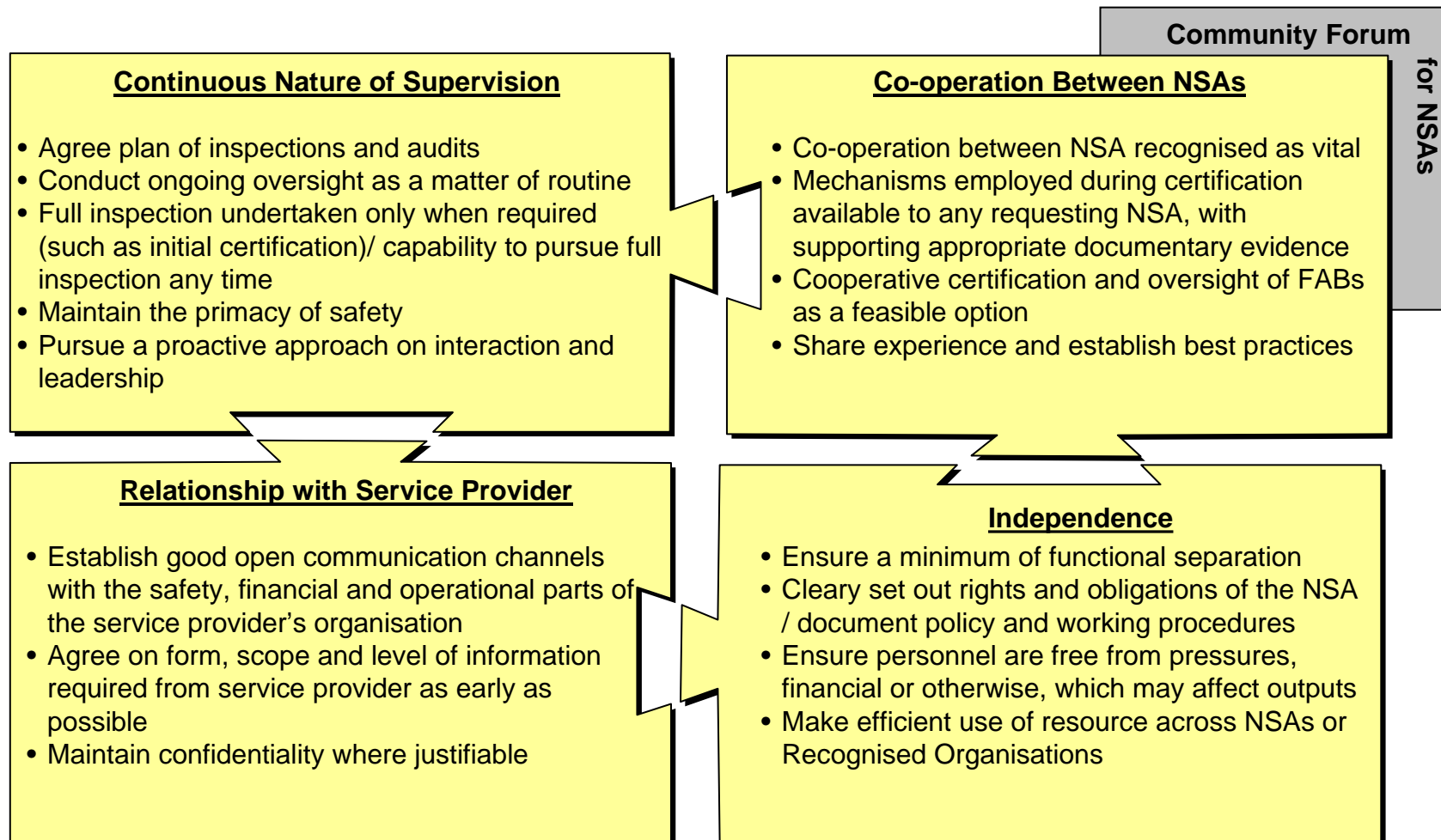


The NSA will provide the essential role during certification and compliance verification of the Common Requirements

- ▶ The creation of a NSA in each Member State requires that
 - A new body be formed
 - An existing body have extended roles, including requirements for coordination with other NSAs
 - And/or a 'Recognised Organisation' be allocated to undertake inspections and surveys on its behalf
- ▶ Compliance with the Common Requirements should allow an NSA in a State where services are provided by organisations based in another State to be confident that the services meet minimal acceptable requirements
 - Various elements including the Business Plan, Annual Plan / Report and individual reporting obligations on services providers, assist in the transfer of information between NSAs as far as possible
- ▶ The actual process towards establishment of the NSA and definition of its working practices is beyond the scope of this Study
 - This is left to the Member State to implement according to the subsidiarity principle
 - However, a series of recommendations for certification are given for guidance



The are four interrelated themes of guidance developed for the NSAs...



It is thus possible to illustrate a chain of activity for NSAs and States...

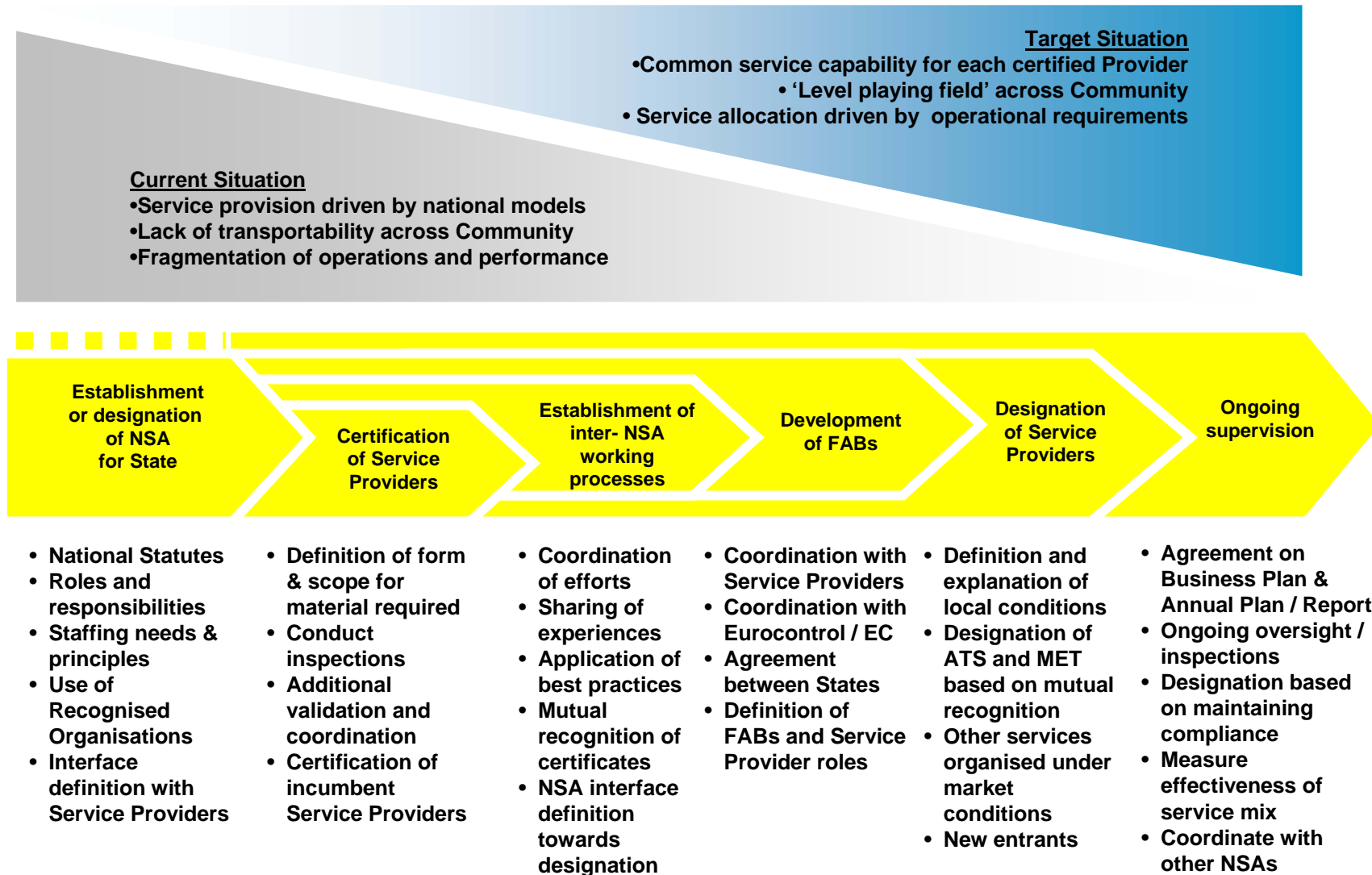
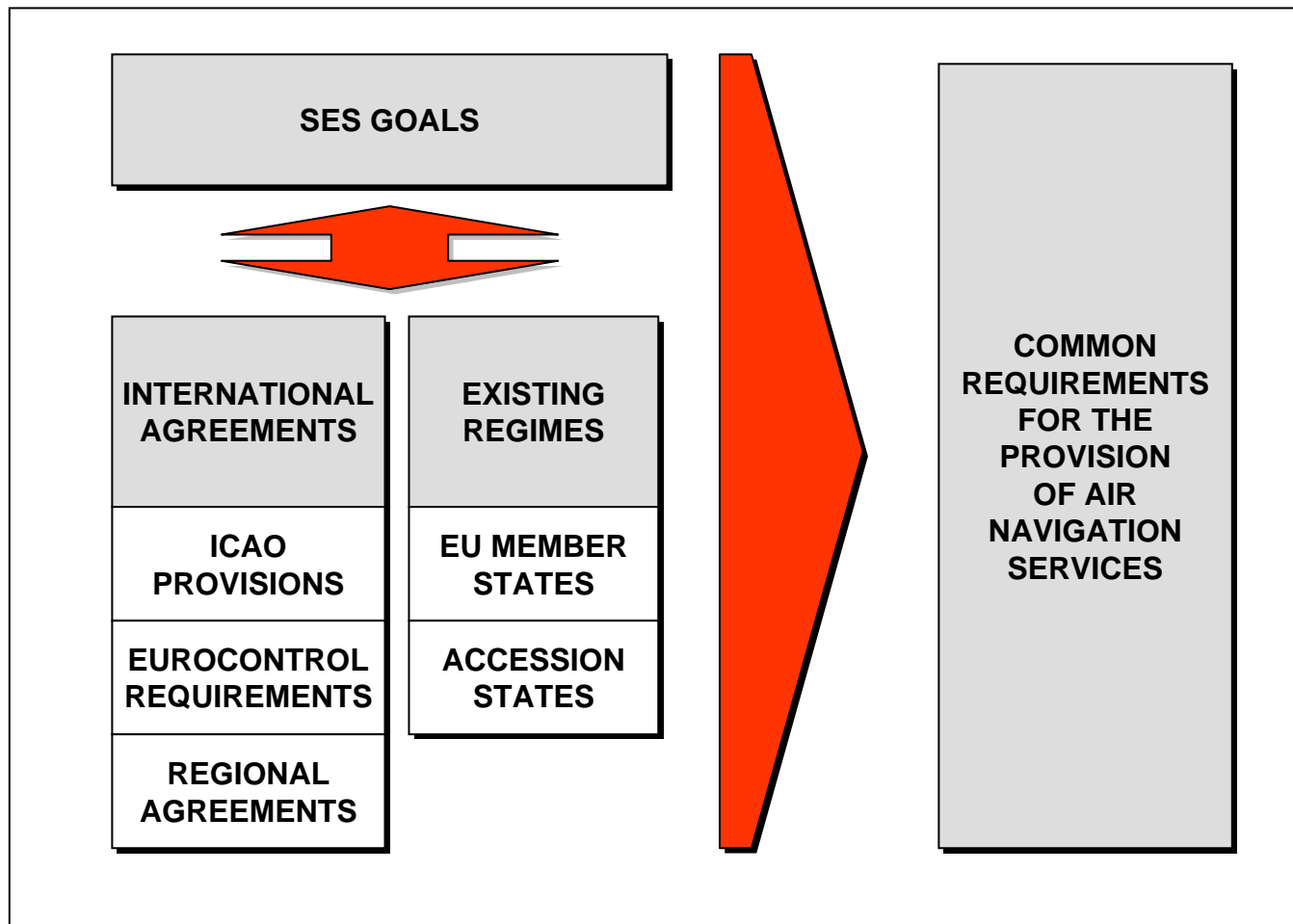


Table Of Contents

- ▶ Overview of Study
- ▶ Definition and Application of Common Requirements
- ▶ Overview of Common Requirements
- ▶ Recommendations for Operational Data



The Common Requirements are a synthesis of the ideas developed by Member States with the information on existing regimes, checked against the goals of the SES



- ▶ Phase 1 of the study provides a better understanding of the current institutional arrangements – gained through consultation with service providers and aviation authorities
- ▶ The methodology has involved a “gap analysis” of the existing international and national rules and agreements against the goals

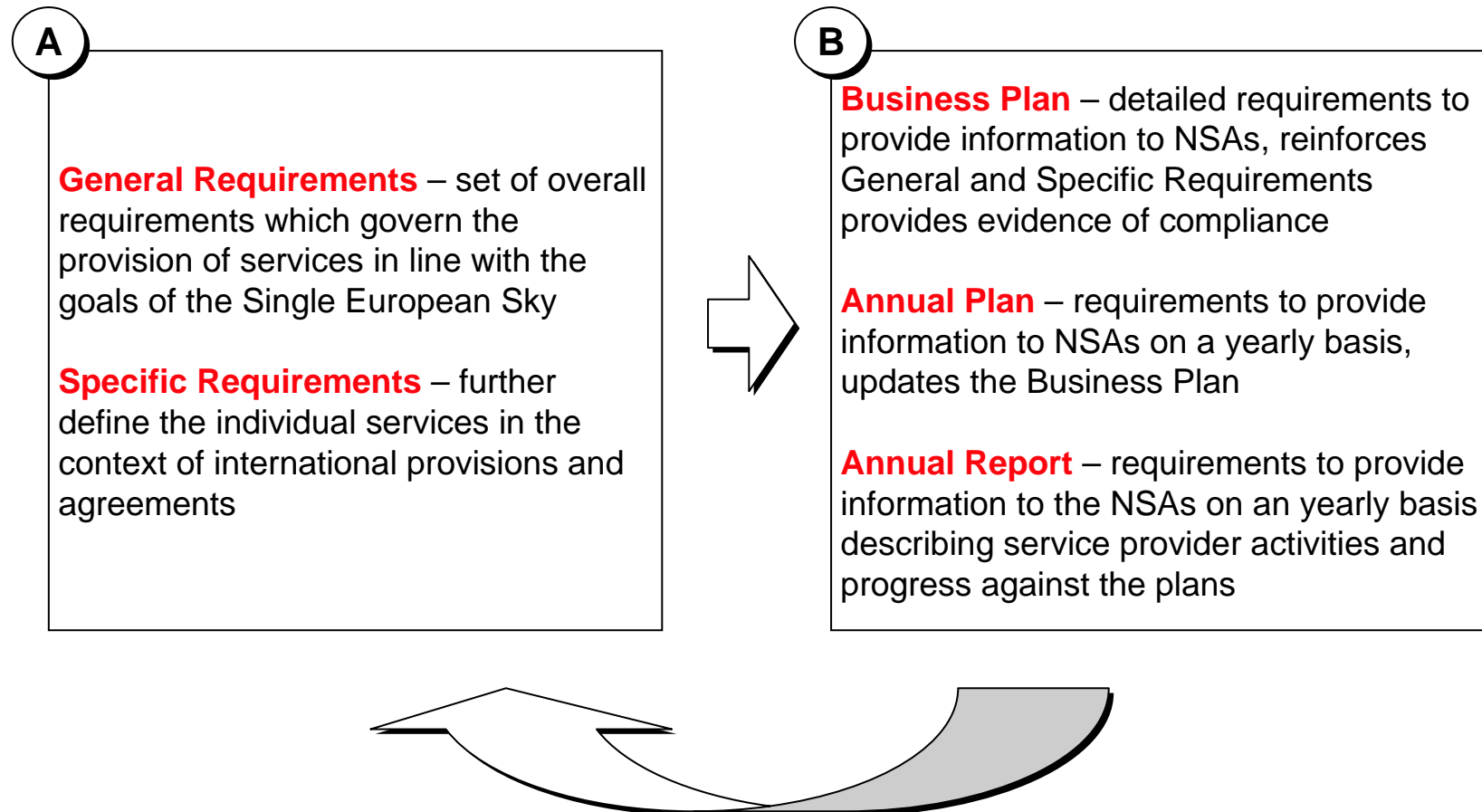


The Common Requirements are structured in five sections - supporting commonality of supervision, facilitation of FABs and equal access for service providers

- ▶ The structure maintains continuity and traceability with previous work but is designed to support clarity and logical flow by placing like subjects under the same headings
- ▶ The nature of the Common Requirements is that there is some degree of overlap
 - where they support the same overall requirement individual Common Requirements are grouped together
- ▶ Those areas which are integrated to some degree into one overall system - following best practice – have been placed together under Technical and Operational Competence and Suitability
 - quality management
 - safety management
 - safety reporting
 - security
 - contingency planning



Together the Common Requirements build a picture of the overall suitability of a service provider for initial certification, while also permitting on-going supervision and assessment



Technical and Operational Competence and Suitability is the first and largest section of the Common Requirements, linking many key areas

- ▶ In general, Common Requirements under this heading place obligations on the service provider to demonstrate its technical competence and suitability
 - However, as with later sections, this demonstration is supported by the production of the Business Plan, Annual Plan and Annual Report – these provide evidence to the NSA that a service provider's obligations have been met
- ▶ Requirements start with some general provisions without which the credibility of the entire suite of Common Requirements would be drawn into question
 - e.g. under **Capability of Providing Services** Common Requirement No.1 “...to provide the air navigation services for which it is certified in a safe, continuous, cost-efficient and sustainable manner...”, is an example of a basic requirement to be expected of service providers – it is made practical by the application of more detailed Common Requirements
- ▶ Other more detailed requirements under this section may be designed to contribute to greater efficiency or support the integrity of the ATM system across the Community or other SES goals



The arrangement of the Common Requirements under Technical and operational Competence and Suitability is intended to follow a logical progression

- ▶ Capability of providing services
- ▶ Maintenance of Operations Manuals
- ▶ Capability of Staff
- ▶ Human Resources Management

- ▶ Quality Management Systems
- ▶ Safety Management Systems
- ▶ Safety Reporting Systems
- ▶ Security Systems and Processes
- ▶ Contingency Plans

- ▶ Operational Data

- ▶ Consultation with Users
- ▶ Consultation with Other Service Providers
- ▶ Consultation with the NSA
- ▶ Civil/Military Cooperation
- ▶ Expert Support to the State
- ▶ Obligation to Alert the NSA



Although each stands on its own merits, the initial General Requirements are built up with more detailed specifics

Capability of Providing Services (1-4)	<ul style="list-style-type: none">• Includes requirement for 2 years equivalent service provision expertise (CR2)• Necessity of maintaining sufficient technical and operational capacity• Basic requirement to manage the organisation to support safe, efficient and continuous provision of services
Maintenance of Operations Manuals	<ul style="list-style-type: none">• Includes requirement to maintain operations manuals and to provide copies to the NSA
Capability of Staff (6-8)	<ul style="list-style-type: none">• Requires service provider to employ sufficient, adequately trained staff• Requires a detailed register of its staff – so supporting inspection and compliance with the Requirements• Specification of the level of staff qualifications is to be in compliance with ICAO Annex 1 and with Section 5 of ESARR 5
Human Resource Management (9-11)	<ul style="list-style-type: none">• Recognises the essential value of the Human Resources in ANS• Supports competence by demonstrating that a service provider has taken steps to ensure the retention and development of staff• Includes requirements in line with identified best practice to adopt formal policies and HR programmes



TECHNICAL AND OPERATIONAL COMPETENCE AND SUITABILITY

Requirements 12 to 21 all contribute to various aspects of the technical and operational competence and suitability of a service provider – they may be already integrated to different degrees

Quality Management Systems (12)	<ul style="list-style-type: none">• Requires a formal quality management system to apply to all certified services – recognising that this may require some element of phasing of implementation• Requires accreditation to a particular standard ISO9001:2000 in order to facilitate a Community-wide standard
Safety Management System (13-14)	<ul style="list-style-type: none">• Requires adoption of a safety management system in compliance with ESARR 3• Requires implementation of risk assessment and mitigation capabilities in compliance with ESARR 4 section 5 – facilitates inspection process by need to provide supporting documentation to the NSA for any changes to the ATM system
Safety Reporting System (15-16)	<ul style="list-style-type: none">• Gives Community-wide legislative weight to the implementation of ESARR 2• Encourages further development of best practice (and therefore efficiency in the ATM System – a goal of the SES) by requiring automated procedures as far as possible• Reporting of incidents must reference airspace organisation – facilitating future FABs



This informal subsection of the requirements is completed by security and contingency plans – there is also an overlap with requirements on operational data

Security Systems and Processes (17-20)	<ul style="list-style-type: none">• Contributes to the safeguarding of civil aviation in general and supports effective management of the organisation by demonstrating that it has taken steps to ensure the security of its facilities, personnel and information• Requires formal, documented procedures for security including cooperation with relevant civil and military authorities
Contingency Plans (21)	<ul style="list-style-type: none">• Requires formal, documented contingency plans to be adopted - demonstrates the service provider's managerial competence and contributes to the sustainability of its service• Good example of how the depth of a Requirement cannot be too prescriptive since likely impacts which should be taken into account under a contingency plan will vary with circumstance
Operational Data (22)	<ul style="list-style-type: none">• Requirement to have procedures in place to exchange data with other service providers and organisations supports the interoperability regulation, and is a basic competency requirement for any service provider• Security of operational data is also dealt with under CR18 security systems and processes



Communication with third parties is a vital part of ANS provision – Common Requirements in this area support competency and drive towards the effective and efficient provision of services

Consultation with users (23-24)	<ul style="list-style-type: none">• Requirement to consult with stakeholders to ensure service provider is providing satisfactory services – evidence will be provided in the Annual Report• Includes quantitative measures to solicit user opinions twice per year
Consultation with other service providers (25)	<ul style="list-style-type: none">• Designed to assist with cooperation between service providers – allows an inspecting NSA to be sure that a certified provider has considered this aspect including where airspace is vertically separated
Consultation with the NSA (26-27)	<ul style="list-style-type: none">• Requirement to provide relevant information on request of the NSA – supports compliance with Requirements in conjunction with the Business Plan, Annual Plan and Annual Report
Civil/military cooperation (28-29)	<ul style="list-style-type: none">• Requirement to agree management of airspace with civil or military counterparts where appropriate – obliges the service provider to facilitate the State's obligations under Article 10 of the Service Provision Regulation• Recognises that Flexible Use of Airspace is a goal of the SES
Expert support to State (30)	<ul style="list-style-type: none">• Recognises that service provider is source of considerable expertise, obliges support to the State as appropriate to meet inter/national obligations
Obligation to Alert NSA (31)	<ul style="list-style-type: none">• Obliges service provider to inform NSA of any factors which may affect its technical and operational competence



Common Requirements relating to **Financial Strength** demonstrate a provider's financial security and contribute to the emergence of a fair market (where appropriate)

- ▶ Services will not be adversely affected by a service provider's financial position if its security can be clearly demonstrated
- ▶ Financial Management of the service provider's organisation is key to its good and efficient management and continuous operation
- ▶ Common Requirements relating to financial management facilitate the application of Community legislation on competition in any market for the provision of ANS

Ability to Meet Financial Obligations (32-34)	<ul style="list-style-type: none"> • Ensures continued operation of services is not jeopardised by a difficult financial position
Management of Assets (35-37)	<ul style="list-style-type: none"> • Includes register of assets – so assisting financial assessment • Prevents disposal of essential assets does not allow them to become subject to claim from third parties without involvement of the supervisory bodies – contributes to the overall integrity of the European ATM system
Non-ANS Activities (38-39)	<ul style="list-style-type: none"> • Activities which carry financial risks <i>which may subsequently damage a provider's ability to provide ANS services</i> are prevented
Obligation to alert NSA (40)	<ul style="list-style-type: none"> • Obliges service provider to inform NSA of any factors which may affect its financial position



Common Requirements on **Ownership and Organisational Structure** highlight any potential conflict of interest and demonstrate that a service provider has an effective structure

- ▶ A clear picture of a service provider's institutional status is a starting point for understanding its relationship to the aviation value chain
- ▶ Identifying organisational responsibilities is essential to confirming a provider's ability to deliver the services required – and to sustain that ability
- ▶ Depending upon the nature of the service provider, the term “ownership”, may not be applicable
 - regardless of status, the same degree of understanding of its institutional status is required, whether privatised, a commercial entity or a government department
- ▶ Common Requirements under the heading of Ownership and Organisational Structure are also contributory factors to an inspecting body or regulatory body's overall understanding of the service provider's make-up and activities



The Common Requirements ask for information on links with other organisations as well as on their internal structure

Ownership (41-44)	<ul style="list-style-type: none">• Requires service provider to provide description of its legal status including identifying its owners, shareholders or public bodies responsible• Restricts ownership of providers of Air Traffic Services to Community governments, individuals or undertakings – ensuring control is ultimately subject to Community legal instruments
Links with other organisations (45-47)	<ul style="list-style-type: none">• Requires description of links with other organisations both in ANS and those not involved with ANS – supports the Financial Strength Requirements and allows full assessment of service provider activity
Organisational Structure (48-51)	<ul style="list-style-type: none">• Includes requirement to provide organisational charts describing reporting lines and how functional and organisation units relate to each functional area – facilitates an assessment of a service provider's managerial competence• Requirement 50, to be organised “in such a way that [the service provider] can accommodate relevant infrastructure and technology developments” also contributes to the overall development of the European network



Common Requirements relating to **Access to Services** are established in order that services provided are available openly and transparently to all users

- ▶ These requirements complement those relating to Technical and Operational Competence

Open and transparent provision of services (52-56)	<ul style="list-style-type: none">• Includes requirement for a documented policy for providing services openly and transparently• Requires non-discriminatory provision of service to all users in service provider's area of responsibility – not desirable to have more closely specified requirements since unreasonable demands on a provider may lead to degradation of other, core services• Supports the goals of the SES to ensure that any restrictions due to defence or security measures are proportionate
--	--



Common Requirements on **Liability and Insurance** assist with clarity of the civil aviation liability chain and support continuity of service provision

- ▶ The development of Functional Airspace Blocks is expected to complicate current arrangements for the allocation of liability in ATM where service providers do so across National boundaries.
- ▶ A service provider must demonstrate arrangements to cover actual or potential liabilities
 - to assist with clarity of the relative positions of parties involved
 - so that continuity of services will not be threatened through liability for damages

Obligation to cover liabilities (57-61)	<ul style="list-style-type: none">• Requirement is to ensure that arrangements to cover losses for damages are in place – no single method can be since they will be appropriate to the nature and legal status of the service provider• Minimum liability levels are also not advocated since they will vary between providers and setting them may affect the price of any commercial policies• Future separation of ATS from other services is allowed for by the inclusion of separate requirements for ATS and non-ATS services• Cooperation with other providers is encouraged since agreements making liability explicit are required where a provider uses the infrastructure of another
---	---



Specific Requirements further define individual services in the context of international provisions and agreements

- ▶ The Specific Requirements have the effect of bringing into Community legislation the provisions of specific international agreements relevant to working methods and operating procedures

Air Traffic Services (62)	<ul style="list-style-type: none">• Requires consistency with ICAO Annex 11, Annex 2, Doc 4444 PANS-ATM and Doc 7030/4 EUR Regional Supplementary Procedures
Meteorological Services (63)	<ul style="list-style-type: none">• Requires consistency with ICAO Annex 3 and Doc 8896 Manual of Aeronautical Practice
Aeronautical Information Services (64)	<ul style="list-style-type: none">• Requires consistency with ICAO Annex 15, Annex 3, Annex 4 Aeronautical Charts and AIS Manual
Communications / Navigation / Surveillance (65)	<ul style="list-style-type: none">• Requires consistency with ICAO Annex 10 Aeronautical Telecommunications
Information Exchange (66-68)	<ul style="list-style-type: none">• Requires information to users to be provided consistent with ICAO Annex 5 Units of Measurement• Also requires service providers only to use operational data from other certified providers unless agreed by the NSA



The **Business Plan** is the first of three key tools which create a package of information – facilitating supervision and demonstrating compliance with the Common Requirements

- ▶ The Business Plan is the major mechanism by which compliance is demonstrated – its contents support many of the General and Specific Requirements

General (69-69.8)	<ul style="list-style-type: none">• The Business Plan sets out the service provider's aims - and strategy for achieving those aims• Requirement for covering a minimum five year period is intended to be sufficiently long to set out a strategy and yet still provide flexibility – it is selected following consultation; longer plans are not precluded• Includes requirements on practical agreement with the NSA (e.g. on form, scope and level of detail) to encourage a constructive relationship with NSA
Management of Assets (69.9-69.12)	<ul style="list-style-type: none">• Along with the General section this supports Common Requirements on Financial Strength and competence of provider• Requires exposition of ability to meet infrastructure costs
Investment Strategies (69.13)	<ul style="list-style-type: none">• Requirement to set out investment strategy demonstrates financial strength and supports requirements on organisational structure
Human Resources (69.14-69.15)	<ul style="list-style-type: none">• Requirement to provide all relevant information relating to HR including recruitment metrics supports the General Requirements in this area (CR 9-11) and assists in maintaining ATCO resources and quality levels
Supervisory & Regulatory Costs (69.14)	<ul style="list-style-type: none">• Where regulatory and NSA costs are supported by the service provider these must be made clear to ensure transparency



The **Annual Plan** is the second tool to facilitate inspection and compliance with Common Requirements – it provides an annual update to longer term plans

- ▶ Common Requirements under the Annual Plan also support many of the General and Specific Requirements

Capacity (70.2-70.3)	<ul style="list-style-type: none">• In order to maintain its certificate a Service Provider must demonstrate that it has sufficient capacity to provide services effectively based on local and regional forecasts• The requirement to demonstrate the methodology used to determine capacity is as important as the plan itself – since this demonstrates a service providers competence and commitment to meeting the Requirements
Quality of Services (70.4-70.6)	<ul style="list-style-type: none">• Requirement is to provide an indication of the level of service delivery (including e.g. delays) and to demonstrate the methodology for determining the level – contributes to overall competence assessment• The requirement cannot be further detailed without specifying the level of performance to be met and these are dependent on circumstances
Financial Plan (70.6-70.8)	<ul style="list-style-type: none">• Requirements to provide an annual financial plan support the longer term Business Plan and ensure consistency and impact determination
Supervisory & Regulatory Costs (70.9-70.10)	<ul style="list-style-type: none">• Requirements to provide an annual plan for these costs allows an NSA to assess them across service providers – includes costs of expert support to the State



The **Annual Report** is the third tool in the package – providing information to the NSA and allowing assessment of compliance with the Common Requirements

- ▶ The Annual Report provides a check of progress against the Business Plan and Annual Plan
 - Facilitates transparency and enables supervision of compliance with Requirements

Capacity (71.2)	<ul style="list-style-type: none"> • Requirements to provide an effectiveness assessment of capacity enables comparison of annual capacity plan
Quality of Services (71.3-71.7)	<ul style="list-style-type: none"> • Requirement to report performance against measures identified in annual plan allows effective review • Requirements also enable review of operational and technical development against annual plans • Requirement to report annually on consultation with users specifies a minimum level of consultation following best practice – and thus contributes to the SES goal of more effective and efficient provision of ANS
Financial Results (71.9)	<ul style="list-style-type: none"> • Requirement to report all relevant financial measures identified in Business Plan and Annual Plan permits review of financial position supporting Common Requirement for Financial Strength • Includes requirement to identify any cross-subsidies – although these are explicitly permitted in the Service Provision Regulation visibility contributes to transparency and a level playing field in ANS
Supervisory & Regulatory Costs (70.10-70.11)	<ul style="list-style-type: none"> • Requirements to provide an a report of these costs permits assessment against plan



Table Of Contents

- ▶ Overview of Study
- ▶ Definition and Application of Common Requirements
- ▶ Overview of Common Requirements
- ▶ Recommendations for Operational Data



The study has focused on two areas relating to the Operational Data and their exchange

► Access and Use of Operational Data

Rationale: The safe access to and use of operational data is critical to ensuring the correct functioning of a coherent ATM system. The ability of an ANSP to manage and exchange data with other providers is therefore essential for the provision of safe and effective air navigation services

► Data Protection and Security

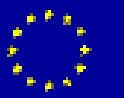
Rationale: Much of the information necessary for ATM is safety-critical or sensitive in commercial or political ways. Therefore, there is an inherent need to manage access rights (replication rights) and other protection aspects in the ATM environment



Access and Use of Operational Data

► General Requirement

22. The service provider shall ensure that it has in place suitable procedures and processes to enable the exchange of data with other services providers and other organisations as detailed in plans developed through Community legislation.



Data Protection and Security

► General Requirement

18. The service provider shall adopt and document security systems and procedures for ensuring the security of data it receives or produces or otherwise employs, so that access to it is restricted only to those authorised

- this shall include the adoption of a security management programme relating to data which is integrated with the design, manufacture, test, installation, operation and maintenance of operational systems
- the security management programme shall identify the means of containing the effects of security breaches internally and externally to the system and identify recover action and mitigation procedures to prevent re-occurrence
- the security management programme shall include measures designed to detect security breaches and to alert users with appropriate security warnings.



THANK YOU

QUESTION AND ANSWERS?

