Handbook

Compliance

eControl
4.4.1.4

ARCONDA.systems

eControl

Index

1. Preface 5

2. Core functionality 8

3. People involved 12

3.1 Competent authority 12

3.2 EASA project office 13

3.2.1 General functions of the project office 13

3.2.2 Competent authority 13

3.2.3 Departments 13

3.2.4 Non-compliance situation 14

3.2.5 Change management during the lifetime of the project 14

3.2.6 Focal point eControl / User support 14

3.3 Airport departments 14

3.4 Management 15

3.5 IT department 15

3.6 eControl / manufacturer 15

4. Airports - step-by-step towards compliance 16

4.1 Project set-up 16

4.2 Verification of relevance and definition of specialised departments 16

4.3 Coordination of non-relevant requirements with the authority 16

4.4 Transfer of work files to the specialised departments by the project office 17

4.5 Processing of requirements by the specialised departments 17

4.6 Global documents 18

4.7 Non-compliance situations 18

4.8 Evaluation of evidence for each requirement 19

4.9 Transfer of compliance information to the competent authority by the project office 20

4.10 Final coordination with the competent authority 20

5. Regulation (EU) No. 139/2014, AMC, CS, und GM and other regulations 21

6. Requirements 22

6.1 General data 22

6.2 Compliance attributes 24

6.3 Versions 25

6.4 Documents 26

6.4.1 Traceability- automatic version management 26

6.4.2 Data protection – reliable access control via compliance categorising 27

Publisher: Arconda Systems AG
Sportallee 6
22335 Hamburg

Date: 01 / 2016

Editors: Frank Espenhain
Pascal Rohmann

Layout&Graphics: Torben Petrina

Copyright: Distribution, copying and reproduction is only permitted with written approval from Arconda Systems AG. This also applies to recording in electronic databases and copying onto storage mediums. All data is protected by copyright.

6.4.3 Administration - integration into a global archive 27
6.4.4 Search functions - metadata 28
6.4.5 Documents and object links 29
6.4.6 Global documents 30
6.5 Measures 32
6.6 History 33
6.7 Object explorer 34
7. Data and authorisation structure 36
7.1 Regulations and requirements 36
7.1.1 Flexible hierarchical structure 36
7.1.2 User permissions for the expansion and changing of the hierarchical structure 37
7.2 Compliance categories and compliance attributes 38
7.2.1 Compliance categories 38
7.2.2 Compliance attributes for requirements 39
7.2.3 Value range 40
7.2.4 Reference data structure 41
7.3 Authorisation structure 43
7.3.1 Design 43
7.3.2 Administration - users and user groups 44
7.3.3 Write and read access to compliance attributes 44
7.3.4 User permissions 45
7.4 Permissions assignment documentation 48
7.4.1 Structure of process attributes 48
7.4.2 Process structure 48
7.4.3 Process authorisations 49
8. Compliance management cockpit 50
8.1 Summary 50
8.2 Query generator 51
8.2.1 Summary 51
8.2.2 Logical operators "AND" and "OR" 51
8.2.3 Comparison operators 51
8.3 System validation 52
8.4 Which right? 53
8.5 SQL queries 53
8.6 Query pool - reusable queries 53
8.7 Storage of query definitions 55
8.8 Change in existing query definitions 56
8.9 Deletion of query definitions 56
8.10 Global query definitions 56
8.11 Start menu 57

9. Reporting 58
9.1 Standard reporting functions 58
9.2 Summary of process attributes 59
9.3 Frequently distribution processes 61
9.4 Process and compliance sheet 63
9.4.1 Report structure – Targeted formatting of content for addresses 65
9.4.2 Selection of compliance categories and attributes 66
9.4.3 Selection of documents 67
9.4.4 Reproducibility 68
9.4.5 Report design 68
9.4.6 Data transfer via ZIP file 69
9.4.7 Non-compliance reports 71
9.5 Process attribute characteristics 74
10. RiskDB - eControl risk database 75
11. Audits - long-term maintenance of compliance level 77
12. Change management 80
13. Training and qualification management 83
13.1 Regulatory requirements 83
13.2 Qualification status 83
13.3 Linking of processes or requirements with qualifications 84
13.4 Read & Sign 84
14. Competent authorities 85
14.1 General requirements 85
14.2 ADR.AR.A.010 Regulations 85
14.3 ADR.AR.B.020 Qualifications 86
14.4 ADR.AR.B.020 certification
- system for the documentation of the certification procedure 86
14.5 Model of operational organisation 87
14.6 Relevant compliance attributes from the perspective of the competent authorities 88
14.6.1 CA Step 1: Header sata 88
14.6.2 CA Step 2: Relevant requirements 88
14.6.3 CA Step 3: Compliance strategy 88
14.6.4 CA Step 4: Evaluation of verification documents 89
14.6.5 CA Step 5 Monitoring programme 89
14.7 ADR.AR.A.015 AltMoC 90
14.8 ADR.AR.B.020 deviations 90
14.9 ADR.AR.B.010 QM-System 90
14.10 ADR.AR.B.015 Changes 91
14.11 ADR.AR.C.040 Change requests 91
14.12 ADR.AR.C.005/010 Audits 93
14.13 ADR.AR.A.030 Incidents 93
14.14 ADR.AR.A.040 Safety instructions 94
14.15 ADR.AR.C.045 Infringements 94

1 Preface

eControl Compliance Management is a software module, by means of which conditions or requirements can be documented and long-term compliance with these regulations can be systematically ensured, irrespective of the current regulations, organisational structure and any requested processing sequences.

This covers not only requirements, coordinated structures and properly displayed processing sequences, but also in particular document, measure, audit and risk management. Events or incidents in day-to-day operations (infringements, damage, other deviations) must also be taken into account and these can be linked to the individual conditions in order to ensure a network of all available information.

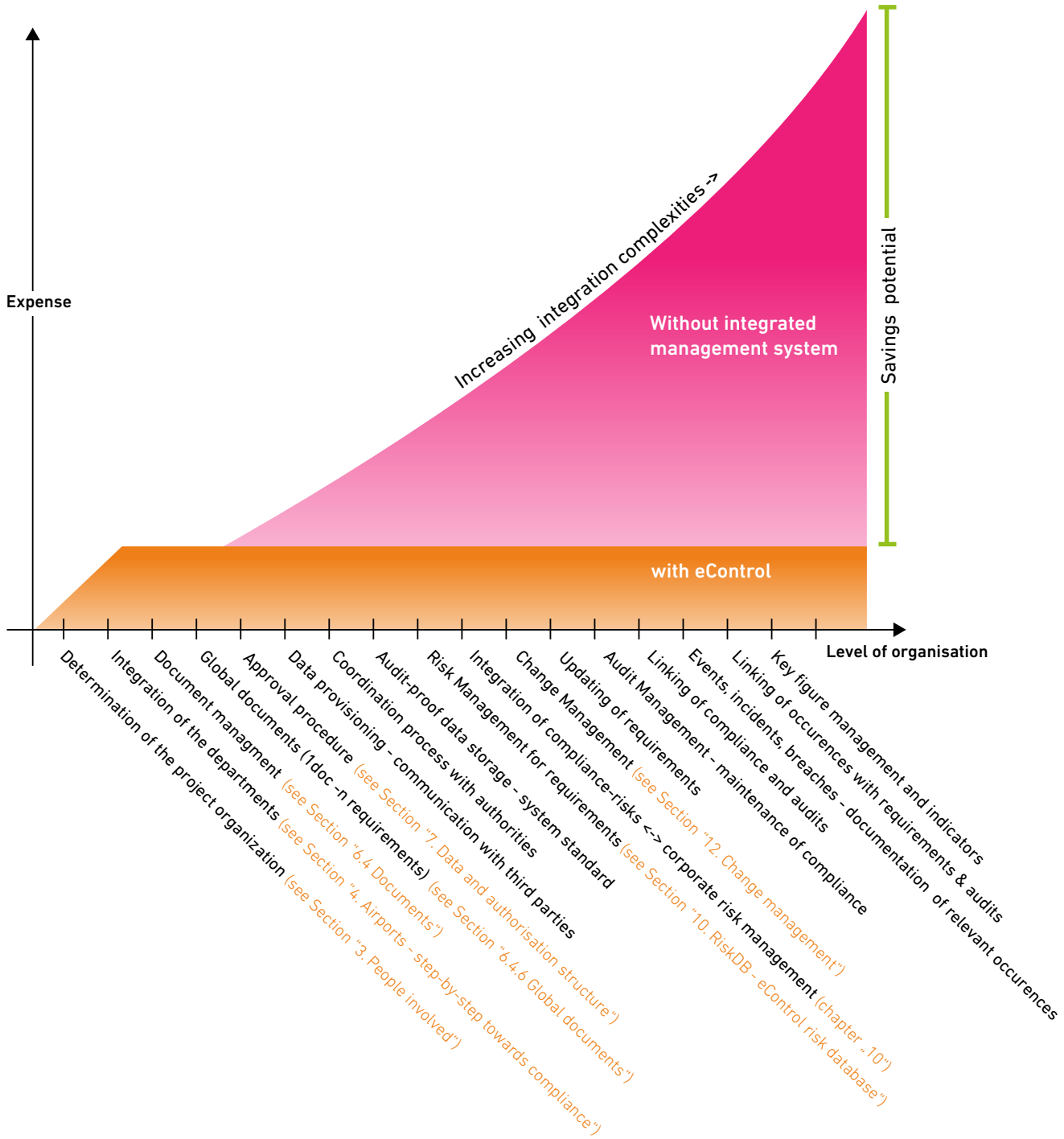
In addition to these services, eControl provides for the traceable storage of data. A sophisticated authorisation control guarantees a company-wide application of these purely web-based systems.

When deciding on the preferred software support for a compliance project, the first attempt is mostly the use of Excel spreadsheets, directory structures or individual in-house applications. This issue arises at the start of the project – in a phase in which both technical aspects and organisational adjustments have to be made in-house. A low priority (unfortunately) is given to audit safety, audit compliance and information networking.

A master plan is required for operational process management, in order to incorporate all relevant decision-making aspects and so provide an objectively viable decision-making basis. That is a difficult task for the EASA working group. Organisational and software interfaces must be created with safety management and where necessary, quality management responsible for audits and other organisational units such as the legal department, in order to achieve consistency between the work areas.

A master plan must also take commercial aspects into consideration. These involve on the one hand the "hard" licensing costs of the eControl standard solution and on the other hand the organisational, IT and other costs for other organisational forms, which clearly exist but are difficult to quantify accurately. We can of course help you with the formulation of system requirements, specifications etc., because as manufacturers we have already had experience of numerous projects with organisations and authorities.

The chart shown on the following page indicates various elements of a master plan.



At the beginning of this long authorisation period, which is likely to last more than 10 years, it is easier to start without an integrated system. The structural application of eControl requires an initial organisational and technical outlay as well as several hours of basic training. However, after a short time the organisation benefits increasingly from the possibility of being able to merge all data and information and use it for specialised purposes.

When determining the outlay that an organisation must make over a long period of time, we assume that the demands on compliance management, processes and networking of components will increase.

The fact is that this – without an integrated overall concept such as eControl – will, technically-speaking, be barely feasible. Instead the data would have to be recorded in many different customised solutions, Excel spreadsheets etc. and expensively maintained.

This manual focuses on the functions in the context of compliance management. For all other functional areas we would be happy to provide you with product catalogues, white papers or even personalised information.

We look forward to hearing from you.

Frank Espenhain
CEO

2 Core functionality

The core functionality of the system is described in summary form below, in order to provide a general summary of the possible applications in the context of compliance management.

- (a) Standardised compliance management
- (b) Compliance management for all regulations
- (c) Compliance management irrespective of the organisational structure
- (d) Freely configurable requirements
- (e) Freely configurable data fields
- (f) Intuitively operable query generator
- (g) Version management for regulations
- (h) Integrated document archive
- (i) Global documents
- (j) Export functionality
- (k) Report generators for project management and monitoring
- (l) Customised user permissions for each different requirement
- (m) Links – object links
- (n) Legally watertight documentation
- (o) Measure management
- (p) Change management
- (q) Risk management
- (r) Audit management

a Standardised compliance management
Compliance management system for airports, airlines and competent authorities.

b Compliance management for all regulations
eControl can be used as a software solution for all compliance management regulations (e.g. Regulation (EU) No. 139/2014, other EU regulations, planning approval notices, authorisation procedures, IATA and ICAO regulations etc.).

c Compliance management irrespective of the organisational structure
eControl can be used for the compliance management of many different organisational units (e.g. several airports, various subsidiaries, etc.), where the operational and structural organisation can be flexibly mapped.

d Freely configurable requirements

A number of different regulations such as Regulations (EU) Nos 216/2008 and 139/2014, ICAO Annex 14, and IATA regulations in addition to spreadsheets and drawings are already available to the manufacturer and are loaded into the system as requested. Essentially all regulations can be updated and changed or new regulations inserted by the customer.

e Freely configurable data fields

Depending on the regulations and the existing project organisations, a number of different data fields or compliance attributes are required. eControl can be freely edited or supplemented by the customer with a working collection of compliance attributes. Data fields for the non-compliance situation ELoS (Equivalent Level of Safety), AltMoC (Alternative Means of Compliance), DAAD (Deviation Acceptance and Actions Document) and SC (Special Condition) are in particular subject to compliance with Regulation (EU) No.139/2014.

f Intuitively operable query generator

The system has a standardised query generator, by means of which each data field can be consulted in order to select requirements and thus formulate all filter criteria. These queries comprise logical operators and parentheses and can be very difficult to define. The queries can be stored and re-used. In order to make it as easy as possible to apply these queries, queries can be specifically defined by the software experts in the project office and made available for use to all specialised departments on demand.

g Version management for regulations

For each requirement eControl provides a version management for the systematisation and tracing of the coordination process with the authorities.

h Integrated document archive

The integrated document archive provides a fully-automatic version management for each document, whereby all documents can be updated and access to old document versions is maintained. For each document a number of different metadata can be stored for tagging and used for full-text searches. Within the context of compliance management, documents are assigned to a number of different requirements. User-specific access to documents depends on whether the user has access to the relevant requirement as well as to the relevant compliance category. In this way, for example, publication of the documents can be restricted in connection with a DAAD strategy, whilst general documents about the relevant requirements are available to a considerably larger group of people.

i Global documents

The structure of this compliance documentation usually follows content-related aspects in the form of manuals, drawings, etc., rather than the regulations. With eControl an administration of global documents can be generated, which can be flexibly linked with many different requirements. The application of global documents simplifies the maintenance and change management of key documents, e.g. the airport manual.

j Export functionality
For each requirement, compliance sheets in PDF format can be generated and selectively merged with all relevant documents in the system to ZIP folders. These ZIP folders enable compliance evidence to be transferred easily and reliably to the competent authorities. The system documents the transfer in a way that is traceable, so that the version of the relevant requirement and attached document version can later be extracted together with the processing history of the relevant requirement.

k Report generators for project management and monitoring
The compliance management module has different report generators, with which freely definable status reports can be generated, e.g. for project progress reports, documentation for work packages, etc. The column layout and selection parameters of these report generators can be completely freely defined and stored for future use. The reporting also comprises process sheets, statistical evaluations including diagrams, cross-tabulation graphics and reports as evidence of any assigned authorisations. All reports can essentially be downloaded in PDF and CSV format and thus processed using, for example, spreadsheet systems such as MS Excel.

l Customised user permissions for each different requirement
eControl enables the smooth and easy integration of different specialised departments and this supports the working process. To safeguard the confidentiality of sensitive information, authorisations for individual requirements, differentiated according to the compliance category, can be assigned for users and user groups. In this way, for example, general compliance information can be disclosed company-wide, but the compliance attributes of any ELoS evidence is reserved for specially authorised users.

m Links – object links
With the links, requirements can be linked with global documents, other requirements, audits, investigations, occurrences, etc.

n Legally watertight documentation
The system's database provides a complete processing history for each data field and therefore a legally watertight documentation. A graduated authorisation procedure exists that regulates the extent to which this processing history may be viewed.

o Measure management
eControl measure management is also available for compliance management. The functional scope of measure management comprises a traffic light control system, automatic measure notifications, a standardised root cause analysis and central reporting.

p Change management
Compliance management supports change management with a number of different functions. The assignment of requirements to components and sub-systems enables, for example, verification of which requirements are involved in the changing of a component. In addition, the linking of global documents can be understood. They offer another indicator for the impact of changes.

q Risk management

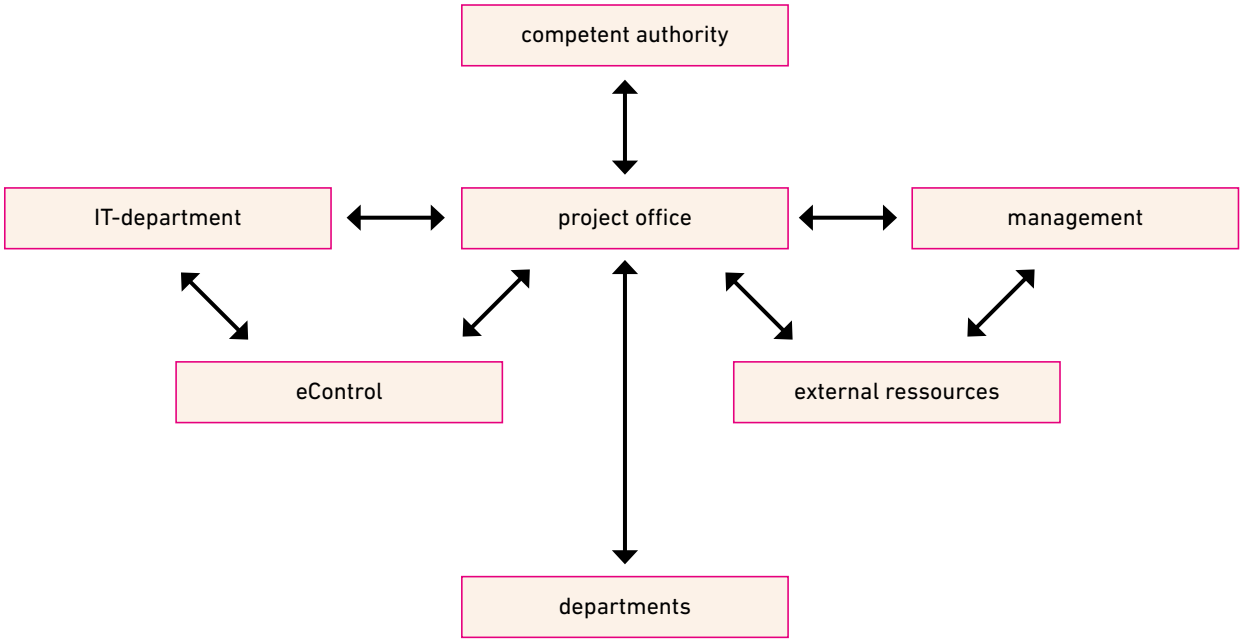
eControl provides a risk database, which enables risk assessments to be systematically stored and the risks classified via a risk matrix (e.g. according to ICAO DOC 9857). Risks can be recorded for each requirement and for each non-compliance situation.

r Audit management

Compliance management describes in general the conversion of an organisation in compliance with a policy. eControl audit management ensures that compliance is maintained over time – in particular in the event of changes and/or amendments to regulations. For Regulation (EU) No. 139/2014 and the Certification Specification (C/S), an audit catalogue is available, which complies with the classification structure of the requirements and supports as best it can the preparation, conduct and follow-up of the four-year auditing cycle.

3 People involved

The people involved in the processing sequences of compliance management are divided according to organisational and functional criteria into the groups of people listed below.



The chart shows the key significance of the project office for the coordination of all the people involved. The task packages of the people involved in the context of compliance management are shown below.

3.1 Competent authority

- Verification of evidence
- Technical and legal coordination of the evidence-based procedures and strategies preferred by the airports
- Schedule coordination to avoid organisational bottlenecks

3.2 EASA project office

3.2.1 General functions of the project office

The different regulations must always be mapped as a hierarchical structure of sub-items and requirements. eControl provides a number of regulations which can be changed or remodelled for the client by the EASA project office where required.

In standard operations the "EASA" node is subdivided into Regulation (EU) No. 139/2014 and the Certification Specification. If the certification bases of more than one airport have to be administered, a substructure for different airports can be incorporated beneath the "EASA" node:

- Monitoring of overall project progress and project timetable
- Central coordination of external resources
- Safety studies, expert reports, etc.
- Minimisation of procurement cost
- Communication of project progress and timetable to management
- Communication to management of personal, organisational and financial support required
- Setting up of a global document archive
- Alignment of structure of documentation and normally divergent structure of requirements

3.2.2 Competent authority

- Communication with the competent authority
- Verification and provision of compliance documentation for the competent authority via export function
- Isolation and coordination of non-relevant requirements

3.2.3 Departments

- Integration of relevant specialised departments into the project
- Explanation of project-specific workflow
- Functional and organisational support of the specialised departments
- Recognition of content-related overlaps in the activities of the specialised departments
- Avoidance of duplication
- Review and optimisation of any necessary change and documentation activities with the specialised departments
- Coordination of change and documentation activities with the competent authority

3.2.4 Non-compliance situation

- Identification of non-compliance situations
- Coordination with the competent authority and ensuring of workable strategies
- Conduct of risk assessments
- Updating of the risk database

3.2.5 Change management during the lifetime of the project

- Analysis of changes with regard to the requirements of the compliance project
- Communication to the specialised departments involved with any changes

3.2.6 Focal point eControl / User support

- Ensuring the standardised use of eControl by the project office and the specialised departments
- Software briefing of the specialised departments by the project office in eControl
- Support of the specialised departments with regard to reporting and query requirements.
- Provision of global query definitions, accessible company-wide
- Explanation to the specialised departments of the EASA structure in eControl
- Explanation to the specialised departments of the data and authorisation structure in eControl
- Application of new users to the IT department
- Assignment of specialised authorisations to the specialised departments for the selective processing of requirements
- Provision and maintenance of compliance categories and compliance attributes
- Maintenance of compliance-specific value ranges (work packages, status, components, etc.)

3.3 Airport departments

- Collation of available documentation
- Uploading of available documents in eControl
- Maintenance of data fields for compliance, evidence-based procedures and change activities in eControl
- Analysis of the legal requirements for those assigned to the relevant specialised department and other relevant requirements (139/2014, C/S, AMCs, GM)

- Verification and evaluation of available documentation in respect of the evidence-based procedure
- Identification of non-compliance situations
- Development of compliance strategies for the avoidance of non-compliance situations
- Coordination of evidence-based procedure and compliance strategy with the project office, where necessary
- Identification of global documents and coordination with the project office
- Request to the project office for external resources required

3.4 Management

- Identification of plan deviations
- Guarantee of adequate support for the project office and the specialised departments

3.5 IT department

- Ensuring of serviceability and data backup
- Publication of eControl in the Intranet of the airport or organisation
- User administration and assignment of permissions to the extent required
- Support in the event of technical problems in the project office

3.6 eControl / manufacturer

- Provision of updated and repaired programme versions
- Support services for the efficient processing and analysis of compliance information
- Provision as required of SQL queries for complex evaluation requirements
- (forensic) support services during the complete analysis of the audit trail
- Conceptual advice with regard to the generation and processing of compliance categories and compliance attributes

4 Airports - step-by-step towards compliance

The procedure described below ensures the traceable processing of the data and documents compiled as evidence of compliance as well as the division of responsibilities and communication between all organisational units involved.

The fine-tuning of the project for the implementation of individual requirements is not one of the primary objectives of this system. However, if required, it is possible to easily establish and maintain dates, completion steps, the anticipated scope of the work and other project control information. If desired, the compliance attribute data fields (see Section "6.2 Compliance attributes") can be created.

In practice a compliance project gives rise to various sub-projects for the creation of compliance, which require control using project management tools such as MS Project.

4.1 Project set-up

Organisational tasks:

- Setting up of the project office
- Appointment of contact partners by the authority and the project office
- Coordination of a global timeframe with the competent authority

Software related tasks:

- Setting up of project office users
- Assignment of permissions for project office users
- Documentation of authorisations awarded

4.2 Verification of relevance and definition of specialised departments

Organisational tasks:

- Review of all requirements of Regulation (EU) No. 139/2014 and certification specification
- Verification of requirements in terms of relevance/ applicability
- Specification of documentation desired/required for certification

Software related tasks:

- Specify EASA certification basis for each requirement
- Make organisational specifications such as organisational unit, department, owners and managers
- Documentation and specification of standardised application of compliance attributes by the various specialised departments

4.3 Coordination of non-relevant requirements with the authority

Organisational tasks:

- Identification of all requirements that are not part of the certification basis
- Documentation about why the relevant requirements do not have to be met by the airport (compliance attribute "EASA compliance verification")

Software related tasks:

- Documentation of the non-relevant requirements with the report "non-relevant requirements"

  Filter: EASA process tree, EASA certification basis = NO

  Columns: standard columns, "EASA compliance verification"

4.4 Transfer of work files to the specialised departments by the project office

Organisational tasks:

- Explanation of workflow and project organisation
- Explanation of global documents where available

Software related tasks:

- Setting up of specialised department users by the IT department
- Provision by the project office of specialised authorisations for the employees in the specialised departments
- Explanation of user interface
- Explanation of data and authorisation concept
- Explanation of uniform application of compliance attributes
- Provision of pre-defined queries by the project office, by means of which the specialised departments can easily filter "their" requirements
- Provision of pre-defined reports by the project office with regard to independent (partial) project control

4.5 Processing of requirements by the specialised departments

Organisational tasks:

- Analysis of assigned requirements by the relevant specialised department
- Collation of documentation by the specialised departments
- Verification and evaluation of available documentation in respect of the verification procedure
- Identification of non-compliance situations
- Rough analysis of compliance strategies for the avoidance of non-compliance situations
- Generation of additional documentation where necessary
- Coordination of verification procedure and compliance strategy with the project office, where necessary
- The project office coordinates the verification procedure and the compliance strategy, where necessary, with the competent authority, in order to avoid unnecessary activities or those deemed unacceptable by the authority
- Coordination of required compliance activities by the specialised department
- Documentation and monitoring of project progress by the specialised departments and the project office

Software related tasks:

- Uploading of the available documents in eControl
- Maintenance of the compliance management data fields
  - Status management for any relevant requirements
- Maintenance of data fields for essential status management

4.6 Global documents

Global documents are an integral component of compliance management projects

- Global documents should be used if a number of different compliance test requirements refer to the same "global" document.
- Global documents can be available in a centralised structure to which all departments have equal access.
- Global documents can be maintained centrally.

Organisational tasks:

- Specification of global documents by the project office in coordination with the relevant specialised department.
- Communication of the global document structure by the project office to all specialised departments.
- Linking of global documents and requirements by the specialised departments.
- Specification and monitoring of maintenance obligation by the project office.
- Making the specialised departments responsible for maintenance aware that a change in "their" global documents can impact on the compliance testing of other specialised departments.

Software related tasks:

- Setting up of a classification structure for global documents by the project office.
- Setting up of structural elements for global documents by the project office.
- Attachment of global documents to these structural elements by the specialised departments responsible for maintenance ("general process master data" compliance category).
- Assignment of specialised maintenance authorisations for the responsible specialised departments.

4.7 Non-compliance situations

Organisational tasks:

- Analysis of change requirement and non-compliance strategy by the project office and the specialised department.
- Coordination of the relevant strategy by the project office with the competent authority.
- Conduct of risk assessments by the project office.
- Prioritisation of the processing of non-compliance situations by the project office according to a critical path of the compliance project.

Software related tasks:

- Documentation of the coordinated strategy in eControl.
- Updating of the risk database by the project office.
- Incorporation as required of the relevant non-compliance attributes into the relevant requirements by the project office.
- Documentation of the relevant non-compliance information – capture of the information for the non-compliance data sheets.

4.8 Evaluation of evidence for each requirement

Organisational tasks:

- The project office checks the completeness of the evidence with regard to the AMCs and the certification specification (C/S).
- Evaluation of evidence quality by the project office.
- If there is any doubt about the evidence or the quality of the evidence, the project office requests amendments from the relevant specialised department.
- Ensuring that when the compliance test is conducted, clear and understandable references are made to the attached documents.
- Selection of documents to be used as evidence with regard to the competent authority. The project management combines all relevant, evidence-related documents from the secondary layers at the level of the requirement, provided that the documents have been stored in the structure beneath the relevant requirement.
- If the project office is not responsible for the release of the requirements, the project office submits the release-stage requirements for release to the organisational unit that is responsible for the release.
- Status management.
    - The project office updates the status of the requirement to "release", if the documentation is suitable for validation by the competent authority.
    - The project office leaves the status of the requirement at "validation" whilst the project office conducts the final processing of the requirement.
    - The project office resets the status of the requirement to "layer component in process", if amendment or completion work has to be done by the specialised department.

Software related tasks:

- Updating of the compliance status of the requirements.
- Merging of the documents at the level of the requirement, in order to enable an automated transfer to the competent authority.

4.9 Transfer of compliance information to the competent authority by the project office

Organisational tasks:

- For each requirement the project office generates a compliance sheet, from which the relevant compliance categories, e.g. "EASA compliance", "EASA compliance verification" and "EASA compliance release" can be specifically selected.
- For each requirement the documents to be submitted to the competent authority must be selected.
- The compliance sheet provided as a PDF document and the selected documents are merged in the system in a ZIP folder by pressing the "Create Zip folder" button.
- Where required the "ZIP export" must be supplemented with a documenting ReadMe file, which is part of the Zip file.
- The Zip expert is documented in the processing history of the requirements. The system tracks which requirement has been transferred to the competent authority with which verification documentation.

Software related tasks:

- Coordination of a transfer process with the competent authority (data carriers, Intranet drives, etc.).
- Generation of ZIP exports and conduct of transfer for each requirement.
- After a transfer of the data package to the competent authority the status is set by the project office to "Evidence transferred to authority".

4.10 Final coordination with the competent authority

Organisatorische Tätigkeiten:

- The project office receives any additional requests for evidence from the competent authority.
- The project office has minimised as far as possible the potential need for amendments by early coordination of the compliance strategy ((4.5) & (4.8)) or, if appropriate, the non-compliance strategy (4.7) .
- The project office provides the competent authority, where required, with amended or updated evidence.
- As soon as the competent authority accepts the evidence, the status of the requirement is set to "approved".

Softwareseitige Tätigkeiten:

- Updating of requirement versions by the project office.
- Content-related documentation detailing the change in the version information by the project office.
- The version of the attached and linked documents is fully automatically incremented in the system.
- New generation of a ZIP export and transfer to the competent authority.

5 Regulation (EU) No. 139/2014, AMC, CS, und GM and other regulations

In addition to the relevant requirements of Regulation (EU) No. 139/2014 and the certification specifications, the Acceptable Means of Compliance (AMCs) and the guidance material that is available for both areas are provided with eControl.

In respect of the compliance and the evidence submitted to the competent authority, Regulation (EU) No. 139/2014, the AMCs and the CS are relevant.

The verification documents can essentially be attached to all elements of the structure in eControl. The possible assignment of the documents depends on the structure of the content in the documents and the differentiation of the individual regulations.

If individual conditions contain a list of sub-items, for which definable, individual evidence can be cited, transparency can be improved by breaking down each section of the conditions into individual sub-items.

Correspondingly, where certification specifications are particularly extensive, it is possible to assign the documents not to the CS themselves but to the guidance material broken down into sections.

Conditions, certification specifications and the guidance material are arranged as "nodes" in a hierarchical structure. The following sections explain how information, documents, measures, etc. can be attached to these nodes.

For the sake of completeness, it should be pointed out that the nodes are homogenous from a technical perspective. The only exception is the "sub-item" type node, which is used only for structuring purposes and to which no data can be attached.

6 Requirements

eControl provides for the systematic, coherent and traceable storage of all available information in the context of a requirement or a condition. The capture of requirements for the compliance management of Regulation (EU) No. 139/2014 is not necessary – these are already provided by the manufacturer. **(see Section "5. Regulation (EU) No. 139/2014, AMC, CS, und GM and other regulations")**

6.1 General data

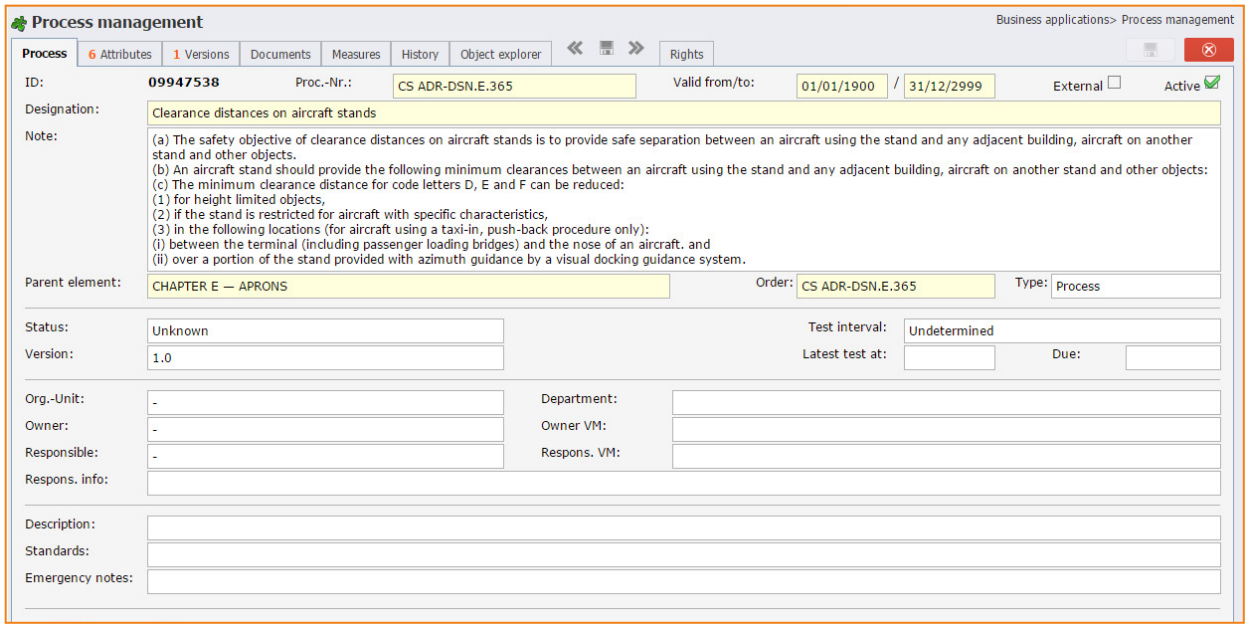
The dialogue for the maintenance of the general master data of a requirement, process or sub-system is shown below.

"Type" data field

The "Type" data field indicates whether a node is used to store the data or whether a sub-item is used to structure the data.

"Version" data field

The "Version" data field provides for the direct release of a new version number. It is at least possible to increment the version number, if data are coherently transferred to the competent authority, e.g. the zip-export, or received by it. In this way it remains clear which documents have been transferred in which version.



"Org. unit" "Department" "Manager" data field

With the "org. unit", "department", "owner" and "manager" data fields, a number of different options are available for the assignment of departments, persons or other organisational units.

"Sort" data field

The "Sort" data field enables sorting that deviates from the "process no.", if for example Roman numerals make sorting difficult.

"assigned to" data field

The "assigned to" data field determines the suspension in the hierarchical structure. If the suspension of a requirement or a sub-item is changed, this impacts on all secondary nodes.

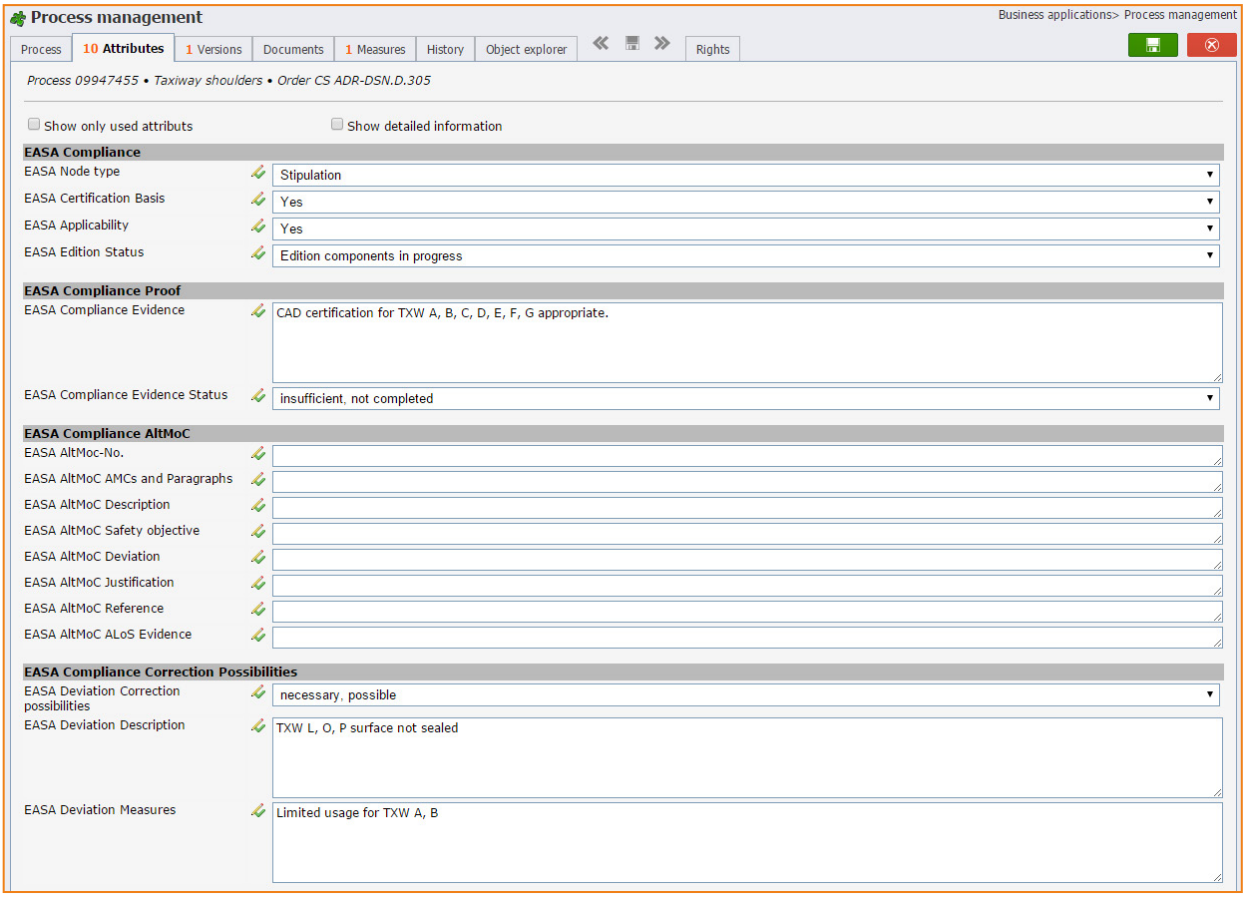
The processing of the "general data" has a far-reaching impact on the structure and requires the compliance permission "general process master data" for the relevant nodes. (see Section "7.3.3 Write and read access to compliance attributes").

6.2 Compliance attributes

In eControl terminology, compliance attributes correspond to data fields of requirements.
These appear on the compliance attributes register tab and can be freely designed by customers.

The administration and structure of compliance categories, compliance attributes and the corresponding data access permissions are described in Section „7. Data and authorisation structure“.

The compliance management module is delivered by the customer with a multitude of pre-defined attributes, which are either directly applied or simply have to be adapted to the requirements of the specific processing sequences of the customer-specific compliance management.



In the example above the logged-on user has access to the following compliance categories:

- **EASA compliance,**
- **EASA compliance - Proof,**
- **EASA compliance - AltMoC,**
- **EASA compliance - correction possibilities,**
- **EASA compliance - validation**

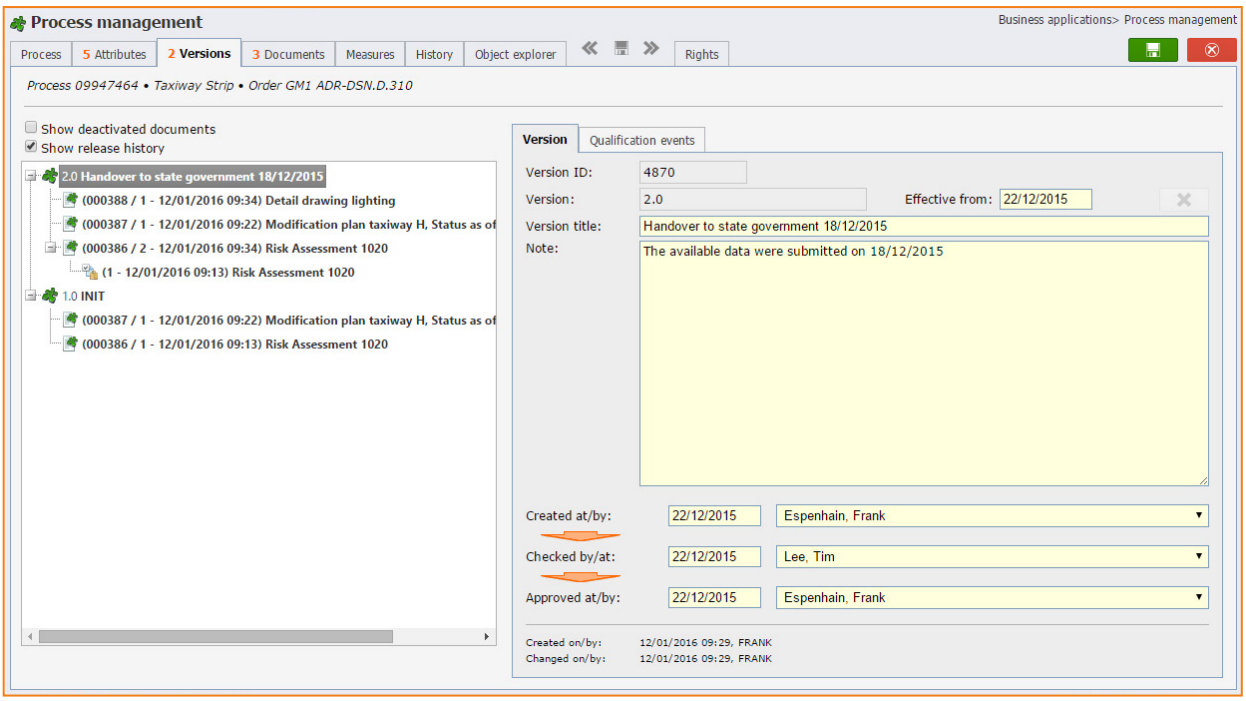
If the logged-on user has no read access to a compliance category, the relevant compliance attributes do not appear to exist for this user.

In this way each category and each requirement can be configured according to which user is to have read and, if necessary also write access.

6.3 Versions

The data fields in the register tab "Versions" provide for a systematic version management for all nodes in the system. As already mentioned, nodes can only be versioned if a node is transferred to the competent authority as a compliance sheet including the relevant documents.

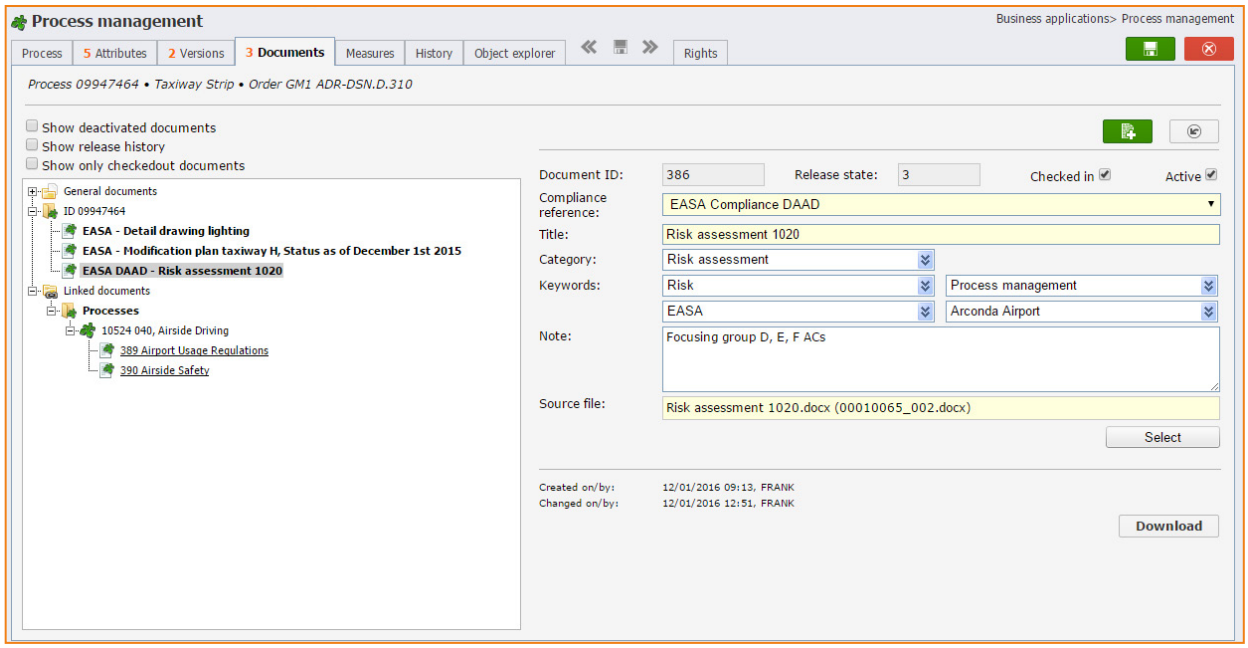
A new version is then generated at exactly the point at which the user manually places a new alpha-numeric version number in the "Version" data field (see Section “6.1 General data“).



6.4 Documents

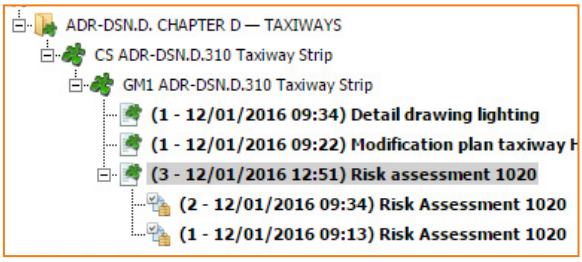
Document management is an important element of compliance management. eControl document management has a number of different intelligent functions, which enable a systematic administration of very large document files. eControl document management meets the strictest requirements of traceability and data protection.

The system has unlimited storage capacity and depends only on the storage capacity of the storage areas.



6.4.1 Traceability- automatic version management

As soon as an attached document or its descriptive metadata are changed, eControl increments the release status of this document fully automatically.



Each version of the uploaded document, including the descriptive metadata is permanently stored in the file and can be accessed at any time. Incrementation of versions can be deferred by the checking in and out of documents until a new releasable document has been compiled.

6.4.2 Data protection – reliable access control via compliance categorising

Each document is assigned to a compliance category by the user. The possibility of viewing this document or, if necessary, editing it, depends on whether the logged-on user has read or write access for the compliance category to which the document is assigned.

Thanks to this system any documents can be attached to a requirement, without having to comply with data protection restrictions. For the administration of access permissions, refer to the description of process permissions in Section "7.4.3 Process authorisations".

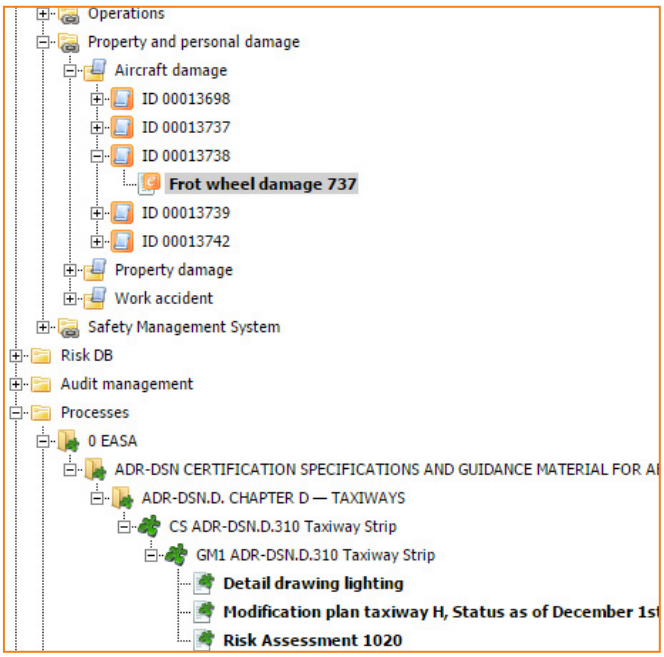
If documents have been assigned to a compliance category for which the user has no read access, he has no access to the archive containing them.

6.4.3 Administration - integration into a global archive

The structure of archives used company-wide must be specified, maintained and acknowledged by the user who is to work with the archive. Data protection requirements make it difficult to use a global archive.

eControl considerably simplifies structuring and authorisation management, because the documents are not stored separately, but only in the context of an object.

An example of the cross-object document structure, into which all compliance management documents are integrated, is shown below.



The object structure therefore defines the basic structure of the document archive. The objects are eForms, audits, risks, etc. – this structure is regularly updated and is easy for the user to understand. The storage of documents in the context of objects avoids outlay for the maintenance of the archive structure – the rights to the objects are assigned equally in terms of read and write access to the relevant documents.

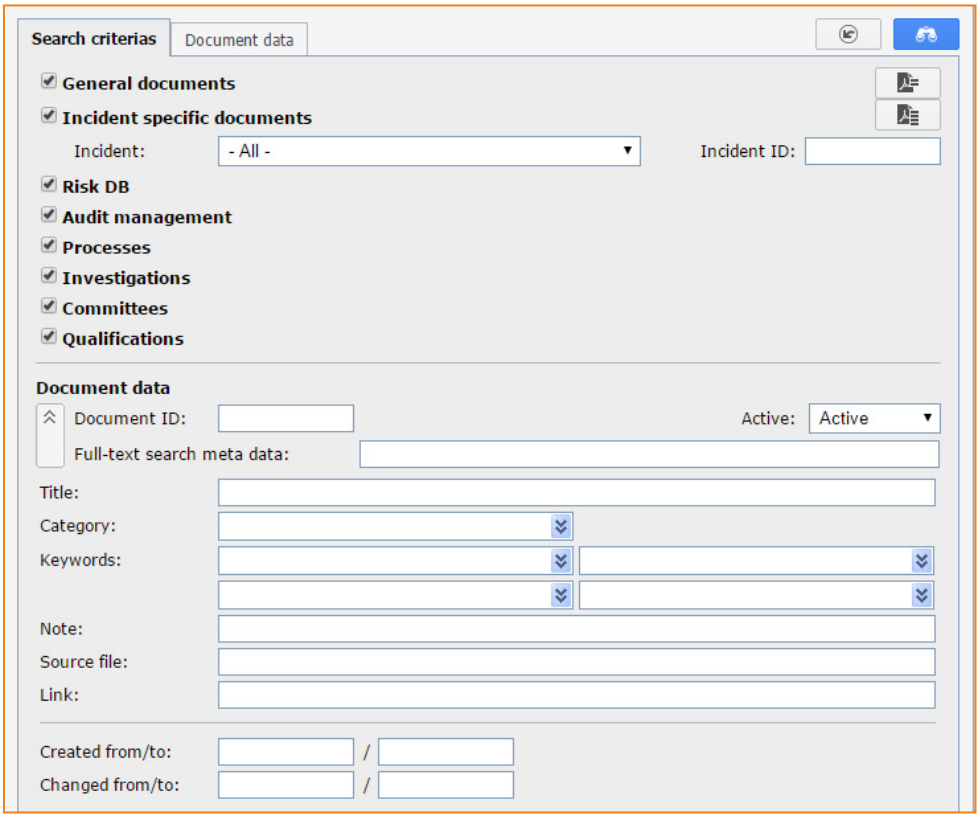
6.4.4 Search functions - metadata

For each document, in addition to the file itself, the descriptive metadata:

- Document title
- Category
- Tag 1
- Tag 2
- Tag 3
- Tag 4
- Reference text

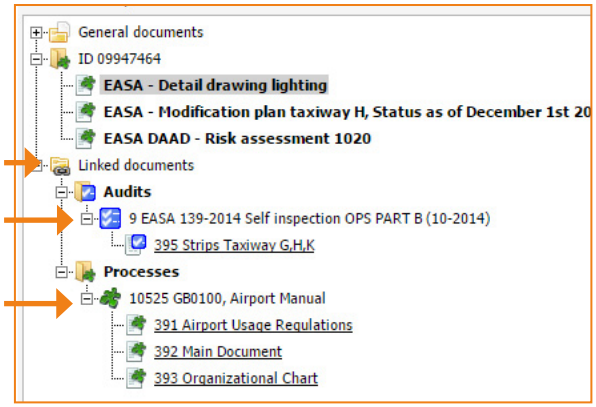
are maintained. The source file or source file name is automatically documented.

For these data fields the system provides both a differentiated search and a full-text search via all fields, by means of which a user can search the entire archive. This search only takes into account the metadata from the files to which the logged-on user has at least read access.



6.4.5 Documents and object links

Content-related objects can be permanently linked via object links. When two objects have been linked with each other, the attached documents can be viewed in both objects as so-called "linked documents", provided that the logged-on user has the appropriate authorisation.



In the example above, the object, e.g. a compliance management requirement, is linked with the audit "69 EASA 139-2014 Self inspection OPS Part B (10-2014)" and with the global airport manual "5450 GB0100, Airport Manual".

The document "983 Strips Taxiway G,H,K", is attached to the audit. The airport user regulation, the main document and the organisational chart are attached to the global airport manual. These four documents can be viewed in the context of the current object, because object links have been stored at the level of the objects.

These object links can also serve as an indicator for change management, because the object links document content-related connections that can provide valuable starting points for the change management impact chains.

6.4.6 Global documents

"Global documents" are of particular significance for compliance management, because the available documents are not clearly assigned to a specific requirement. Instead, they are required where applicable for compliance testing where there is more than one requirement. It must also be noted that these "global documents", which are assigned to several requirements, are often also maintained by other specialised departments.

The process described below enables the central maintenance of a global document by a specialised department and at the same time the use of this document by all or by the authorised specialised departments for evidence of "their" requirements.

Specification of global documents

The global documents themselves must be catalogued by the project office in collaboration with the specialised departments. The airport manual or evidence of obstacle clearance can be given as examples of global documents.

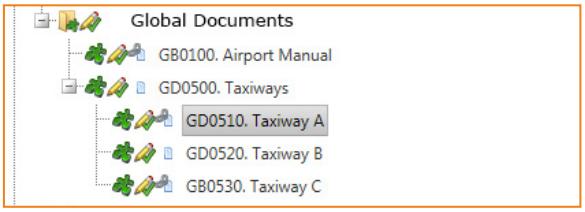
The structure, use and specified responsibilities must be communicated by the project office to all specialised departments involved.

Maintenance of global documents

The project office, in collaboration with the project offices that are hitherto responsible for the generation and updating of documents, must determine responsibility for maintaining the software for the global documents. Coordination is also required with the specialised departments that use these global documents for compliance testing and may have additional document requirements. In accordance with the recommended implementation strategy, responsibility can, where required, also be delegated to more than one specialised department or individual.

Implementation of classification structure

Global documents are generated by the project office as individual branches with a hierarchical structure in the hierarchical tree of the system. A node is created for each global document or for a group of similar documents.



For each node it can now be exactly specified which user or user groups are authorised to view and, where applicable, maintain (see Section “7.3.3 Write and read access to compliance attributes”).

If a general read access is authorised, the documents must simply be assigned to the compliance category "general process master data".

The authorisation control for global documents corresponds exactly to the authorisation control for requirements.

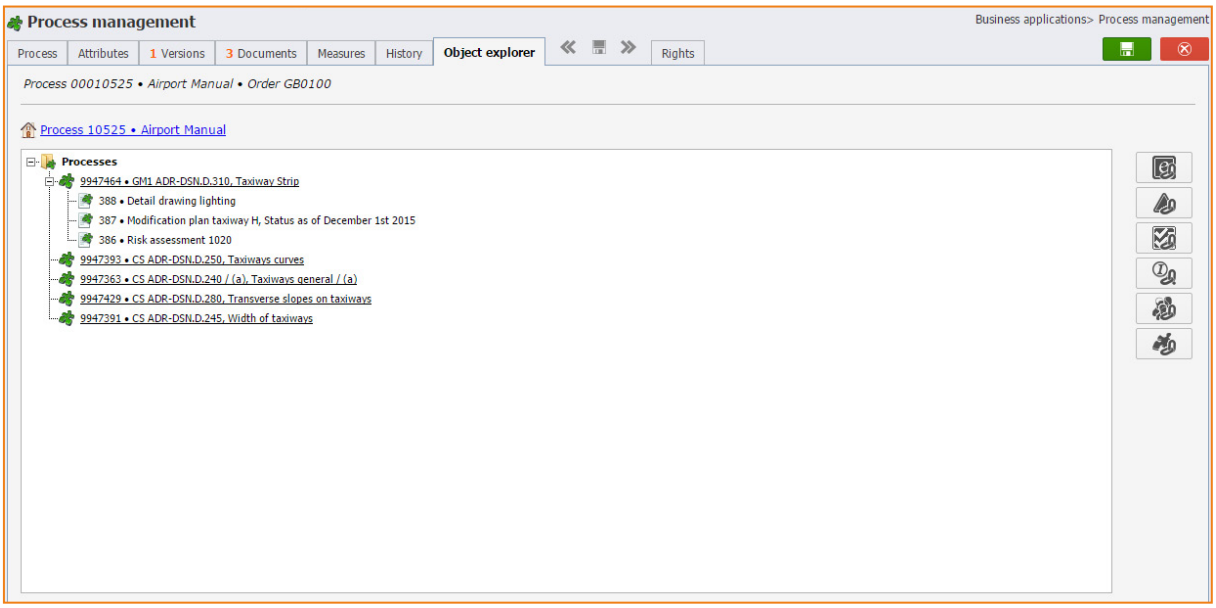
Uploading of global documents

In order to apply the classification structure shown below for the archiving of global documents, they must now, as with a requirement, be uploaded. When uploading it must be specified which compliance category the relevant document is to belong to – if the compliance category "general process master data" is selected, the document can be read by all users without specific user permissions.

Change management

Through the linking of various requirements with a global document, a connection is created that can serve as a further indicator for change management (see Section "12. Change management").

In this example, the CAD documentation for "Taxiway A" is linked with the listed requirements – in the event of changes to this taxiway, the impacts on all requirements related to this global document for the purposes of compliance testing must be verified.



6.5 Measures

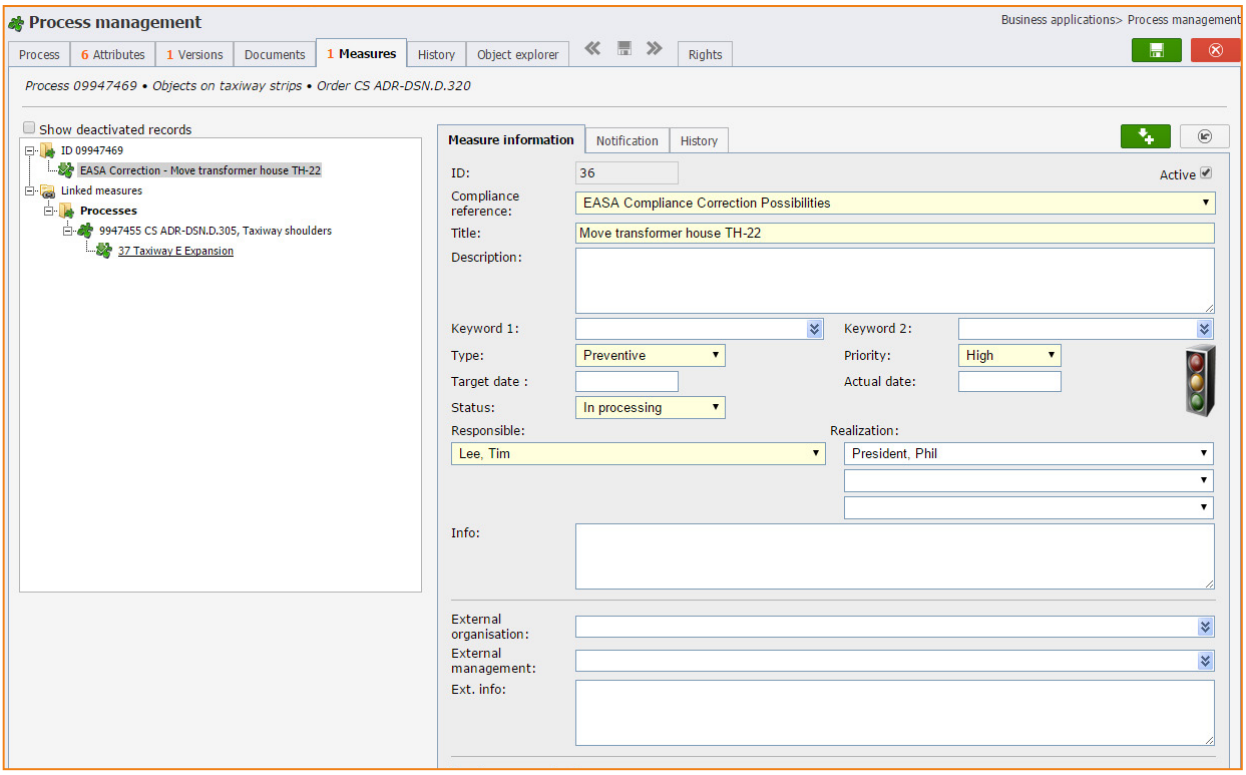
In its process management system eControl has a measure management that is standardised across the system, which must be operated in all modules in a standardised manner.

With eControl, measures

- can be planned,
- responsibility for implementation can be specified,
- the implementation dates can be monitored (traffic light control system),
- automatic reminder emails – e.g. if deadlines are exceeded – can be sent on the system,
- an efficiency test can be conducted,
- information about root cause analysis can be recorded, and
- reports on the control of all activities can be generated.

For measures in the context of requirements a compliance reference must also be specified. The authorisation of the logged-on user with regard to this compliance category determines whether the measures can be viewed and, if necessary, maintained. Additional user permissions are required in order to apply the measures (see Section "7.3.4 User permissions").

For the processing of measures, measures are also displayed by linked objects. In this way overlaps or interference with already existing measures can be avoided.



The possibilities of eControl measure management cannot be fully described here. In our opinion, measure management is part of the fine-tuning of compliance projects, which is not the focus of the compliance management module.

6.6 History

The "History" register tab documents which data field or compliance attribute has been changed by which user and when.

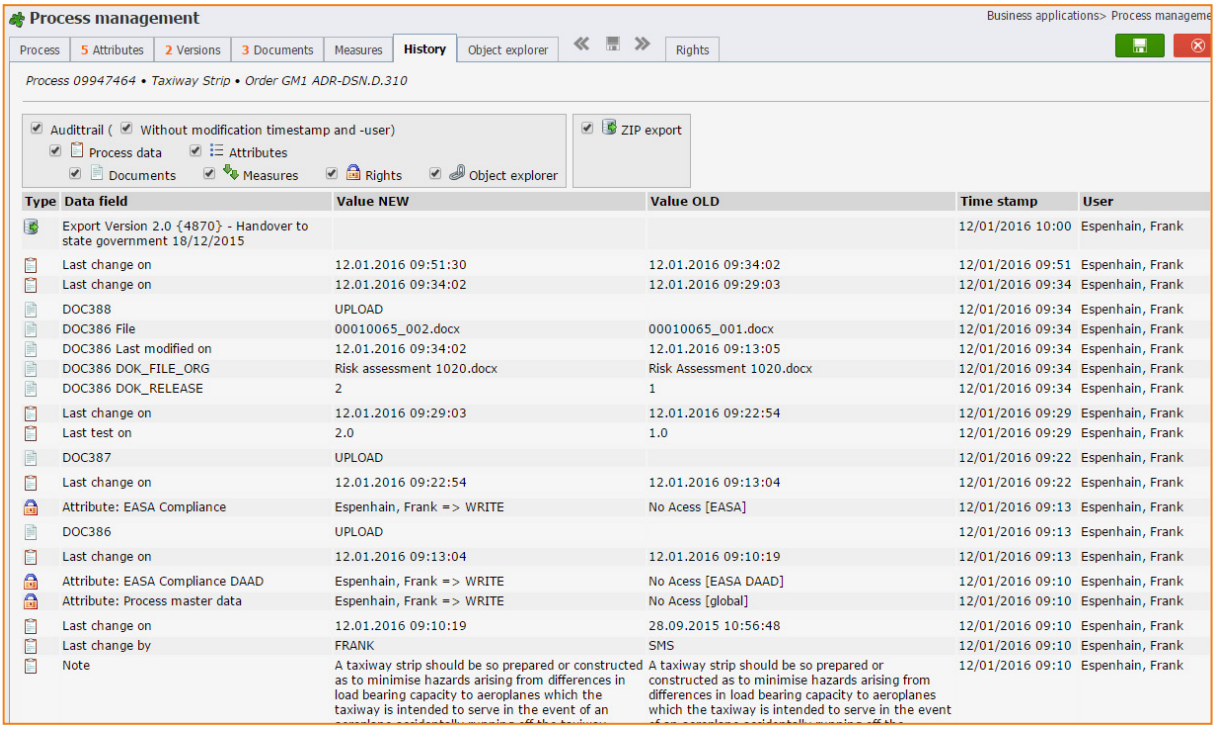
This history also comprises changes to the objects:

- documents
- measures
- permissions and
- (object) explorer links

The history register tab is available in a legible and interpretable form and can therefore be understood by every authorised user without any technical background.

Generally the availability of the "history" register tab is conditional on the user permission "process history". In order to be able to see the user who has made the relevant changes, the user permission "process history user information" is also required (see Section "7.3.4 User permissions").

The history comprises only the changes relating to the objects to which the user has access permission. If changes are made to a document that is assigned to a compliance category to which the logged-on user has no read access, these changes are no longer listed in the history.



Type	Data field	Value NEW	Value OLD	Time stamp	User
	Export Version 2.0 {4870} - Handover to state government 18/12/2015			12/01/2016 10:00	Espenhain, Frank
	Last change on	12.01.2016 09:51:30	12.01.2016 09:34:02	12/01/2016 09:51	Espenhain, Frank
	Last change on	12.01.2016 09:34:02	12.01.2016 09:29:03	12/01/2016 09:34	Espenhain, Frank
	DOC388	UPLOAD		12/01/2016 09:34	Espenhain, Frank
	DOC386 File	00010065_002.docx	00010065_001.docx	12/01/2016 09:34	Espenhain, Frank
	DOC386 Last modified on	12.01.2016 09:34:02	12.01.2016 09:13:05	12/01/2016 09:34	Espenhain, Frank
	DOC386 DOK_FILE_ORG	Risk assessment 1020.docx	Risk Assessment 1020.docx	12/01/2016 09:34	Espenhain, Frank
	DOC386 DOK_RELEASE	2	1	12/01/2016 09:34	Espenhain, Frank
	Last change on	12.01.2016 09:29:03	12.01.2016 09:22:54	12/01/2016 09:29	Espenhain, Frank
	Last test on	2.0	1.0	12/01/2016 09:29	Espenhain, Frank
	DOC387	UPLOAD		12/01/2016 09:22	Espenhain, Frank
	Last change on	12.01.2016 09:22:54	12.01.2016 09:13:04	12/01/2016 09:22	Espenhain, Frank
	Attribute: EASA Compliance	Espenhain, Frank => WRITE	No Acess [EASA]	12/01/2016 09:13	Espenhain, Frank
	DOC386	UPLOAD		12/01/2016 09:13	Espenhain, Frank
	Last change on	12.01.2016 09:13:04	12.01.2016 09:10:19	12/01/2016 09:13	Espenhain, Frank
	Attribute: EASA Compliance DAAD	Espenhain, Frank => WRITE	No Acess [EASA DAAD]	12/01/2016 09:10	Espenhain, Frank
	Attribute: Process master data	Espenhain, Frank => WRITE	No Acess [global]	12/01/2016 09:10	Espenhain, Frank
	Last change on	12.01.2016 09:10:19	28.09.2015 10:56:48	12/01/2016 09:10	Espenhain, Frank
	Last change by	FRANK	SMS	12/01/2016 09:10	Espenhain, Frank
	Note	A taxiway strip should be so prepared or constructed as to minimise hazards arising from differences in load bearing capacity to aeroplanes which the taxiway is intended to serve in the event of an	A taxiway strip should be so prepared or constructed as to minimise hazards arising from differences in load bearing capacity to aeroplanes which the taxiway is intended to serve in the event	12/01/2016 09:10	Espenhain, Frank

The change history is independently managed by the Oracle database and cannot be bypassed by the application or the user or administrator.

In its traceable system eControl documents not only the changes in the area of compliance management but also those for all data spreadsheets.

These data changes can only be viewed by correctly authorised administrators (see Section "7.3.4 User permissions").

6.7 Object explorer

The eControl object explorer enables the linking of requirements with

- events (which are available as an electronic form)
- risks
- audits
- Investigations
- safety committee meetings

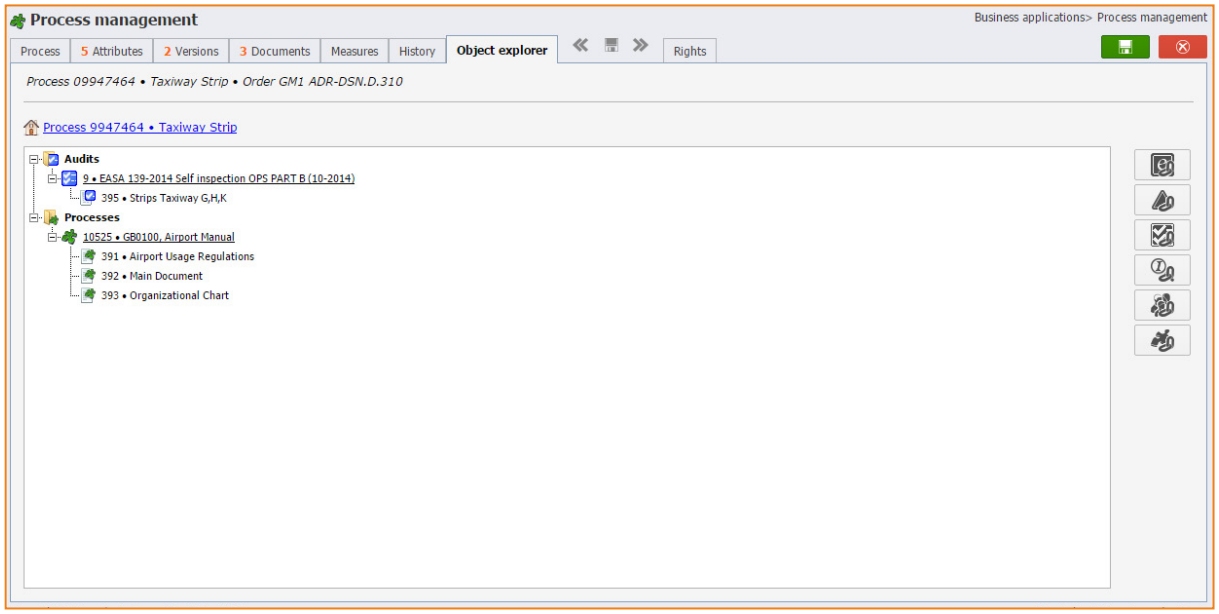
and

- processes

When a requirement is linked with an object, this connection is permanently stored and the documents (see Section "6.4.5 Documents and object links") and measures (see Section "6.5 Measures") of the linked objects are mutually visible.

This linking of requirements with other objects is also a basis for the use of global documents (see Section "6.4.6 Global documents").

Below the "Object explorer" register tab is described, which, in the example chosen, comprises a link with the audit "EASA 139-2014 Self inspection OPS PART B (10-2014)" and another link with the global document "Airport Manual", to which documents 1065, 1066 and 1067 are attached:

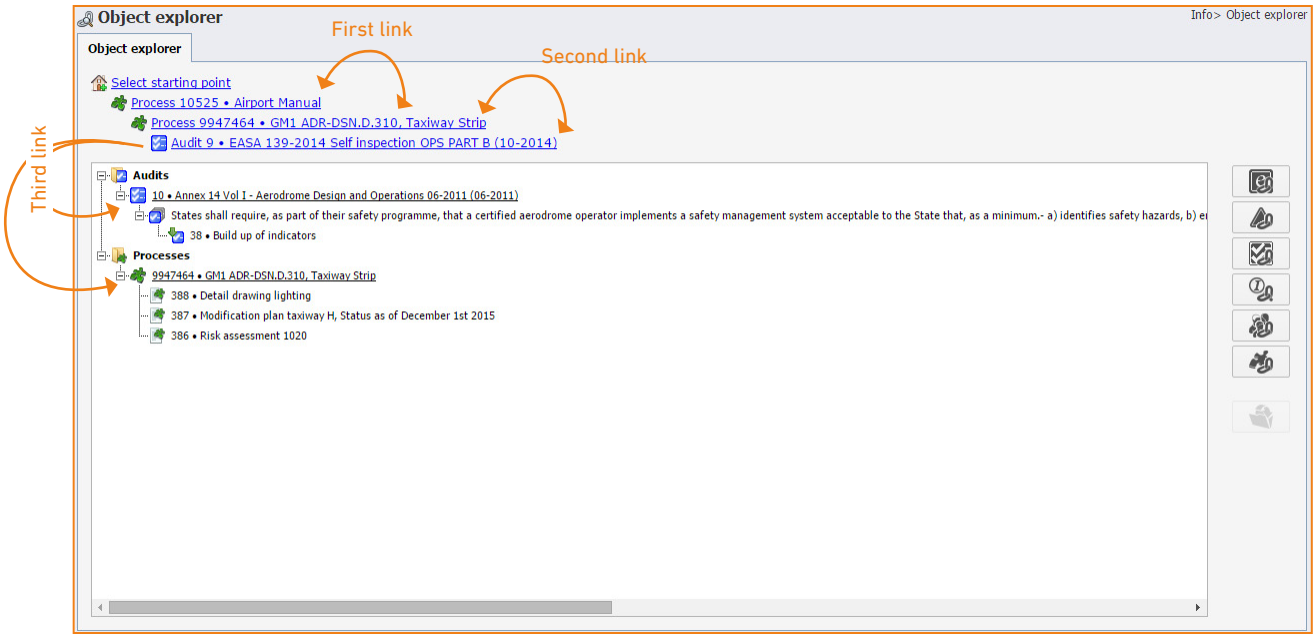


If the object explorer links are not self-explanatory, a maximum 4,000 character-long explanation can be added to the link documentation.

An object can be linked with various objects, which in their turn are linked with other objects. A "chain of objects" is produced which can be displayed via the menu item "Info -> Object explorer".

In the example shown below, the global document "Airport Manual" (object type - process) serves as a starting point. The "Airport Manual" is linked with the requirement "CS ADR-DSN.D.310, Taxiway Strip" (object type - process).

By clicking on " " the link with self-inspection "EASA 139-2014 Self inspection OPS PART B (10-2014)" is loaded. This self-inspection in turn has a link to another audit "12 Annex 14 Vol I - Aerodrome Design and Operations 06-2011 (06-2011)", for which the measure "Create 86 indicators" has been generated.



In the example chosen, the self-inspection "Audit 69" is also linked with the requirement "CS ADR-DSN.D.310 Taxiway Strip", to which documents 1079, 1080 and 1076 are attached.

7 Data and authorisation structure

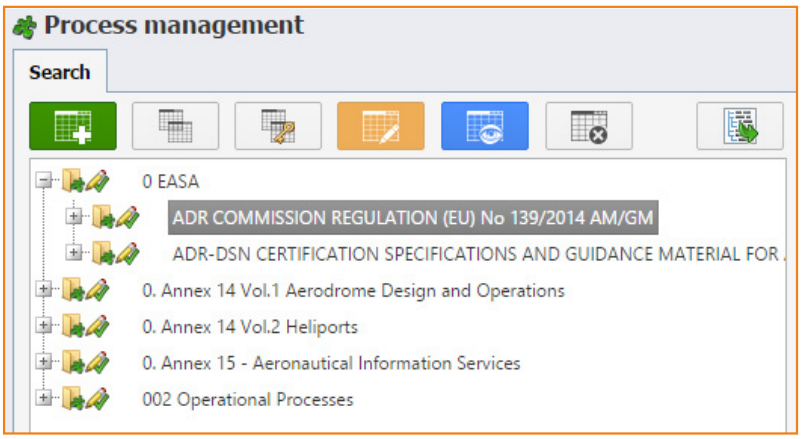
A flexible data structure and a needs-based authorisation structure are required for a company-wide application of the system and thus for a specialised compliance management.

7.1 Regulations and requirements

7.1.1 Flexible hierarchical structure

The different regulations are mapped in a hierarchical structure of sub-items and requirements. eControl services already comprise as standard a large number of regulations, which can be altered or redesigned by the customer.

As standard the "EASA" nodes are sub-divided into the branches Regulation (EU) No. "139/2014" and "Certification Specifications". If the certification bases of several different airports have to be administered, an additional hierarchy level can simply be included for the various airports below the "EASA" nodes.



For the processing of the hierarchical structuring the following basic information is available in the "process management" dialogue:

Add new sub-items or requirements

Copy new sub-item or requirement from the existing node

Copy new sub-item or requirement from the existing node and apply attributes and permissions from the source node

Edit node

View node

Shut down node or reactivate shut-down node

Maximise tree diagram

With these tools the system can be expanded and updated according to the needs of the manufacturer and customer. For example, in addition to compliance projects as such, planning approval decisions or compliance with any other regulations can be controlled.

7.1.2 User permissions for the expansion and changing of the hierarchical structure

The expansion and changing of the hierarchical structure has a significant impact on all stored data, attached data, etc. This is particularly true for the "repositioning" of nodes – in this case all nodes that are positioned hierarchically below the repositioned nodes are moved.

The repositioning of a sub-item requires the administrative data authorisation "general process master data". This authorisation is also required for versioning and authorisation control, and it should therefore be assigned as sparingly as possible.

A separate user permission is required for the generation of requirements.

7.2 Compliance categories and compliance attributes

The sequences used for the processing of the regulations can vary widely from organisation to organisation. Key factors in this regard are the size of the project team and thus the extent of the division of labour, the quality and structure of the available evidence, the approach coordinated with the relevant authorities, etc..

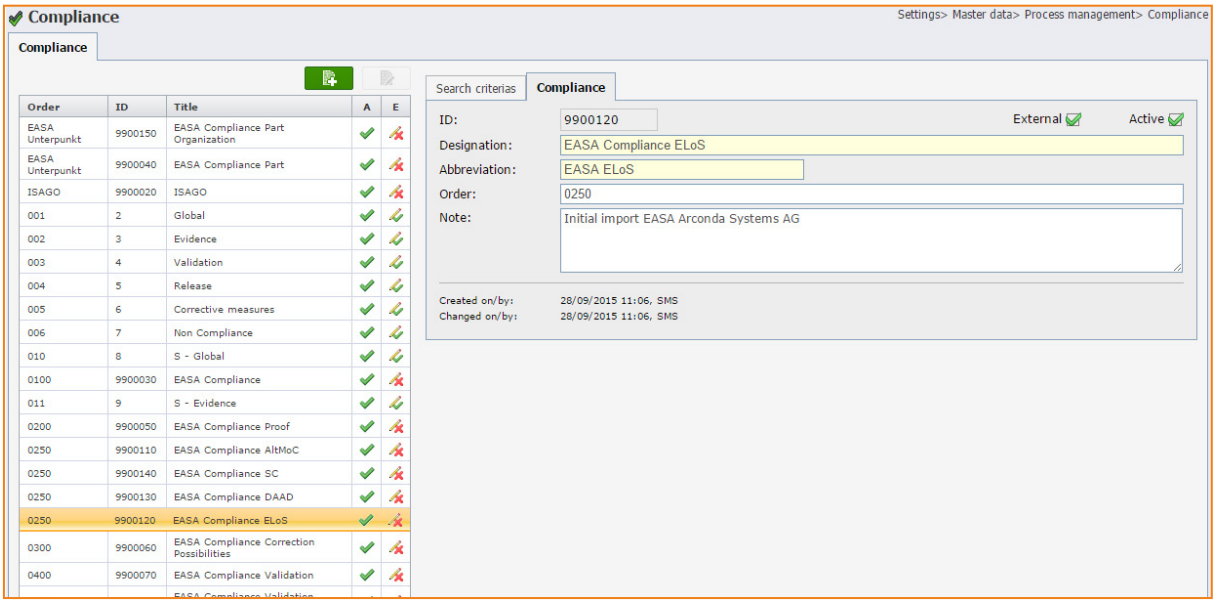
7.2.1 Compliance categories

Depending on the processing sequences a variety of data fields and user permissions are required for the systematic control of the compliance project.

The data fields can be individually generated as compliance attributes for requirements. In order to simplify the user permissions for these compliance attributes and to structure the data optimally, several compliance attributes can be grouped into compliance categories.

Each node and all sub-items and requirements have as standard the compliance category "general process master data", which can be viewed by all users without further authorisation.

In addition to this compliance category "general process master data", other categories can be created, to which other data fields or compliance attributes must then be assigned.

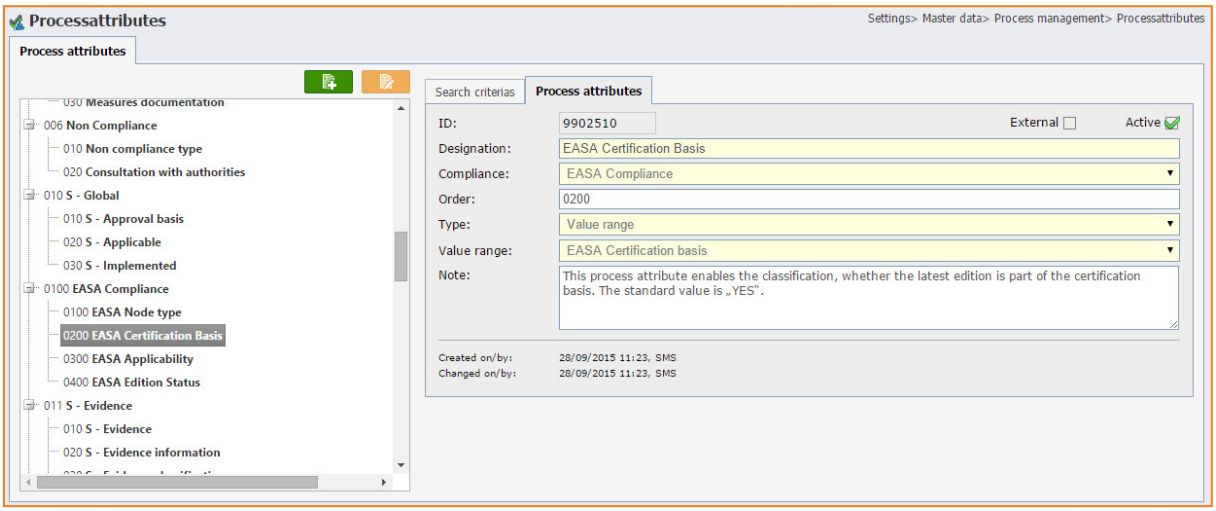


As standard, eControl is already equipped with a number of different compliance categories, which can be adjusted where required (see Section “7.2.1 Compliance categories”).

7.2.2 Compliance attributes for requirements

The compliance attributes are data fields that can be generated by the customer. eControl has four different field types for the definition of attributes:

Text	Text field for the storage of a text with a maximum of 4,000 characters
Value range	List box from a value range (see Section "7.2.3 Value range")
Date	Data field for the recording of date values
Numeric	Data field for the recording of numerical values

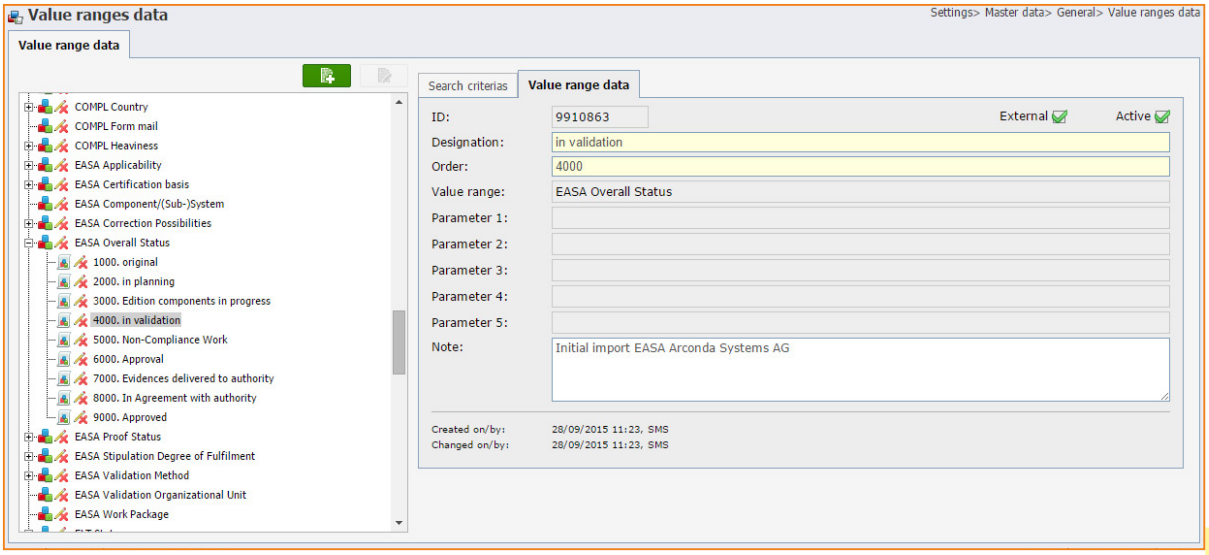


For each attribute an explanatory text can be added in the "reference" field, which is displayed as mouseover text during the subsequent processing of the requirements, in order to help the processor.

7.2.3 Value range

Value ranges and list boxes can also be generated where required. For every list box any number of values (value range data) can be organised, which can then be used for a compliance attribute of the value range type.

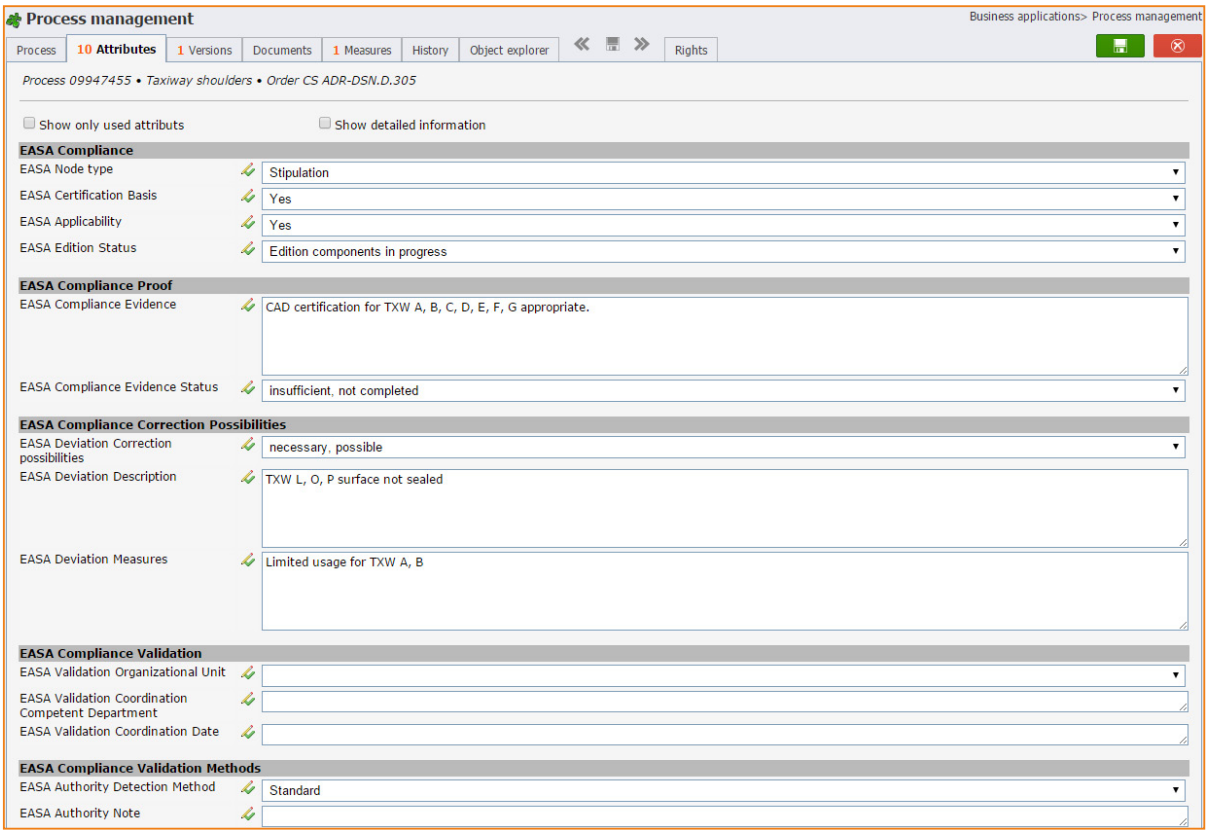
For this purpose a compliance attribute of the "value range" type must be defined and the previously generated value range must be stated for the list box.



7.2.4 Reference data structure

Extensive reference attributes are already available to the manufacturer for the application of compliance management with regard to airports and competent authorities and these simplify and accelerate the use of the system.

The references shown below can be most effectively applied for the processing sequence described in the sub-item "step-by-step towards compliance".



In addition to the compliance attributes mentioned above, data fields exist for AltMoCs and the deviation types ELoS, DAAD and SC, which can also be "cut in" as required.

Corresponding compliance categories for these deviation types are provided for the control of access rights and structuring of data.

The example listed below shows the compliance attributes for the compliance category "Alternative Means of Compliance (AltMoC)":

EASA Compliance AltMoC	
EASA AltMoc-No.	
EASA AltMoC AMCs and Paragraphs	
EASA AltMoC Description	
EASA AltMoC Safety objective	
EASA AltMoC Deviation	
EASA AltMoC Justification	
EASA AltMoC Reference	
EASA AltMoC ALoS Evidence	

7.3 Authorisation structure

7.3.1 Design

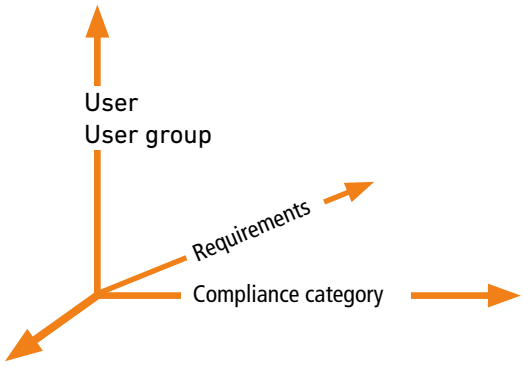
The eControl authorisation structure ensures an application-specific access to and processing of compliance attributes. The authorisation procedure therefore supports a number of different processing sequences in the form desired.

eControl can therefore be applied company-wide and be made available to all specialised departments that are integrated into specialised compliance projects. A project team can in this way be ideally assisted by the specialised departments, thus freeing up experts for the processing of deviations.

The compliance project can be broken down into work packages, each of which comprises several requirements, for which the write and read permissions of the individual users must be set.

All compliance attributes (= requirement data fields) are assigned to compliance categories, by means of which access is controlled.

In order to administer the user permissions more easily and flexibly, authorisations can be specified for users and user groups.



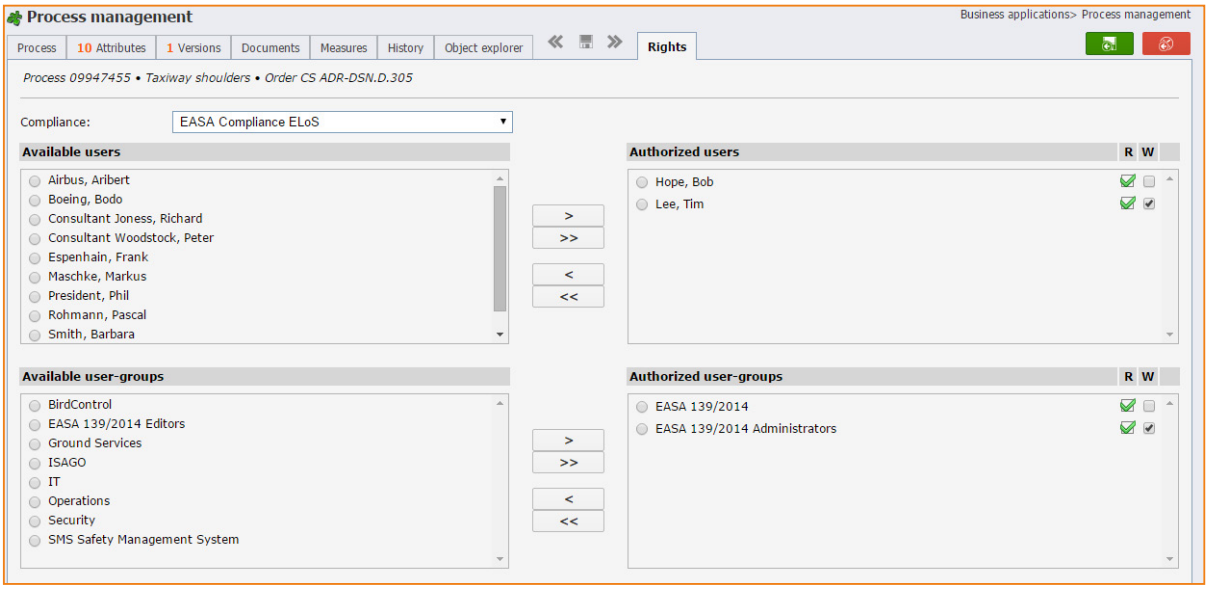
In this way the authorisation structure of eControl authorises both extensive user permissions – e.g. for the project manager – and very limited user permissions – e.g. the merging of existing documents for individual requirements.

7.3.2 Administration - users and user groups

The authorisation structure should be organised as simply and transparently as possible and be easy to change.

The use of user groups is – where possible - preferred.

In user management one person can easily be added to a user group. All authorisation settings for this user group are automatically transferred to the additional person. Correspondingly the user group settings can be adjusted to changing requirements and are transferred automatically to all users who are assigned to the changed user group.



7.3.3 Write and read access to compliance attributes

The authorisation structure of the system provides for a needs-based control of the compliance attributes, in order to fulfil the requirements of a specialised compliance management.

The read access "R" (Read) is required for read access to all compliance attributes in a compliance category.

The write access "W" (Write) must also be assigned for the processing of the attributes.

The authorisations are individually set for each requirement and for each node. Write access to the compliance category "general process master data" is required for the setting of the authorisations.

Each user who has this access permission can assign authorisations to or withdraw them from all users. This permission must therefore be assigned sparingly.

Organisationally eControl therefore provides the option of delegating access management for parts of the standard to a variety of specialist administrators.

All processes, regulations and sub-systems are recognisable for each user as nodes, and a user must always read the "general process master data". For all other compliance categories, however, special user permissions must be assigned. This authorisation logic applies not only for compliance attributes but also equally for all documents and measures that are attached to the relevant requirements.

Documents and measures can be read or processed if the logged-on user has read or write access to the compliance category to which these documents and measures are attached. However, the "general process master data" are an exception. Documents and measures that are assigned to the general personnel master data can be viewed by all users without further user permissions – they are therefore published.

The read and write access permissions assigned for the compliance categories are tracked in the history (see Section "6.6 History") of the relevant requirement.

7.3.4 User permissions

eControl has some general user permissions, with which basis functional authorisations are assigned. These user permissions are assigned in the "user master data" dialogue. The administration of user permissions is an administrative activity, during which all authorisation settings can be changed.

Edit public process queries
The user is authorised to store queries publicly or globally, in order to make them available to all users (see Section "8.10 Global query definitions").

Edit SQL process queries
The user is authorised to use freely definable SQL statements to query requirements, processes and sub-systems. The assignment of the authorisation must be very limited, because SQL queries can be used to bypass the authorisation logic of the system.

Process history
The user permission processing history provides a processing history of all data fields for which the user has at least read access.

Process history user information
This permission supplements the processing history with information about which user has made the relevant change.

Process permissions administration
This permission gives an administrator the right to assign large numbers of authorisations to requirements, processes and sub-systems. This right therefore implicitly makes it possible for the administrator to grant himself access to all compliance categories and should therefore only be granted to IT administrators and if necessary specialised administrators.

Create processes/systems
This user permission authorises the user to set up new nodes or additional requirements, processes or sub-systems. The assignment of this permission should also be limited, in order to ensure the proper organisation of the hierarchical structure of the data and avoid "proliferation". If no additional requirement needs to be set up, but repositioning within the structure is required, write access to the "general process master data" of the relevant node is required – this can subsequently be "repositioned" as desired.

Compliance/Standards
This user permission enables compliance categories to be generated and processed, in order to restructure attributes or bundle together new attributes.
This user permission should be granted exclusively to specialised administrators.

Process attributes
This user permission enables the master data of existing compliance attributes to be maintained or additional compliance attributes to be created and assigned to a compliance category. This user permission should also be granted exclusively to specialised administrators.

Edit value ranges
This user permission authorises a user to create new value ranges or list boxes and to edit existing list boxes. The data structure of the value ranges is used in all software modules in the system, and therefore edit should be reserved for the system administration and specialised administrators only.

Master data value range data
This user permission authorises a user to add to and change the individual list box values. This user permission should also be reserved for the system administration and specialised administrators. In this regard a basic knowledge of relational databases is required in order not to inadvertently compromise the interpretation of historical databases.

Global symbols
The user permission "global symbols" authorises the user to generate global tiles, which each user can then select in the start menu (see Section “8.11 Start menu“).

Edit users
The user permission "edit users" enables the generation and processing of users. This also includes the assignment of user and data access permissions.

The user permission "edit users" allows the user to bypass all authorisation structures and must be assigned very sparingly. The permission "edit users" is equivalent to unlimited access to all data in the system.

Read risk database
The user permission "read risk database" is required for read access to the risks in the risk database and the attached documents and measures (see Section “10. RiskDB - eControl risk database“).

Edit risk database
The user permission "Edit risk database" is required for the processing of the risk database and the attached documents and measures (see Section “10. RiskDB - eControl risk database“).

Read measures
The user permission "read measures" is required across the system for read access to measures (see Section “6.5 Measures“). This user permission is required for a user to participate in measure management.

Edit measures
The user permission "Edit measures" is required across the system for the generation and processing of measures (see Section “6.5 Measures“). This user permission is required for the generation of a measure for a requirement as well as write access to the relevant compliance category to which the measure is to be assigned.

Notifications measures
The user permission "notifications measures" is required for the definition of automatic measure notifications by e-mail (see Section “6.5 Measures“), which can be sent fully automatically by the system depending on deadlines and other events.

Read object links
The user permission "read object links" is required across the system for the inspection of existing object links (see Section “6.7 Object explorer“). If this permission is not assigned, the object links are not displayed on the register tab, and the associated documents and measures of linked objects are not visible.

Edit object links
The user permission "edit object links" is required for the generation and processing of object links (see Section “6.7 Object explorer“).

Read audit trail
The user permission "read audit trail" enables the user to view all data changes in the system via the "audit trail" report.

With this user permission all data changes to all objects can be viewed, irrespective of the authorisation of the logged-on user – the complex authorisation system of eControl is not valid in this case.

The user permission "read audit trail" must therefore be reserved for the technical administrators. The interpretation requires in-depth knowledge of the data model in the case of relational databases.

A data dictionary is available for eControl. However, for reliable information it is advisable to contact the manufacturer.

7.4 Permissions assignment documentation

eControl makes available reports for the verification of the structure and authorisations, the most significant of which are listed here.

7.4.1 Structure of process attributes

This report documents the structure of the compliance categories and compliance attributes. It is a master data report of the system, for which no specific user permissions are required.

9900030	**EASA Compliance**	EASA	✓
9902520	**EASA Applicability**	Value range	✓
Note:	This process attribute documents, whether the latest edition is applicable within the recent EASA certification. The standard value is „YES".		
9902510	**EASA Certification Basis**	Value range	✓
Note:	This process attribute enables the classification, whether the latest edition is part of the certification basis. The standard value is „YES".		
9902530	**EASA Edition Status**	Value range	✓
Note:	This process attributes displays the total edition status for the edition considering all assigned edition components. This process attribute is of central importance for the compliance's valuation and the edit progress. New editions will get the status „original".		
9902500	**EASA Node type**	Value range	✓
Note:	This process attribute serves to classify EASA nodes in edition and edition componentents in order to facilitate the systematic filtering. All editions shall carry the status „Edition".		
9900110	**EASA Compliance AltMoC**	EASA AltMoC	✓
9902820	**EASA AltMoC ALoS Evidence**	Text attribute	✓
Note:	This process attribute serves for the in note form given evidence of the acceptable safety level (ALoS) or the results of the corresponding Risk Assessments. Max. 4.000 Characters Field Length.		
9902760	**EASA AltMoC AMCs and Paragraphs**	Text attribute	✓
Note:	This process attribute serves to specify the Acceptable Means of Compliance and Paragraphs of the EASA standard. An alternative detection method shall be agreed with the authority for this standard. Max. 4.000 Characters Field Length.		
9902770	**EASA AltMoC Description**	Text attribute	✓
Note:	This process attribute serves to describe the alternative detection method. Max. 4.000 Characters Field Length.		
9902790	**EASA AltMoC Deviation**	Text attribute	✓
Note:	This process attribute describes the deviation of the Alternative Means of Compliance (AltMoC) towards the Acceptable Means of Compliance (AMC). Max. 4.000 Characters Field Length.		
9902800	**EASA AltMoC Justification**	Text attribute	✓
Note:	This process attribute describes the justification, that evaluates the Alternative Means of Compliance and Acceptable Means of Compliance as equivalent. Max. 4.000 Characters Field Length.		
9902810	**EASA AltMoC Reference**	Text attribute	✓
Note:	This process attribute serves to document another airport and if necessary member state, for which are already applied the Alternative Means of Compliance. Max. 4.000 Characters Field Length.		
9902780	**EASA AltMoC Safety objective**	Text attribute	✓
Note:	This process attribute serves to describe in note form the safety objective, for that an alternative detection method is used. Max. 4.000 Characters Field Length.		
9902750	**EASA AltMoc-No.**	Text attribute	✓
Note:	This process attribute serves to save the alphanumeric AltMoc-No. Max. 4.000 Characters Field Length.		
9900060	**EASA Compliance Correction Possibilities**	EASA Correction	✓
9902560	**EASA Deviation Correction possibilities**	Value range	✓
Note:	This process gives information about the correction possibilites, that are for the removal of Non-Compliance. New editions will get the status „open".		
9902570	**EASA Deviation Description**	Text attribute	✓

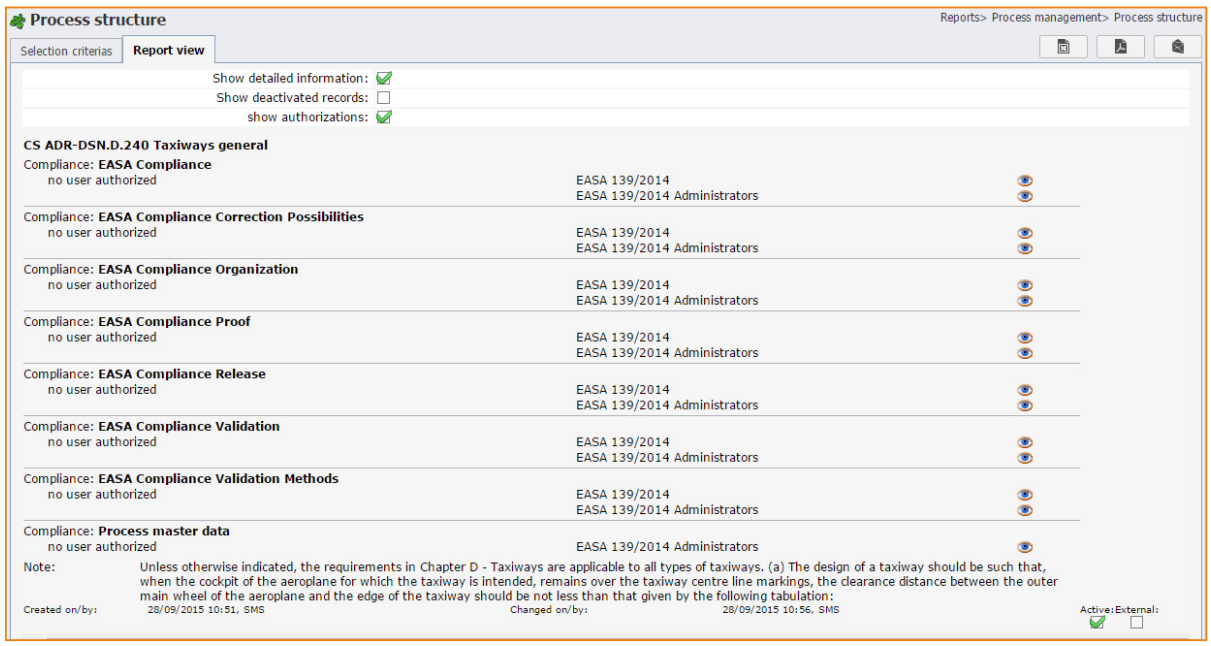
7.4.2 Process structure

This report documents the hierarchical structure of the requirements and sub-systems. Universal filter criteria make it possible to document the requirements for each specialised department or process progress.

In this way work packages or areas of responsibility can be coherently displayed.

Provided that the logged-on user has the user permission:

"Processing permissions of administrators across all specialised departments" (see Section "7.3.4 User permissions").



7.4.3 Process authorisations

The report "process authorisations" documents which user has access to the compliance categories of the relevant nodes.

The report can essentially be retrieved in three different forms:

- Processes / compliance category / user
- User / processes / compliance category
- User / compliance category / processes

Processes / compliance category / user
For each process the report describes for each compliance category which users have read and write access to the data fields, documents and measures. This report accurately describes the extent of the access permissions for individual requirements.

User / processes / compliance category
For each user the report describes for each process to which compliance category the user has read or write access. This report accurately documents the total extent of the user permissions of a user or a group of users.

User / compliance category / processes
For each user the report describes for each compliance category to which processes the user has read or write access. This version of the report summarises the compliance categories for each user and thus describes whether the appropriate data access permissions have been assigned for the intended involvement of the relevant users in the processing sequences.

8 Compliance management cockpit

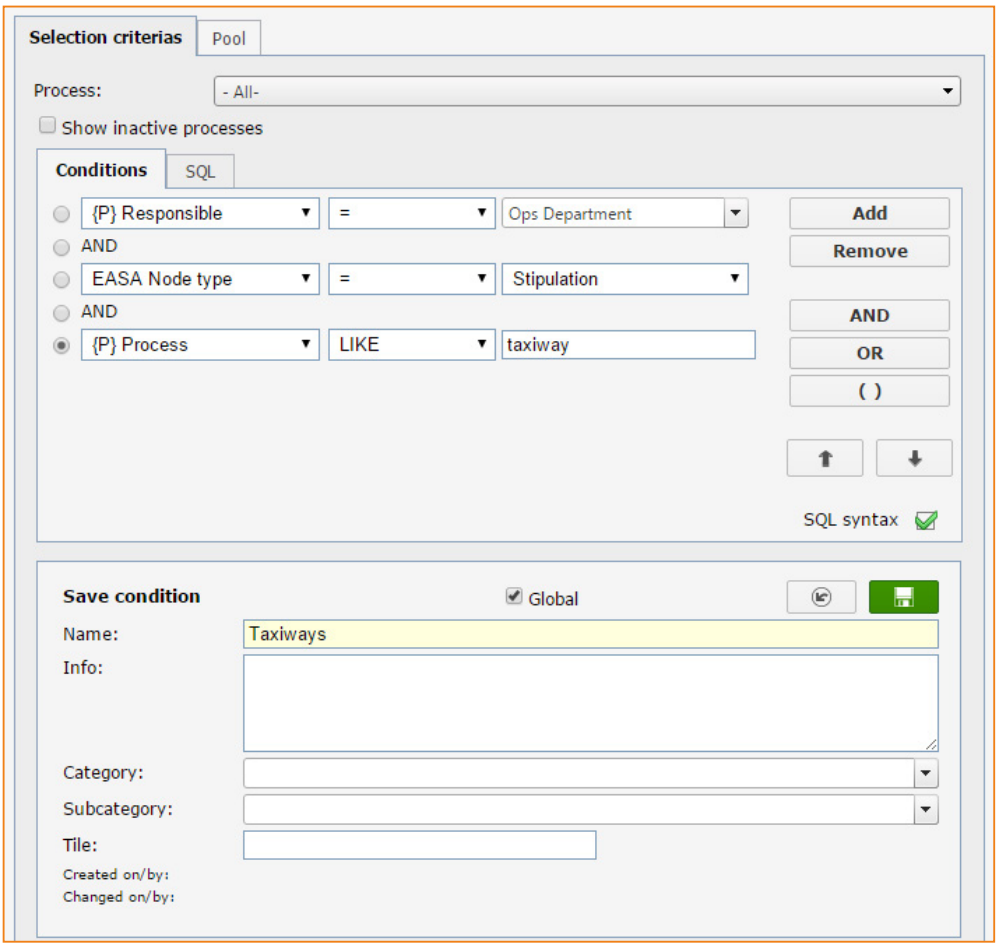
8.1 Summary

The selection of requirements depends on the processing sequence, the compliance categories, the established compliance attributes, the permissions of the users and a number of other factors.

eControl provides a standardised compliance management cockpit for the filtering of requirements. This cockpit is used for:

- Processing of requirements
- Reports and statistics
- Authorisation management

In this way the filter, which has already been defined by the user for the filtering of the requirements of a specialised department, can also serve for example, without modification, to express a status list for this specialised department.

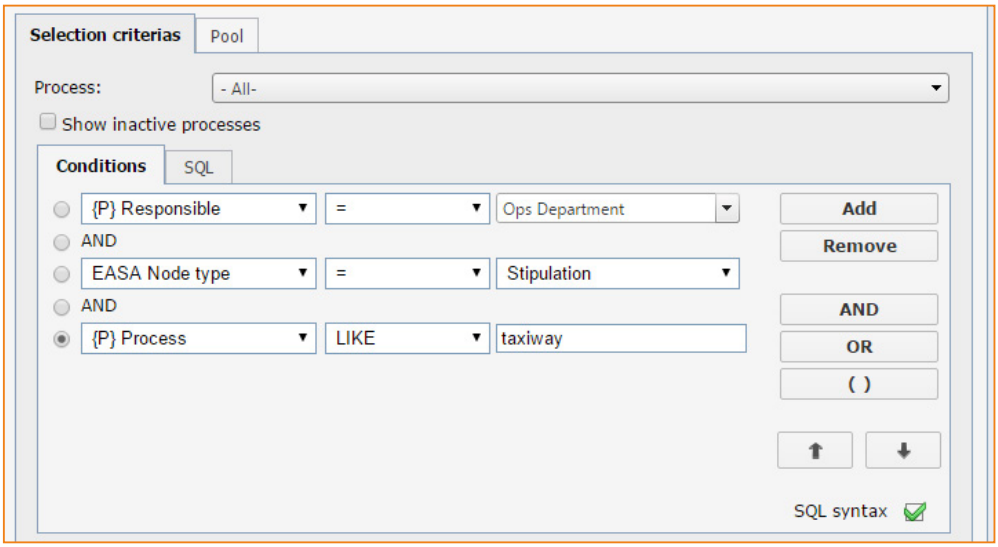


eControl enables the free definition of compliance categories, compliance attributes and an assignment of permissions based on these. For this reason a selection dialogue must be structured in a completely variable way. In order to make it as easy as possible for the user to operate the system, the same selection dialogue is used in each dialogue.

8.2 Query generator

8.2.1 Summary

The compliance management cockpit enables requirements to be filtered by means of each compliance attribute. This is done with a universal condition generator, by means of which one or more compliance attributes can be used via comparison operators and reference values to formulate filter conditions.



8.2.2 Logical operators "AND" and "OR"

To formulate complex conditions the logical operators AND and OR are also available plus brackets.

(condition1 **AND** condition2) **OR** (condition3 **AND** condition4)

8.2.3 Comparison operators

The comparison operators available for the formulation of conditions depend on the type of compliance attribute (see Section "7.2.2 Compliance attributes for requirements").

Text	=, <>, LIKE (includes)
Value range	=, <>, IS ZERO (is empty) IS NOT ZERO (is not empty)
Datum	=, <>,<,>,<=,>=
Numerisch	=, <>,<,>,<=,>=

In the example above a compound condition has been defined for the filtering of nodes. The individual elements can be added or deleted via the buttons on the right-hand margin of the dialogue.

Add Add new sub-condition

Remove	Remove selected sub-condition
AND	Add "AND" logical operator
OR	Add "OR" logical operator
( )	Add an opening and a closing bracket
⬆ ⬇	Move selected sub-condition, operator or bracket up or down a line

The specific example shows a condition composed of three sub-conditions. The first condition " {P} Responsible | = | Ops Department " reduces the nodes to those that the Ops department have as the responsible department.

The {P} prefix of the compliance attribute indicates that it is a compliance attribute of the "general process master data".

This first sub-condition is linked via the operator " AND " in the second line with the second sub-condition in the third line.

The second sub-condition " EASA Node type | = | Stipulation " also filters onto all "condition" type nodes. In this way all sub-condition node types are excluded. The approximately 280 conditions from Regulation (EU) No. 139/2014 and the certification specification (C/S) remain. In this connection, knowledge of the reference data structure (see Section "7.2.4 Reference data structure") is required.

The second and third sub-conditions are also combined in line 4 with the logical operator " AND ". In this way the desired nodes or requirements must meet condition 1 as well as conditions 2 and 3.

Condition 3 in line 5 states that the data field "{P} process title" must contain the word "taxiway". The system refrains from complete compliance with the word "taxiway", because the comparison operator "LIKE" has been used. "LIKE" is available for text attributes and finds all elements that contain at least the text – irrespective of upper or lower case.

8.3 System validation

In particular when formulating a complex query logical errors can inadvertently occur in the formulation of queries.

With the help of the Oracle database the system independently checks the syntax of all queries.

" SQL Syntax ☑ "

denotes a logically correct query

whilst the missing diacritic

" SQL Syntax ☐ "

describes a logically incorrect statement.

Essentially the formulation of queries requires a certain analytical understanding as well as, of course, knowledge of the compliance attributes – the user must at least know which data are stored

according to which rules in which compliance attributes.

In any case it is assumed that the members of the compliance management team meet these requirements. If it is necessary to define more complex queries, these can be defined by the project office as "global" and made available to the specialised departments (see Section “8.10 Global query definitions“).

8.4 Which right?

The compliance management cockpit is available to every eControl user. According to the authorisation standards of the system, only requirements to which the logged-on user has at least read access can be filtered. Requirements for which an "ELoS" has been agreed can be searched for under the following simple condition:

However, the system will only display the requirements for which an ELoS has been agreed and for which the logged-on user also has read access. In this way the "ELoS" information via the "ELoS" compliance category can be controlled in such a way that each specialised department can only view its own "ELoS" requirements.

8.5 SQL queries

If the multiple query generation options do not fulfil the specialised filter criteria, SQL queries can be used, with which the entire database can be queried without restrictions.

For the formulation of these queries the additional user permission

"Edit SQL process queries" (see Section “7.3.4 User permissions“)

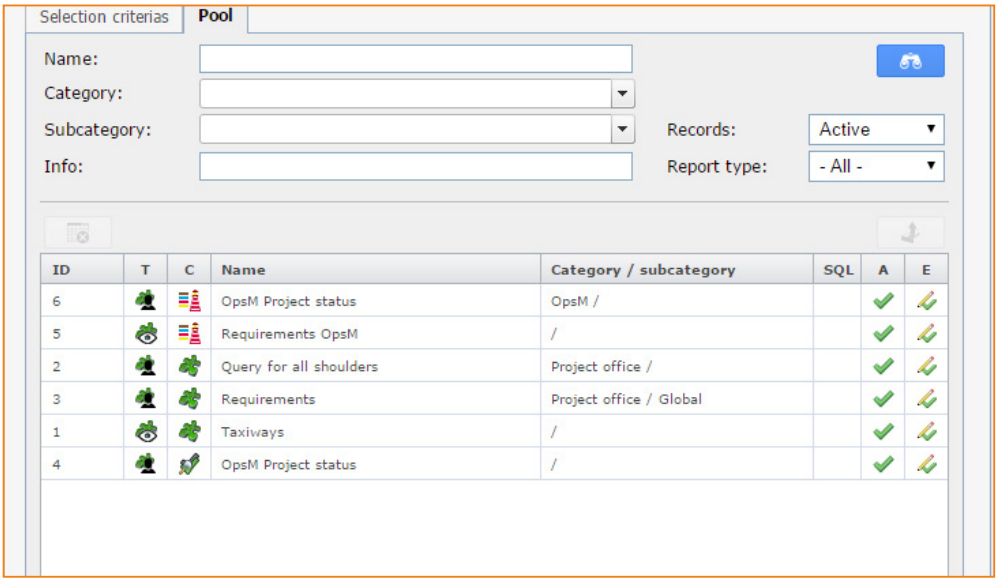
is required, because the use of SQL queries bypasses the user permissions (see Section “8.4 Which right?“).

It is however possible for each user to insert pre-defined globally defined queries, which are based on SQL statements. Modification of the SQL query statements – and thus potential abuse – requires in turn the administrative user permission mentioned above.

It must be noted that data access permissions are not essentially taken into account when SQL queries are used, neither for the person who has generated the query, nor for the persons who insert the query.

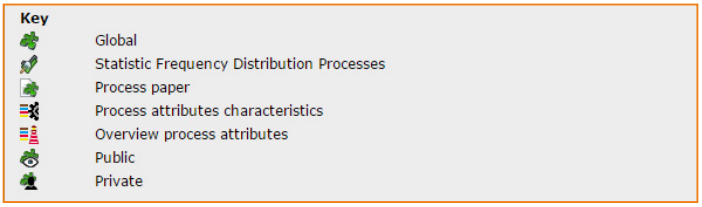
8.6 Query pool - reusable queries

With eControl query definitions can be stored and reused at the press of a button. In this way a complex query definition can be used more than once.



The "pool" of queries listed on the register tab can be loaded into the selection criteria by clicking the " " button. Then the process tree is automatically filtered according to the loaded criteria.

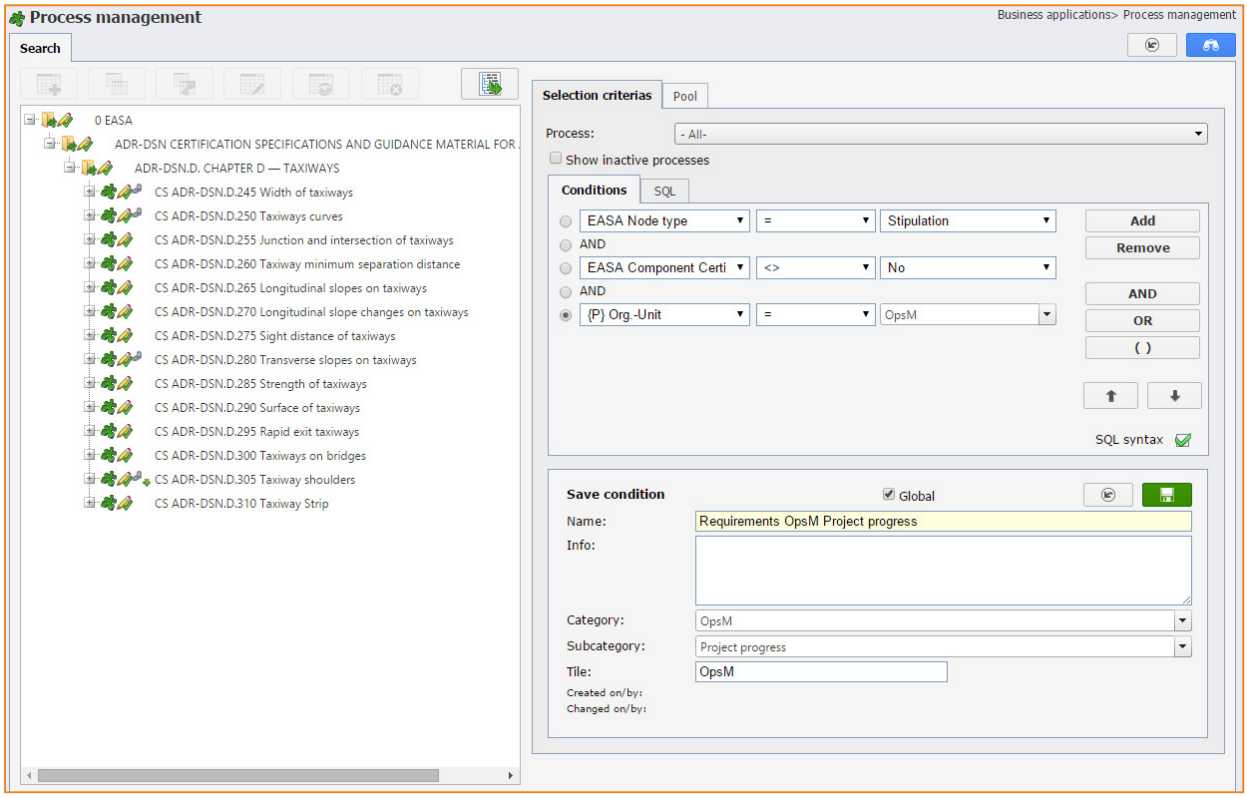
With the query definitions described in Section "8.2 Query generator" report settings are also stored, provided that the condition definition has been stored in the context of a report. The same report can be reproduced with minimal outlay. The specific query types must be removed from the key in the lower section of the pool definition, although the context in which a query definition has been generated can be accessed by means of the symbols.



All query types are available for selection for the processing of requirements or of the dialogue "process master data".

8.7 Storage of query definitions

For the storage of queries in the query pool, refer again to the example given in Section “8.2 Query generator”.



In order to systematically store the query definitions and locate them easily later, the following settings can be stored in the dialogue area "store condition definitions":

- Name
- Requirements
- OpsM
- Project progress

Name
The "Name" field gives the query a suitable title and thus describes the content of the query.

Info
When reusing this query, the info-text makes it easier to understand which requirements are filtered according to which criteria and for what purpose.

Category
This is a data field that categorises or groups queries. They are categorised here according to specialised department. If there is more than one query definition for the "OpsM" specialised department, these can be found easily.

Already used categories can be loaded via the drop-down menu. It is advisable to load terms via the drop-down menu, in order to avoid spelling mistakes.

Sub-category
This data fields sub-categorises or sub-groups queries. They are sub-categorised according to project progress. In this way further queries for "overdue requirements", "deviations" etc. are predefined. Here also, already used categories can be loaded via the drop-down menu.

Tiles
This data field pre-sets a tile text, if the query in the start menu needs to be linked with the menu item "process management"(see Section “8.11 Start menu“).

8.8 Change in existing query definitions

When changing an existing query definition, this must be stored again under the name of the query to be overwritten – if necessary report settings to be stored are also updated.

8.9 Deletion of query definitions

Queries can be deleted by operating the " " button.

8.10 Global query definitions

As standard each user has access to his own queries and the “global queries”.

In this way an overview is preserved – even if a high number of users has generated a multitude of individual queries over time.

Global queries can be prepared, for example by the project office or by the IT department and then used by all users.
In this way users who only use the system infrequently can also work with complex queries.
The generation of global queries requires the administrative user permission.

“Maintenance of public process queries” **(see Section “7.3.4 User permissions“)**

The undesired inflationary use of global query definitions is avoided and the quality of global queries is successfully safeguarded.

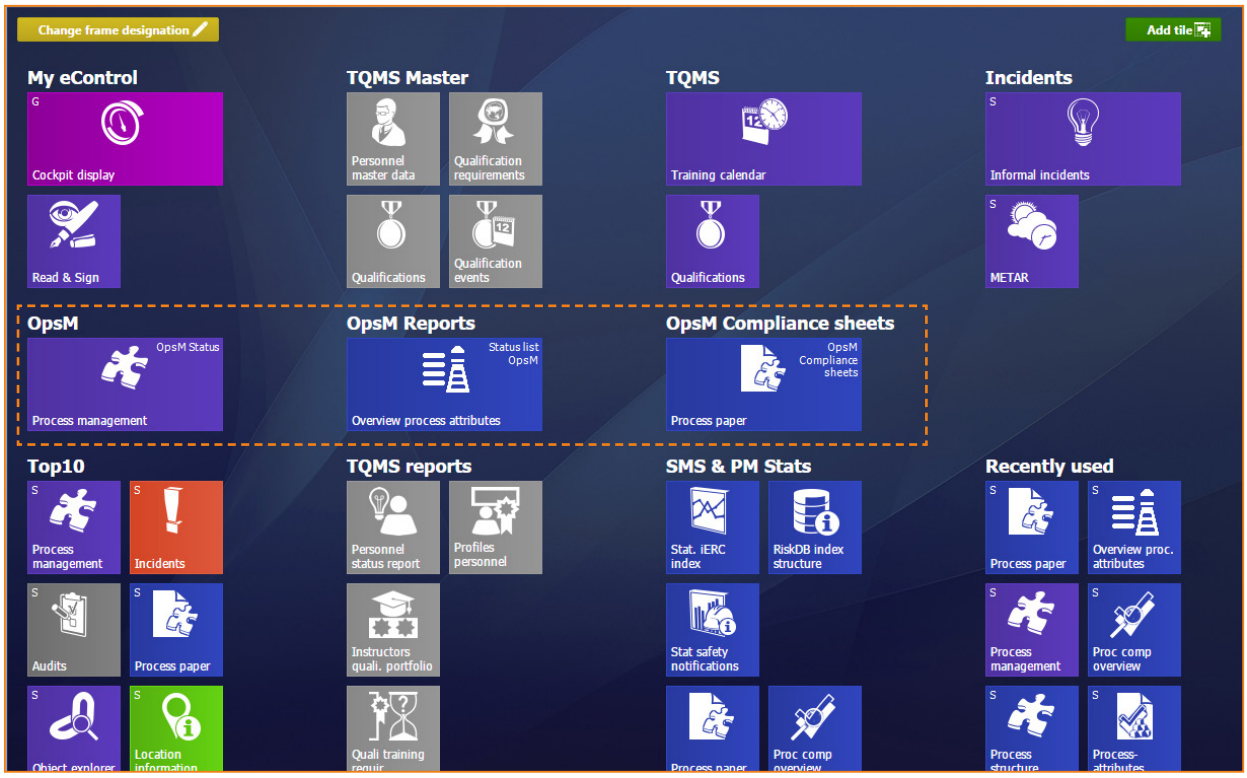
Data protection requirements are not compromised by the definition of global queries. Essentially a global query definition can be implemented by every user – however, only requirements to which the relevant user has at least read access are filtered. The SQL queries are an exception. (see Section “8.5 SQL queries“).

8.11 Start menu

The eControl start menu has a quick selection facility for the most frequently used menu items. The menu points of the process management can also be linked with query definitions – the opening of a report including a complex query definition and a multitude of report settings are reduced at the single click of a mouse.

In the example shown below the start menu of the logged-on user "Konstantin Sorge" comprises the tiles

- **"OpsM Status" process management**
- **Summary of process attributes "OpsM status list"**
- **"OpsM compliance sheets" process sheet**



The same report can be put more than once on the start menu, linked with different queries. In this way for example the status lists of several specialised departments can be predefined and stored.

Basically, each user can independently update the precise tiles that he needs for a quick selection of menu points.

If some tiles are to be displayed to all users, the user permission

"Global symbols" (see Section "7.3.4 User permissions")

is required. It is also possible to assign symbols specifically to individual users, however they also require user permission

"Edit user" (see Section "7.3.4 User permissions")

9 Reporting

The most important reports for the project management of compliance management projects are listed below

A number of reports for the verification of the process and authorisation structure are also available, and these are described in Section "7.4 Permissions assignment documentation" .

9.1 Standard reporting functions

The user interface for reporting in eControl is standardised.

Compliance-Management-Cockit
The compliance management cockpit (see Section "8. Compliance management cockpit") & (chapter „8.2") is available for the definition of queries and the reuse of stored statements.

Compliance reports – storage of report parameters
As well as the query definitions, all report settings, dynamic column structure, display options etc. can be stored for reuse for all compliance management reports.

Selection criteria documentation
The set selection criteria is automatically printed in the report header, in order to document restrictions.

CSV format for data processing
Every report can be stored in CSV format and therefore used digitally – for example with MS Excel, for a more in-depth statistical analysis.

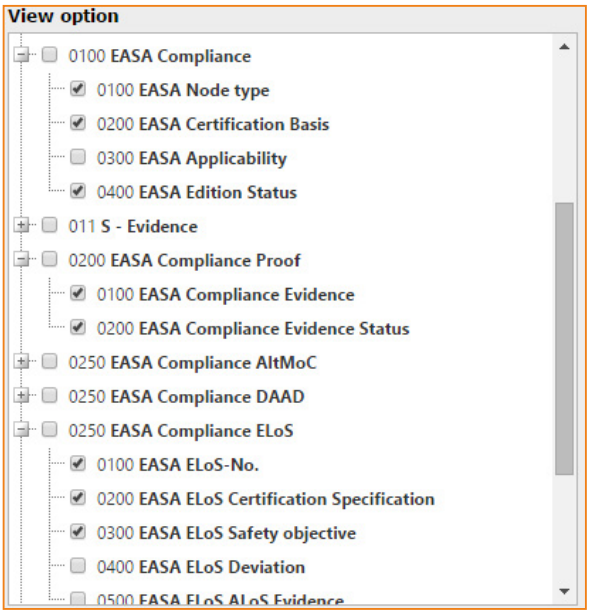
PDF e-mail dispatch
The standard dispatch method is the PDF format, whereby all reports can be sent as an attached email directly via the integrated email client.

9.2 Summary of process attributes

The "process attributes summary" is a key report about the generation of status lists.

The required status lists are a reflection of the processing sequences and their structure must vary sufficiently.

In order to be able to organise the structure of status lists clearly and adequately, the system has a hierarchical structure of compliance category and compliance attributes, from which the desired columns of the reports can be extracted at the click of a mouse.



The above-mentioned hierarchical element enables both the selection of the individual compliance categories and the selection of the "general process master data".

Overview process attributes

Reports> Process management> Overview process attributes

Selection criterias | **Report view**

Process: CERTIFICATION SPECIFICATIONS AND GUIDANCE MATERIAL FOR AERODROMES
EASA Compliance: EASA Certification Basis, EASA Applicability, EASA Edition Status
EASA Compliance Proof: EASA Compliance Evidence Status
Selection criteria: EASA Node type = Stipulation
AND
{P} Process LIKE taxi
Order: Process master data - Order

Process ID	Proc.-Nr.	Designation	EASA Certification Basis	EASA Applicability	EASA Edition Status	EASA Compliance Evidence Status
9947391	CS ADR-DSN.D.245	**Width of taxiways**	Yes	Yes	Edition components in progress	insufficient, not completed
9947393	CS ADR-DSN.D.250	**Taxiways curves**	Yes	Yes	Edition components in progress	sufficient
9947399	CS ADR-DSN.D.255	**Junction and intersection of taxiways**	Yes	Yes	in validation	sufficient
9947403	CS ADR-DSN.D.260	**Taxiway minimum separation distance**	Yes	Yes	in validation	sufficient
9947412	CS ADR-DSN.D.265	**Longitudinal slopes on taxiways**	Yes	Yes	Edition components in progress	insufficient, not completed
9947417	CS ADR-DSN.D.270	**Longitudinal slope changes on taxiways**	Yes	Yes	Edition components in progress	insufficient, not completed
9947423	CS ADR-DSN.D.275	**Sight distance of taxiways**	Yes	Yes	in validation	insufficient, not completed
9947429	CS ADR-DSN.D.280	**Transverse slopes on taxiways**	Yes	Yes	Edition components in progress	insufficient, not completed
9947434	CS ADR-DSN.D.285	**Strength of taxiways**	Yes	Yes	original	unknown
9947436	CS ADR-DSN.D.290	**Surface of taxiways**	Yes	Yes	Non-Compliance Work	unknown
9947440	CS ADR-DSN.D.295	**Rapid exit taxiways**	Yes	Yes	in validation	sufficient
9947450	CS ADR-DSN.D.300	**Taxiways on bridges**	No	Yes	original	unknown
9947455	CS ADR-DSN.D.305	**Taxiway shoulders**	Yes	Yes	Edition components in progress	insufficient, not completed

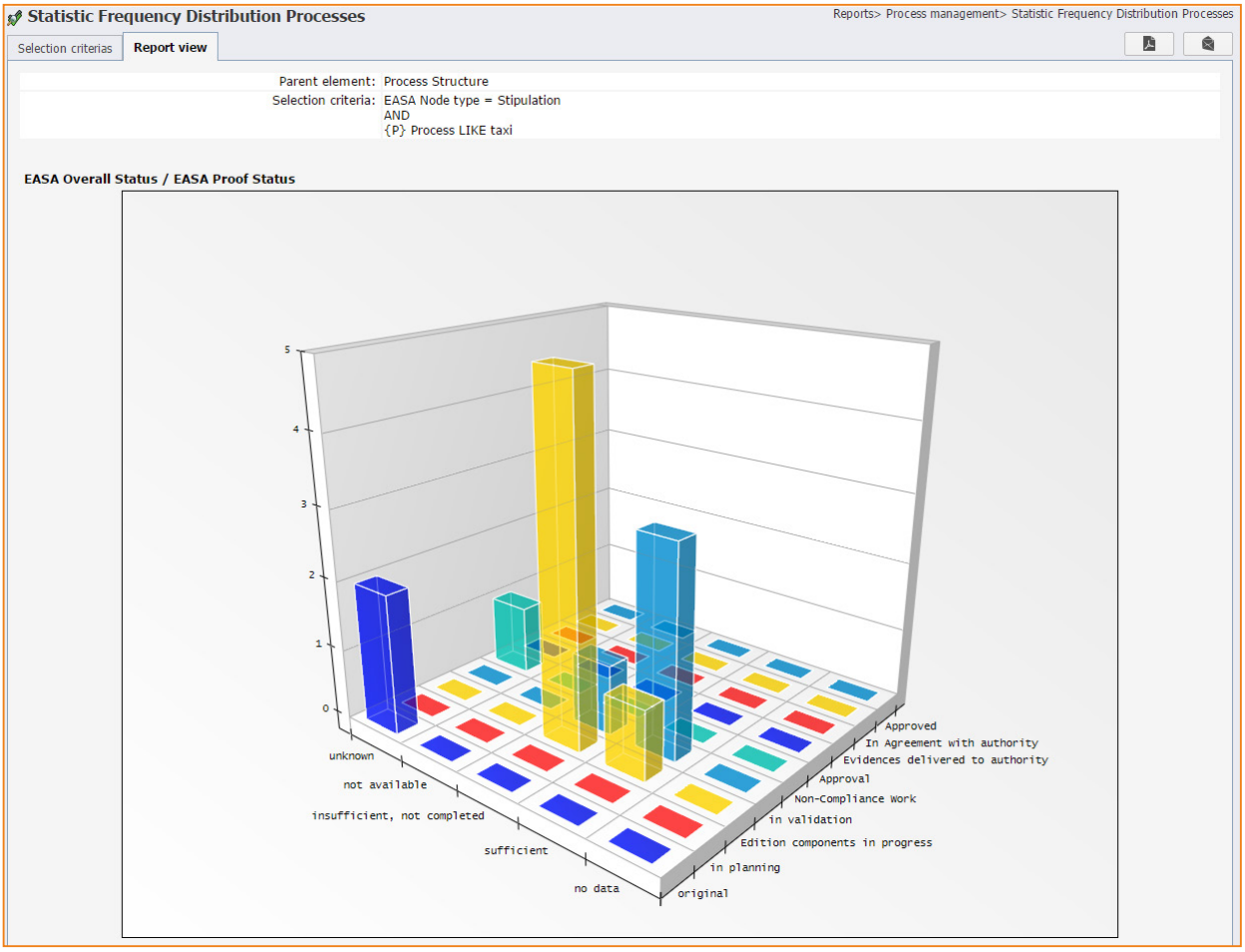
The report structure and the filter settings made can be stored and reused. For further information, please refer to the compliance management cockpit (see Section “8. Compliance management cockpit“) & (chapter „8.2“).

9.3 Frequently distribution processes

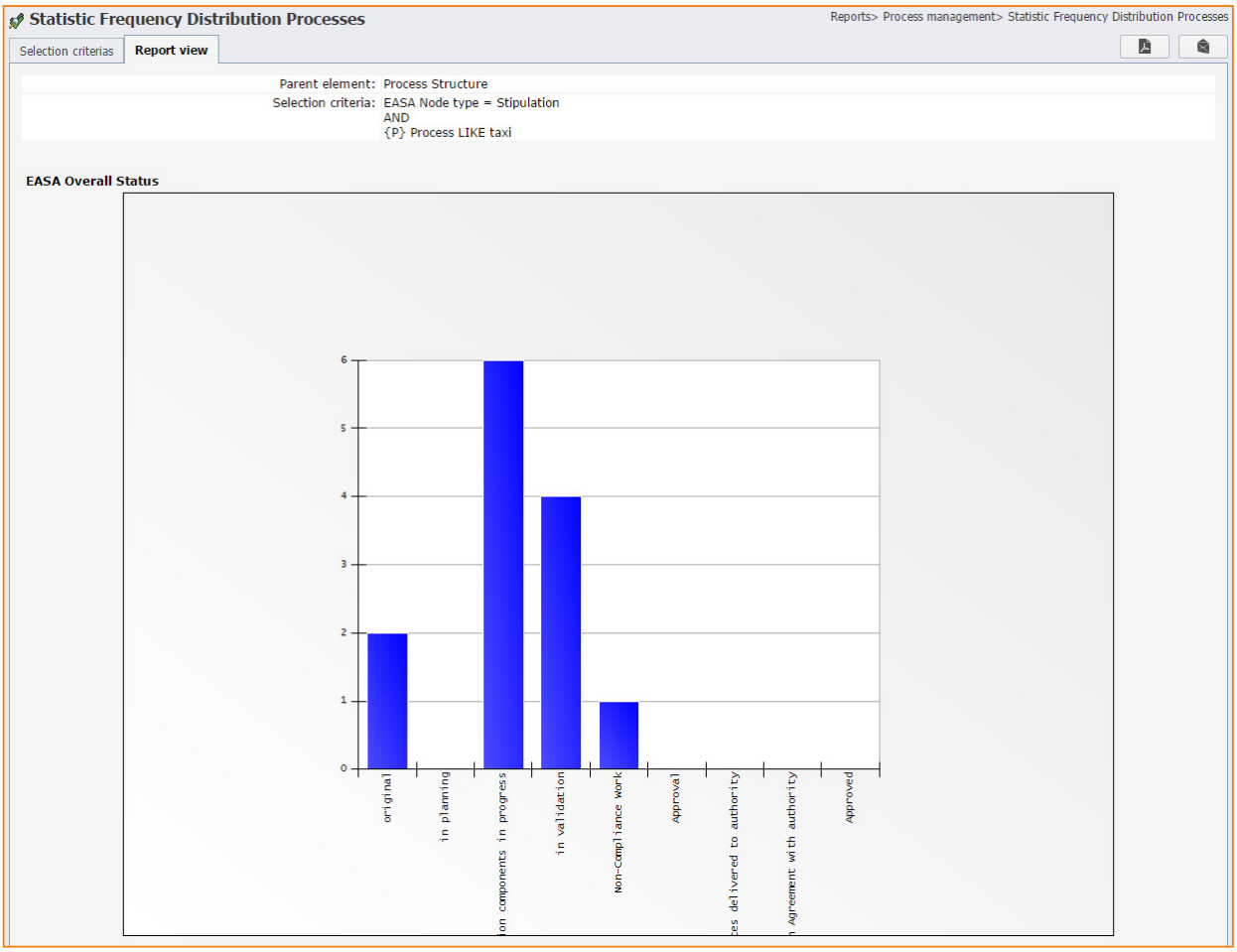
The "frequency distribution processes" statistic provides charts for the frequency distribution of compliance attributes. Essentially all "value range" type compliance attributes (see Section "7.2.2 Compliance attributes for requirements") can be used, provided that they do not have more than 10 items of value range data (see Section "7.2.3 Value range"). This graphic illustration is particularly useful for seeing project progress at a glance. Because a single graphic illustration often does not carry enough weight, the same data can be displayed one below the other in five different ways.

For these frequency distributions both two-dimensional bar charts and three-dimensional cross-tabulation analyses can be generated. The cross-tabulation analyses provide for the comparison of two different criteria, whilst the two-dimensional bar charts provide frequency distributions of a compliance attribute.

Three-dimensional cross-tabulation illustration



Two-dimensional bar chart



As an attachment for each filtered requirement, a maximum of five further data fields can also be printed in list form for documentation purposes.

This attachment is printed below the chart(s).

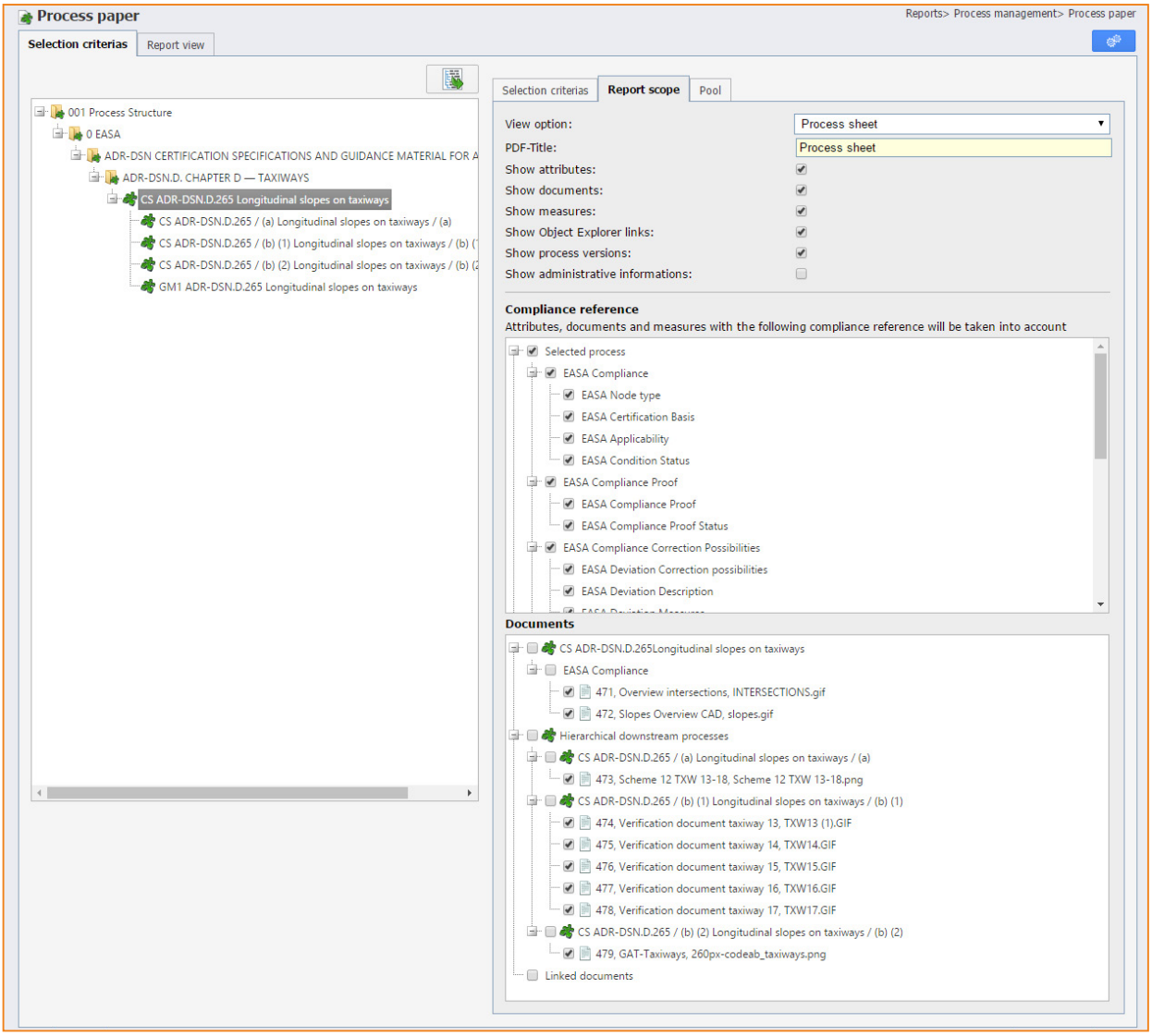
9.4 Process and compliance sheet

The "Process paper" report is used to summarise the documentation of all data stored for a requirement, process or for a sub-system. As well as generating a report, it provides the option to merge any selected attachments in a ZIP file and export them in this way.

The "Process paper" report displays the same data in different forms. The process sheet is divided into different sections and enables all available data to be printed. The compliance sheet has a rather more limited scope and is used specifically to format documents and compliance attributes.

	Process sheet	Compliance sheet
Requirements (-master data)	mandatory	mandatory
Compliance attributes	optional	mandatory
Documents	optional	optional
Measures	optional	optional
Object Explorer	optional	no
Version information	optional	no
Administrative information (Time stamp for creation and update)	optional	no

In the example shown below, a compliance sheet for the requirement “CS ADR-DSN.D.265 Longitudinal slopes on taxiways” should be generated. This requirement has been divided into sub-requirements a, b.1 and b.2, which in turn comprise supporting documents and compliance data.



9.4.1 Report structure – Targeted formatting of content for addresses

This report generator is very flexible so that exactly the required content and report elements can be gathered for each recipient. In general, process and compliance sheets can summarise the content of the selected requirement and all hierarchically downstream sub-requirements in an overall report.

For the selected requirement the following content can be included in the report:

- **Requirement master data**
- **(Compliance) attributes** **(see Section "6.2 Compliance attributes")**
- **Documents**
  - Documents, that are assigned to the current requirement
  - Documents from linked objects
  - Global documents
- **Measures** **(see Section "6.5 Measures")**

From an organisational perspective, the elements "(Compliance) attributes", "Documents" and "Measures" are linked to compliance categories. By selecting or deselecting a compliance category in the "Compliance reference" dialogue element, documents and measures in each category are added or removed.

For the hierarchically downstream sub-requirements, the information

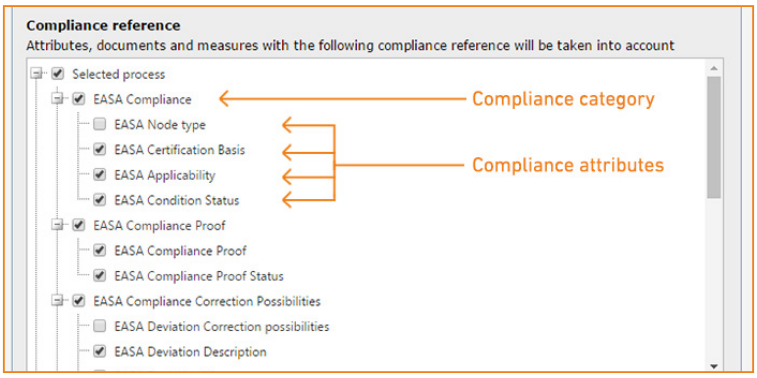
- **(Compliance-) attributes**
- **Documents**

can be integrated into the report. The sub-requirements can also be as deeply structured as desired or are selected for all other levels.

With regard to the downstream sub-requirements, the system does not take into account any documents from objects to which the sub-requirements are linked. If linked documents are important for compliance testing, they must be assigned to the higher-level requirement.

9.4.2 Selection of compliance categories and attributes

Compliance categories and compliance attributes are selected easily from the tree element "Compliance Reference" shown below.



The elements shown depend on the permissions of the logged-on user relating to the requirements and any deviating permissions relating to the hierarchically downstream sub-requirements.

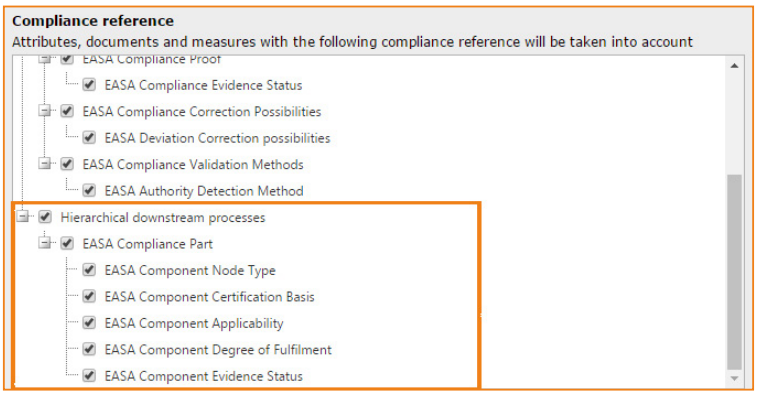
The amount of information or elements available depends on which user generates the compliance sheet.

By selecting or deselecting a compliance category, for example, "EASA Compliance" or "EASA Compliance Correction Options", documents and measures in each category are generally added or removed.

In the above-mentioned example, documents and measures in the category "EASA Compliance Correction Options" are not taken into account, as this compliance category has been deselected.

A compliance category can have different compliance attributes, which can be included attribute by attribute in the report.
In the above-mentioned example for instance, neither the compliance attribute "EASA Node Type", nor the compliance attribute "EASA Deviation Correction Options" and EASA deviation description category "EASA Compliance Correction Options" are shown.

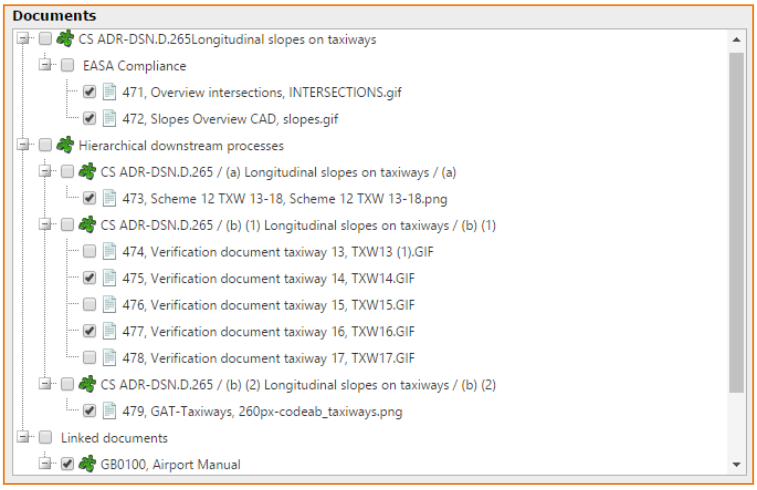
Finally, the tree element "Compliance Reference" contains the hierarchically downstream processes or sub-requirements. According to the above-mentioned logic, compliance categories and compliance attributes can also be selected here, whereby the settings apply as standard for all downstream sub-requirements.



To simplify the parameterisation of the compliance sheet, the only attributes and categories shown are those which have been used at least once or to which at least one document has been assigned.

9.4.3 Selection of documents

The lower section "Documents" is used for the targeted selection of individual documents:



The document area is primarily structured according to:

- **Requirement (or "CS ADR-DSN.D.265 Longitudinal slopes on taxiways")**
- **Hierarchically downstream processes and**
- **Linked documents.**

The documents can be individually selected and deselected. In the example shown above, the documents with the internal document numbers 474, 476 and 478 should not be included in the current compliance sheet.

The documents known as "linked documents" are documents that are assigned to object links of the requirement "CS ADR-DSN.D.265 Longitudinal slopes on taxiways". The example refers to a "Global Document" – the "Airport manual", which is integrated into the compliance sheet together with the main document and other applicable documents.

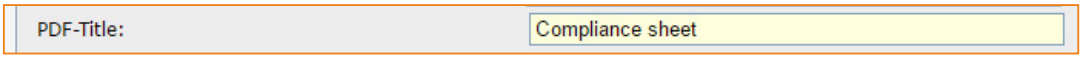
9.4.4 Reproducibility

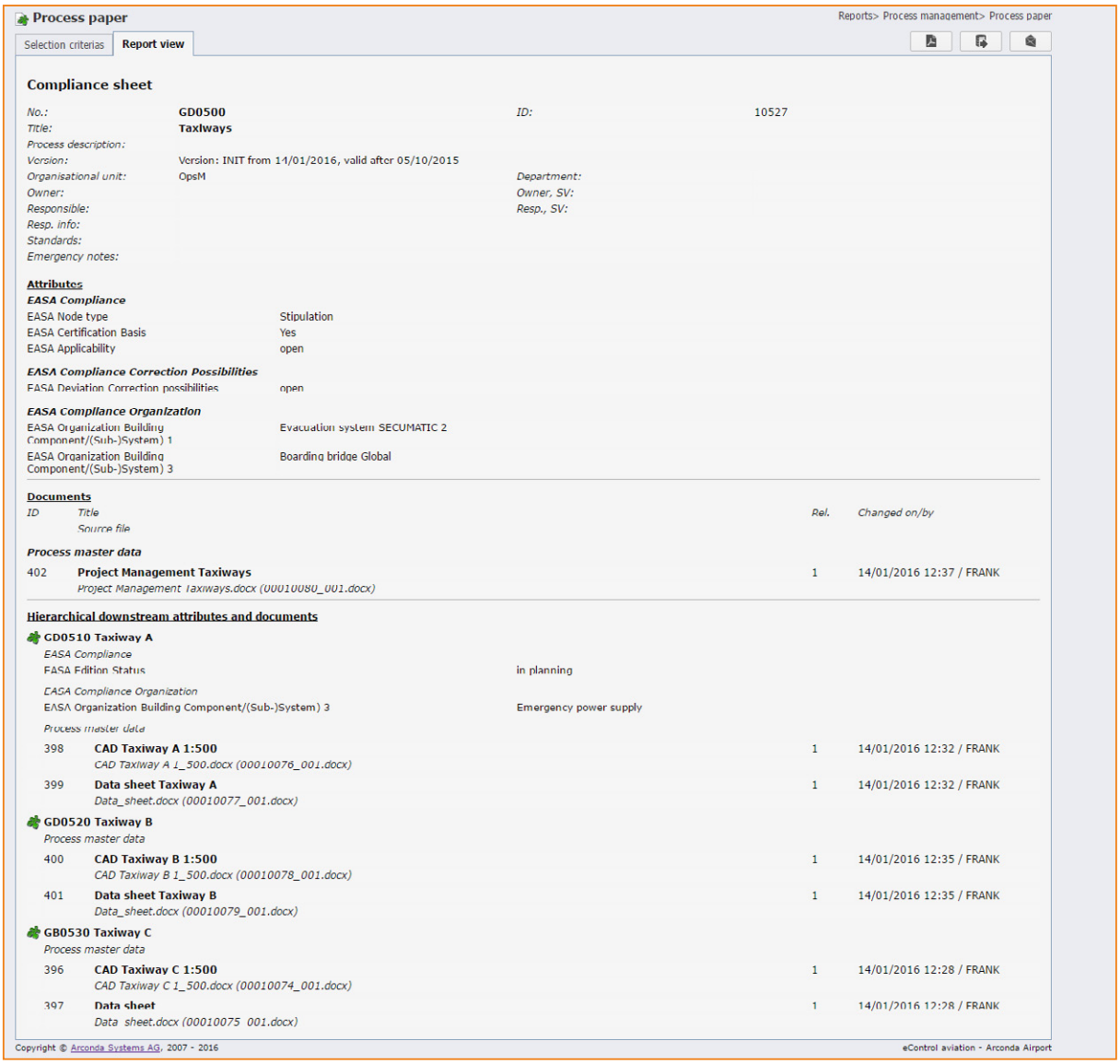
All settings that have been used for the process and compliance sheet can be stored again as query settings in the query pool for future use. A compliance sheet can be compiled in advance by the project office during the processing of requirements and sub-requirements and easily added on completion.

9.4.5 Report design

The currently selected compliance attributes, documents and other report components are displayed in print preview when the following button is pressed:

The print preview can be displayed as a PDF file. An individual report title can be assigned for the PDF file in the input field “PDF title”.





Process paper

Reports> Process management> Process paper

Selection criterias | Report view

Compliance sheet

No.:	**GD0500**	*ID:*	10527
Title:	**Taxiways**		
Process description:			
Version:	Version: INIT from 14/01/2016, valid after 05/10/2015		
Organisational unit:	OpsM	*Department:*	
Owner:		*Owner, SV:*	
Responsible:		*Resp., SV:*	
Resp. info:			
Standards:			
Emergency notes:			

Attributes

EASA Compliance

EASA Node type	Stipulation
EASA Certification Basis	Yes
EASA Applicability	open

EASA Compliance Correction Possibilities

EASA Deviation Correction possibilities	open

EASA Compliance Organization

EASA Organization Building Component/(Sub-)System) 1	Evacuation system SECUMATIC 2
EASA Organization Building Component/(Sub-)System) 3	Boarding bridge Global

Documents

ID	Title / Source file	Rel.	Changed on/by
Process master data			
402	**Project Management Taxiways** *Project Management Taxiways.docx (00010080_001.docx)*	1	14/01/2016 12:37 / FRANK

Hierarchical downstream attributes and documents

GD0510 Taxiway A			
EASA Compliance			
EASA Edition Status	in planning		
EASA Compliance Organization			
EASA Organization Building Component/(Sub-)System) 3	Emergency power supply		
Process master data			
398	**CAD Taxiway A 1:500** *CAD Taxiway A 1_500.docx (00010076_001.docx)*	1	14/01/2016 12:32 / FRANK
399	**Data sheet Taxiway A** *Data_sheet.docx (00010077_001.docx)*	1	14/01/2016 12:32 / FRANK
GD0520 Taxiway B			
Process master data			
400	**CAD Taxiway B 1:500** *CAD Taxiway B 1_500.docx (00010078_001.docx)*	1	14/01/2016 12:35 / FRANK
401	**Data sheet Taxiway B** *Data_sheet.docx (00010079_001.docx)*	1	14/01/2016 12:35 / FRANK
GB0530 Taxiway C			
Process master data			
396	**CAD Taxiway C 1:500** *CAD Taxiway C 1_500.docx (00010074_001.docx)*	1	14/01/2016 12:28 / FRANK
397	**Data sheet** *Data_sheet.docx (00010075_001.docx)*	1	14/01/2016 12:28 / FRANK

Copyright © Arconda Systems AG, 2007 - 2016

eControl aviation - Arconda Airport

9.4.6 Data transfer via ZIP file

The simplified transfer of data to authorities or other external recipients is an important feature of the software module Compliance Management.

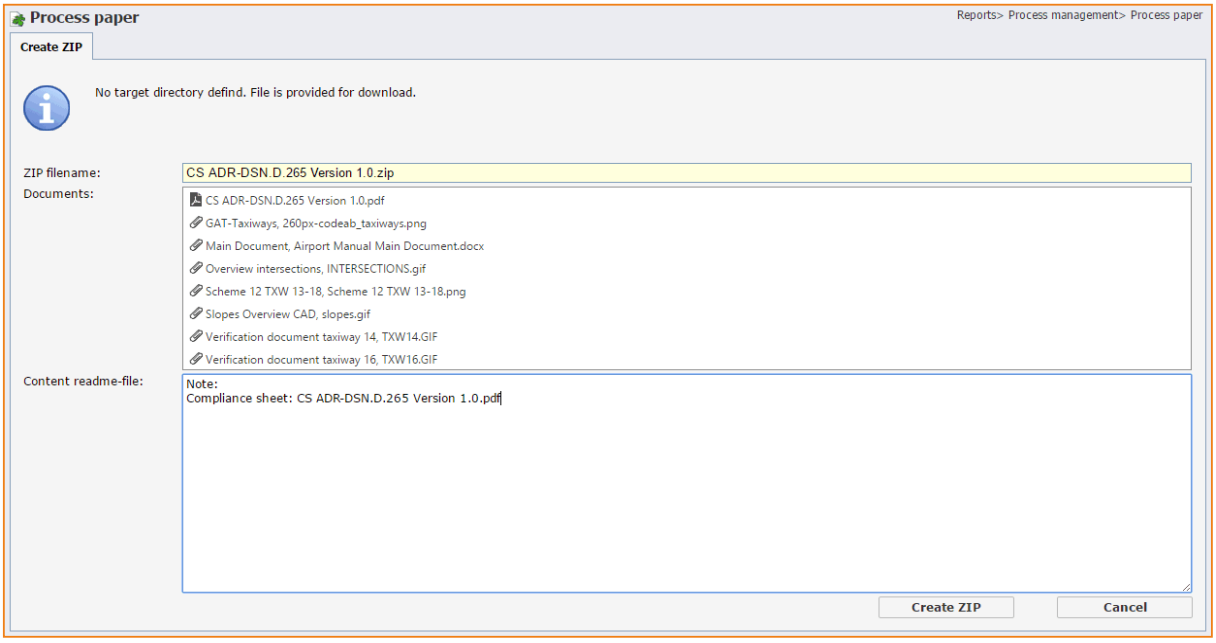
When this data is transferred, a ZIP file is generated, which can consist of the components

- Compliance/process sheet in PDF format
- Documents according to selection dialogue
- README file.

A ZIP file is generated subsequent to the generation of a print preview.

Pressing the button

opens the dialogue shown below:



The data field “ZIP filename” enables the ZIP file name suggested by the system to be changed.

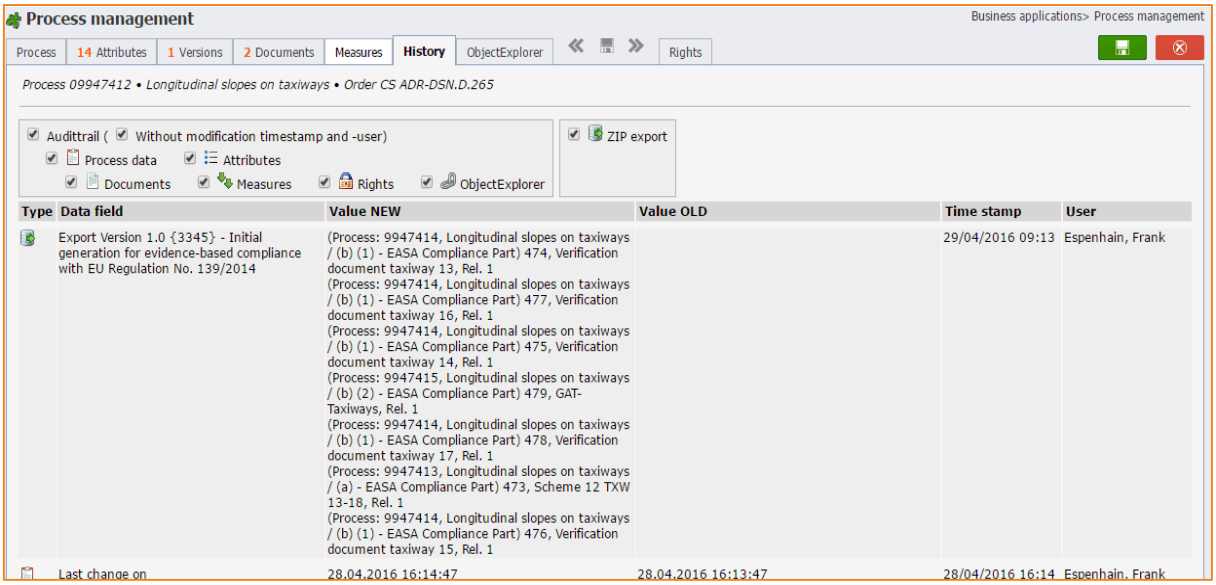
The list box “Documents” contains the documents selected for export. The file CS ADR-DSN.D.265 Version 1.0.PDF contains the compliance sheet itself.

The data field “Content readme-file” is used to capture information about the use of the ZIP file for the recipient. The file is given the name “README.TXT” and is only generated if an explanatory text has actually been captured.

The ZIP file is automatically saved by the server in a directory, provided that the system parameter 9900433 has been set. If the system parameter 9900433 has not been completed, the ZIP file is available in the relevant download directory of the browser.

The ZIP file and the compliance sheet in PDF format are not archived by the system.

In the change history of the requirement, for which the ZIP file has been generated, the content of the export is not documented:



In the data field "Export Version 1.0 {3345} – Initial generation for evidence-based compliance with EU Regulation No. 139/2014", the system documents that the requirement has been exported in the process version "1.0". This version of the requirement operates the unique version key 3345 and the version title "Initial generation for evidence-based compliance with EU Regulation No. 139/2014".

For each document contained in the export, the following information is provided:

(Process: 9947414, Longitudinal slopes on taxiways / (b) (1) - EASA Compliance Part) 474, Verification document taxiway 13, Rel. 1

Process: 9947414
Unique key for the requirement or the hierarchically downstream sub-requirement, which is assigned to the respective document.

Longitudinal slopes on taxiways / (b) (1)
Title of the requirement or the hierarchically downstream sub-requirement, which is assigned to the respective document.

EASA Compliance Part
Compliance category, which is assigned to the document in the requirement or the hierarchically downstream sub-requirement.

474
Unique document key of the document. The document can be accessed directly via the document ID.

Verification document taxiway 13
Document title of the document.

Rel. 1
Release version number of the transferred document. The release version numbers are fully-automatically incremented by the system. The unique document key "1111" and the release version number "Rel. 1" enable the exact identification of the file version that has been included in the report – this is particularly relevant if the supporting documents are supplemented or updated.

The data field “Time stamp” documents that the export in the above-mentioned example was carried out on 26.02.2016 at 11:59. The export was carried out by the user “Sorge, Konstantin”.

It must be noted that the entry in the process history is generated automatically by clicking on the following button:

Create ZIP

If this file is rejected for any reason, the entry in the process history is not removed. Alternatively, any data field – e.g. “Version History Reference” can serve to document this fact.

9.4.7 Non-compliance reports

The non-compliance or deviation reports are special forms of the compliance sheet. Compliance attributes are supplied by the manufacturer for the non-compliance situation ELoS (Equivalent Level of Safety), AltMoC (Alternative Means of Compliance), DAAD (Deviation Acceptance and Actions Document) und SC (Special Condition). These special sheets can be generated by a targeted selection of the relevant compliance category, the designated compliance attributes and the associated documents.

In the example shown below, only the compliance category „EASA Compliance SC“ with the compliance attributes specifically allocated for the special condition was selected.

Only the procedure for the wingman mentioned in the special condition is shown in the „General Process Master Data“. By means of the suspension in the „General Process Master Data“, this document can be viewed by all users without any special permissions.

Selection criterias | **Report scope** | Pool

View option: Compliance sheet

PDF-Title: Special condition report

Show attributes: ☑

Show documents: ☑

Show measures: ☑

Show Object Explorer links: ☐

Show process versions: ☐

Show administrative informations: ☐

Compliance reference

Attributes, documents and measures with the following compliance reference will be taken into account

- ☑ Selected process
  - ☐ EASA Compliance
  - ☐ EASA Compliance Proof
  - ☑ EASA Compliance SC
    - ☑ EASA SC-Nr.
    - ☑ EASA SC Certification Specification
    - ☑ EASA SC Safety Objective
    - ☑ EASA SC Deviation
    - ☑ EASA SC Reason
    - ☑ EASA SC ALoS Evidence
  - ☐ EASA Compliance Validation
  - ☐ EASA Compliance Proof Procedure
  - ☑ Process master data

Documents

- ☐ CS ADR-DSN.D.260Taxiway minimum separation distance
  - ☐ EASA Compliance SC
    - ☑ 463, Taxiway details for SC, taxiway details.gif
  - ☐ Process master data
    - ☑ 464, Taxiway procdure for TXY 34A, 150_5340_1k_consolidated.pdf
- ☐ Hierarchical downstream processes
- ☐ Linked documents
  - ☐ GB0100, Airport Manual
    - ☐ 391, Airport Usage Regulations - Update 2015
    - ☑ 392, Main Document
    - ☐ 393, Organizational Chart

The following print preview is displayed:

Special condition report

Condition: 29/04/2016 10:28
By: Frank Espenhain

No.:	**CS ADR-DSN.D.260**	*ID:*	9947403
Title:	**Taxiway minimum separation distance**		
Process description:			
Version:	Version: 1.0 from 28/09/2015, valid after 01/01/1900		
Organisational unit:	-	*Department:*	
Owner:	-	*Owner, SV:*	
Responsible:	-	*Resp., SV:*	
Resp. info:			
Standards:			
Emergency notes:			

Attributes

EASA Compliance SC

EASA SC-Nr.	SC-Nr - AA -1
EASA SC Certification Specification	CS ADR-DSN.D.260 and CS ADR-DSN.T.915 Siting of equipment and installations on operational areas
EASA SC Safety Objective	The safety objective of minimum taxi separation distances ist to allow safe use of taxiways and aircraft stand taxilanes to prevent possible collision with other aeroplanes operating on adjacent runways or taxiways, or collision with adjacent objectives.
EASA SC Deviation	An existing single storey building (3.7m high and 41.5m north of the Alpha taxiway centreline) infringes Alpha Code E strip between hold points Alpha 2 and Alpha 3 by 2m. Aircraft with wingspan greater than 52m (Code E) can only proceed along this section of taxiway Alpha under the supervision of a wingman as per the documented procedure.
EASA SC Reason	Building cannot be removed
EASA SC ALoS Evidence	Qualitative evidence: Aircraft with wingspan greater than 52m (Code E) can only proceed along this section of taxiway Alpha under the supervision of a wingman as per the documented procedure.

Documents

ID	*Title* / *Source file*	*Rel.*	*Changed on/by*
EASA Compliance SC			
463	**Taxiway details for SC** *taxiway details.gif (00010141_001.gif)*	4	29/04/2016 10:24 / SMS
Process master data			
464	**Taxiway procdure for TXY 34A** *150_5340_1k_consolidated.pdf (00010142_001.pdf)*	1	18/04/2016 16:21 / FRANK
Linked documents			
392	**Main Document** *Airport Manual Main Document.docx (00010071_001.docx)*	1	12/01/2016 15:16 / FRANK

Attributes and documents of subsequent nodes.

CS ADR-DSN.D.260 / (a) Taxiway minimum separation distance / (a)
EASA Compliance Part
EASA Component Applicability — Partially

eControl aviation — *Condition: 29/04/2016 10:29* — **Page 1 / 3**

9.5 Process attribute characteristics

This report contains a list summarising the characteristics of the relevant compliance attribute for the filtered requirements.

The desired classification structure can also be inserted via the "display option" field.

The scope of the filtered requirements and displayed characteristics of the compliance attributes depends on the individual authorisations of the logged-on user.

Process attributes characteristics Reports> Process management> Process attributes characteristics

Selection criterias | **Report view**

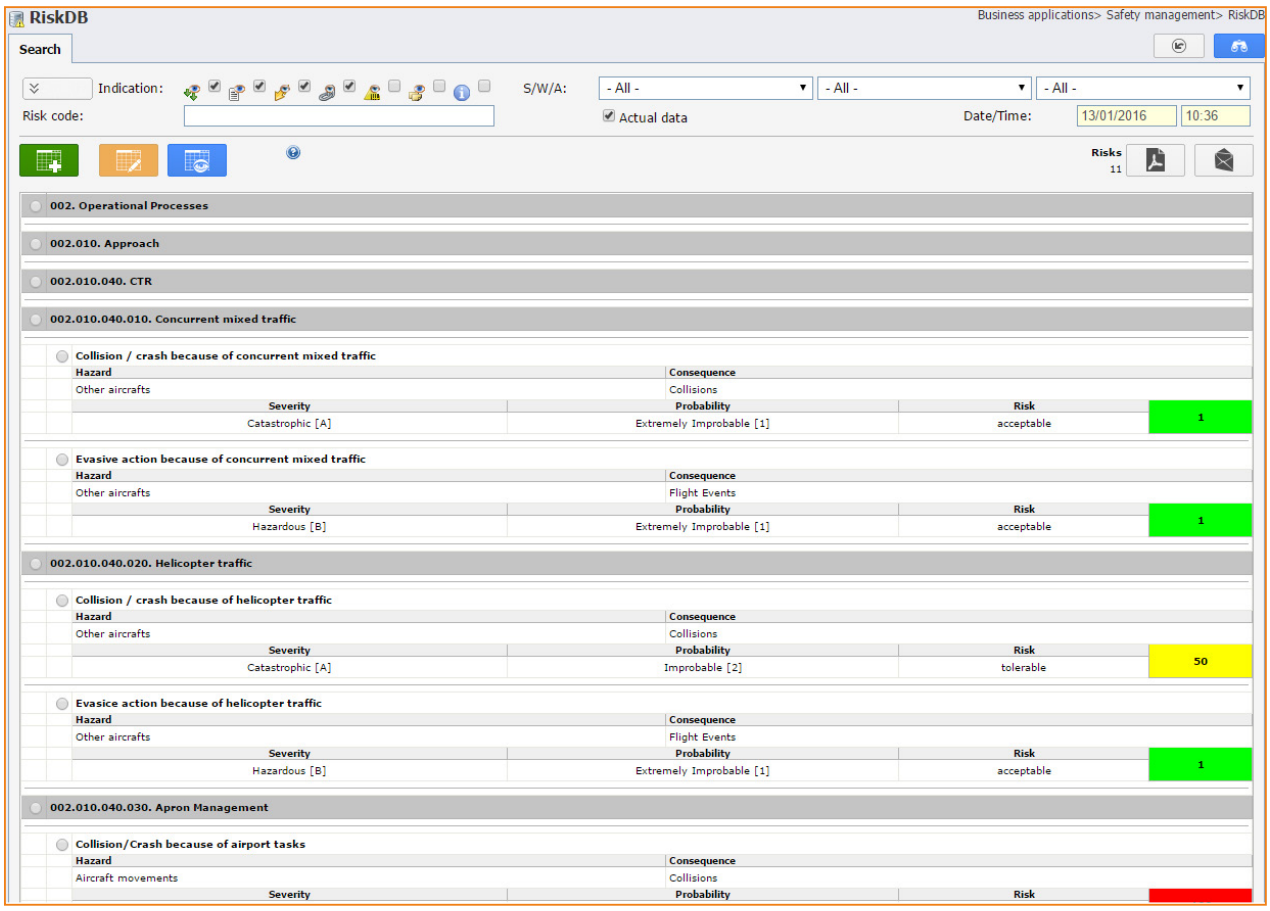
View option: Attribute characteristics grouped by attributes
Creation and edit information: ☐
Show attribute information: ☑
Selection criteria: EASA Node type = Stipulation
AND
{P} Process LIKE taxiway

Compliance short designation	Compliancebezeichnung	
Attribute ID	Attribute Designation	
Attribute Note		
Process ID	Process title	Attribute value
EASA	EASA Compliance	
9902500	EASA Node type	
This process attribute serves to classify EASA nodes in edition and edition componentents in order to facilitate the systematic filtering. All editions shall carry the status „Edition".		
9947391	CS ADR-DSN.D.245 Width of taxiways	Stipulation
9947393	CS ADR-DSN.D.250 Taxiways curves	Stipulation
9947399	CS ADR-DSN.D.255 Junction and intersection of taxiways	Stipulation
9947403	CS ADR-DSN.D.260 Taxiway minimum separation distance	Stipulation
9947412	CS ADR-DSN.D.265 Longitudinal slopes on taxiways	Stipulation
9947417	CS ADR-DSN.D.270 Longitudinal slope changes on taxiways	Stipulation
9947423	CS ADR-DSN.D.275 Sight distance of taxiways	Stipulation
9947429	CS ADR-DSN.D.280 Transverse slopes on taxiways	Stipulation
9947434	CS ADR-DSN.D.285 Strength of taxiways	Stipulation
9947436	CS ADR-DSN.D.290 Surface of taxiways	Stipulation
9947440	CS ADR-DSN.D.295 Rapid exit taxiways	Stipulation
9947450	CS ADR-DSN.D.300 Taxiways on bridges	Stipulation
9947455	CS ADR-DSN.D.305 Taxiway shoulders	Stipulation
9947463	CS ADR-DSN.D.310 Taxiway Strip	Stipulation
9902510	EASA Certification Basis	
This process attribute enables the classification, whether the latest edition is part of the certification basis. The standard value is „YES".		
9947391	CS ADR-DSN.D.245 Width of taxiways	Yes
9947393	CS ADR-DSN.D.250 Taxiways curves	Yes
9947399	CS ADR-DSN.D.255 Junction and intersection of taxiways	Yes
9947403	CS ADR-DSN.D.260 Taxiway minimum separation distance	Yes
9947412	CS ADR-DSN.D.265 Longitudinal slopes on taxiways	Yes
9947417	CS ADR-DSN.D.270 Longitudinal slope changes on taxiways	Yes
9947423	CS ADR-DSN.D.275 Sight distance of taxiways	Yes
9947429	CS ADR-DSN.D.280 Transverse slopes on taxiways	Yes
9947434	CS ADR-DSN.D.285 Strength of taxiways	Yes
9947436	CS ADR-DSN.D.290 Surface of taxiways	Yes
9947440	CS ADR-DSN.D.295 Rapid exit taxiways	Yes
9947450	CS ADR-DSN.D.300 Taxiways on bridges	No
9947455	CS ADR-DSN.D.305 Taxiway shoulders	Yes
9947463	CS ADR-DSN.D.310 Taxiway Strip	Yes
9902520	EASA Applicability	
This process attribute documents, whether the latest edition is applicable within the recent EASA certification. The standard value is „YES".		
9947391	CS ADR-DSN.D.245 Width of taxiways	Yes
9947393	CS ADR-DSN.D.250 Taxiways curves	Yes
9947399	CS ADR-DSN.D.255 Junction and intersection of taxiways	Yes
9947403	CS ADR-DSN.D.260 Taxiway minimum separation distance	Yes
9947412	CS ADR-DSN.D.265 Longitudinal slopes on taxiways	Yes
9947417	CS ADR-DSN.D.270 Longitudinal slope changes on taxiways	Yes
9947423	CS ADR-DSN.D.275 Sight distance of taxiways	Yes
9947429	CS ADR-DSN.D.280 Transverse slopes on taxiways	Yes
9947434	CS ADR-DSN.D.285 Strength of taxiways	Yes
9947436	CS ADR-DSN.D.290 Surface of taxiways	Yes
9947440	CS ADR-DSN.D.295 Rapid exit taxiways	Yes
9947450	CS ADR-DSN.D.300 Taxiways on bridges	Yes
9947455	CS ADR-DSN.D.305 Taxiway shoulders	Yes
9947463	CS ADR-DSN.D.310 Taxiway Strip	Yes
9902530	EASA Edition Status	
This process attributes displays the total edition status for the edition considering all assigned edition components. This process attribute is of central importance for the compliance's valuation and the edit progress. New editions will get the status „original".		
9947391	CS ADR-DSN.D.245 Width of taxiways	Edition components in progress
9947393	CS ADR-DSN.D.250 Taxiways curves	Edition components in progress
9947399	CS ADR-DSN.D.255 Junction and intersection of taxiways	in validation
9947403	CS ADR-DSN.D.260 Taxiway minimum separation distance	in validation
9947412	CS ADR-DSN.D.265 Longitudinal slopes on taxiways	Edition components in progress
9947417	CS ADR-DSN.D.270 Longitudinal slope changes on taxiways	Edition components in progress
9947423	CS ADR-DSN.D.275 Sight distance of taxiways	in validation
9947429	CS ADR-DSN.D.280 Transverse slopes on taxiways	Edition components in progress
9947434	CS ADR-DSN.D.285 Strength of taxiways	original
9947436	CS ADR-DSN.D.290 Surface of taxiways	Non-Compliance Work
9947440	CS ADR-DSN.D.295 Rapid exit taxiways	in validation
9947450	CS ADR-DSN.D.300 Taxiways on bridges	original

10 RiskDB - eControl risk database

The risk database is characterised by the organisational structure and the infrastructure. It follows that the structure of processes, sub-systems and requirements is also the backbone of the risk database RiskDB. In the context of compliance management the risk database is of particular significance, in the event of alternative verification procedures (AltMoC) or deviations (ELoS, DAAD, SC) from the certification provisions.

The risk database provides a systematic documentation of all risks identified in connection with the certification basis.



The eControl risk database "RiskDB" must show not only the risks that are determined in the context of compliance management or certification according to Regulation (EU) No. 139/2014, but also all company-wide risks which have been determined and which have come to light in the course of risk assessments and operational risk management.

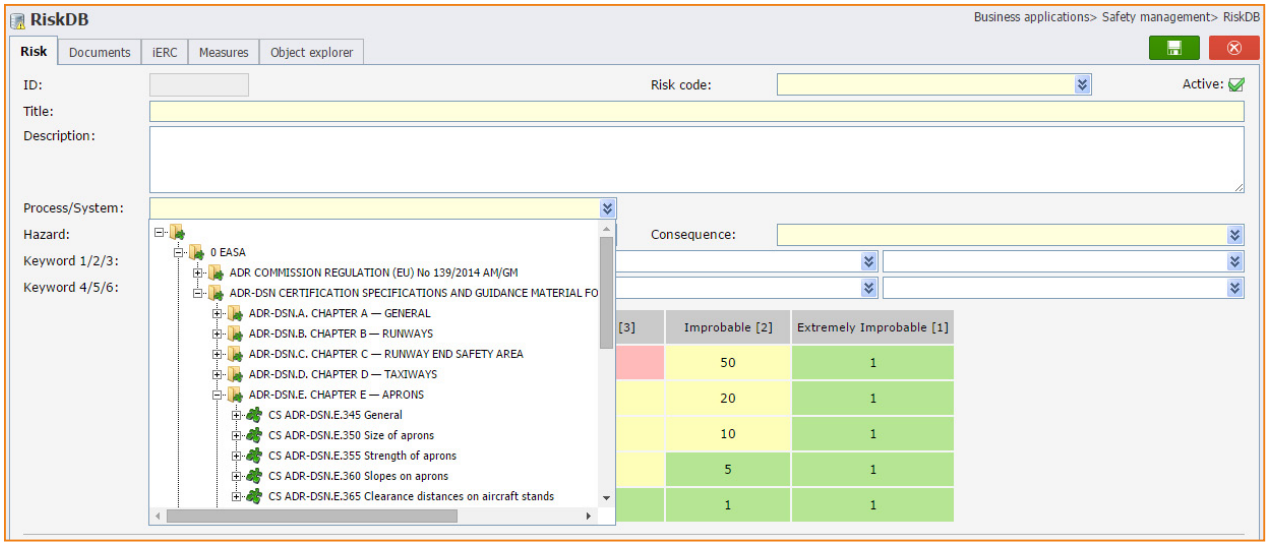
In this way eControl provides a company-wide or corporate risk management. The company-wide approach is a requirement for the control and evaluation of the risk mitigation process (cf. RiskDB risk index trend analysis statistics).

In the dialogue shown below, identified risks are documented and assigned to a requirement.

For each requirement any number of risks can be isolated. At the same time risk assessments that relate to more than one requirement can be properly integrated.

The risks must also be incorporated into a risk matrix. In the example shown below, a risk matrix according to ICAO DOC 9859 is used, but there are a number of other classification options in the system,

which provide for automatic compliance with the future specifications of the competent authority.



This risk assessment, in the form of one or more documents, is stored according to the system standard in the register tab "documents". Risk reduction measures can be documented in the register tab "measures".

If the risks are also linked with the requirement via the object explorer, documents and measures in the risk database can be viewed directly from the requirement and vice-versa.

For read access to the risks in the risk database the user permission "Read risk database" (see Section “7.3.4 User permissions“) is required.

SMS

For further information about risk management with eControl see our product catalogue:
"SMS & Audit - Safety and Audit Management"

11 Audits - long-term maintenance of compliance level

eControl audit management covers

- planning,
- preparation,
- conduct and
- follow-up

of

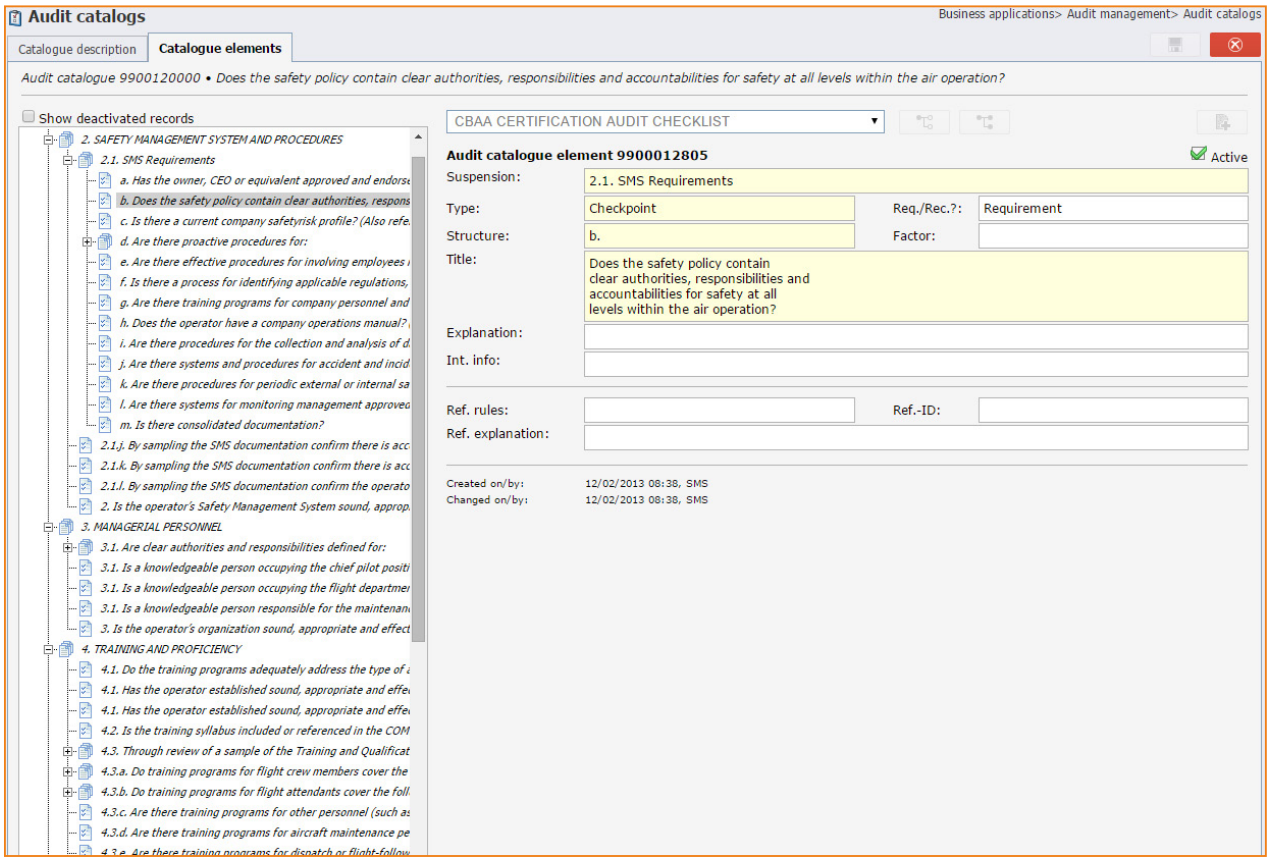
- external audits,
- self-inspections and
- supplier audits,

although compliance audits deal mainly with self-inspections and external audits.

The organisations certified according to Registration (EU) No. 139/2014 must be audited in full after no more than 48 months, which requires the audited organisations and the competent authorities to take a number of different auditing measures. According to the system philosophy of eControl, compliance management initially tests compliance and maintains this situation in the context of change management. Audit management is a tool by means of which this level of compliance is maintained or guaranteed in the long term.

eControl simplifies the conduct of audits through the provision by the manufacturer of audit catalogues for the most important regulations – naturally catalogues for "Regulation (EU) No. 139/2014" and "ICAO Annex 14" are also provided.

Hereinafter is an extract from the audit catalogue for Regulation (EU) No. 139/2014:



The combination of compliance management with the audit results is facilitated by a corresponding classification structure in accordance with the current standard.

eControl provides further support with its own additional catalogue for the conduct of self-inspection and supplier audits. These can include specific details of the relevant organisations or learning effects from findings from past audits.

The catalogues provided by the manufacturer can be used partially or wholly for the pre-setting of audits and amended as required.

For each item in an audit eControl compares the standard (left) and the audit results (right).

Audits

Business applications> Audit management> Audit

Audit | Rights | Attributes | Audit elements | **Audit results** | 2 Documents | 1 Measures | Obj.Exp.

Audit 00000007 • INTERN ISAGO Passenger Handling 01-2013

Audit results | 1/2 Documents | 1/1 Measures

ID: 1424

Type: Checkpoint | Req./Rec.?: Requirement | Factor: 20

Title: 1.2.3. The Provider shall have procedures in accordance with requirements of the customer airline(s) for the check-in of heavy or overweight baggage, and to ensure such baggage is accounted for in the load control process. (GM)

Explanation:

Int. info:

Ref. rules: | Ref.-ID:

Info: Heavy or overweight baggage would have to be defined in accordance with requirements of the customer airline(s). Typically, baggage more than 23 kgs might be considered heavy, while more than 32kgs is considered as exceeding the maximum weight limit (i.e., overweight). However, weight restrictions may vary with each customer airline.

Info:

Category A:

Category B:

Category C:

Category D:

Created on/by: 29/05/2013 09:28, FRANK

Changed on/by: 21/04/2015 11:53, FRANK

Applicable ☑ | Checked ☑ | Accept ☐ | Date: 24/01/2013

Compliance: significantly

Info: No applicative procedure to proactively implement all ongoing changes regarding heavy or overweight baggage.

Deviation degree : low

Info: Old regulations still apply.

Deviation frequency: rarely

Info: Changes are comparatively rare.

Deviation consequence : irrelevant

Info: Mainly commertial. Load balances are correct.

Ext. rating:

Ext. explanation Text:

Ext. info:

Plan verification:

For each item in an audit, documents and measures can be recorded according to the system standard.

For the audit an object explorer link with the relevant requirement can be established, in order to highlight the requirements that have become apparent during auditing. The user interface for documents, measures and object explorer is standardised across the system.

SMS

For further information about risk management with eControl see our product catalogue:
"SMS & Audit - Safety and Audit Management"

12 Change management

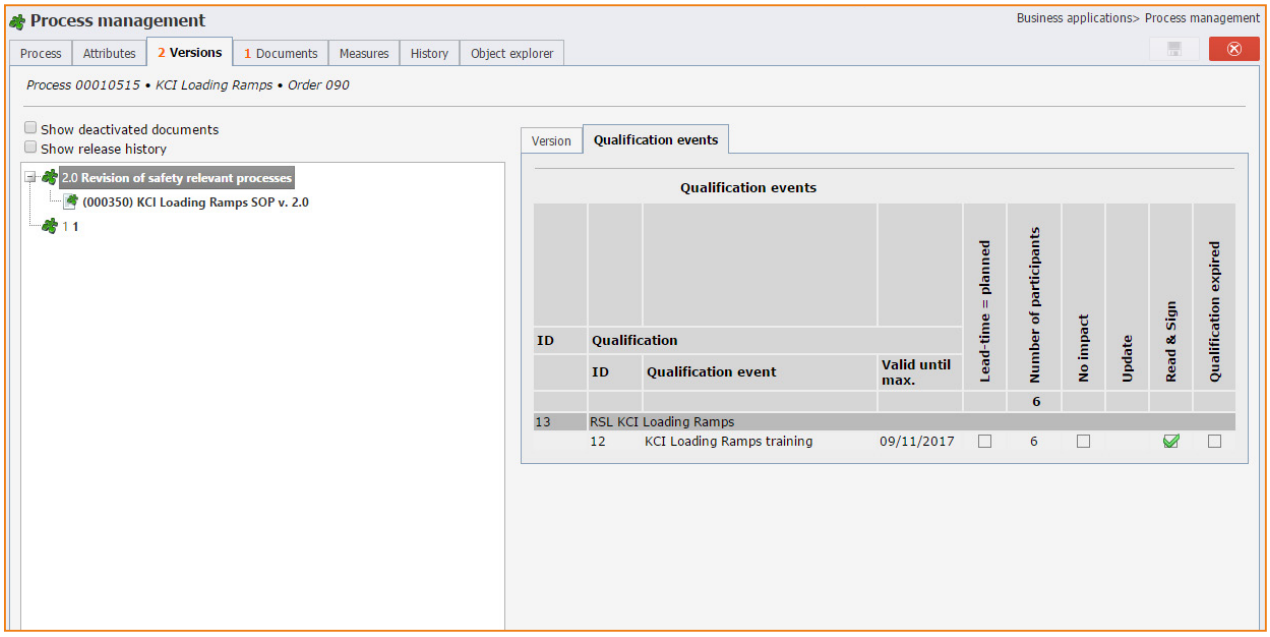
eControl can support the change management of the organisation in several respects. The key steps of the change processes and their support by eControl are shown below.

Rough analysis of the anticipated impacts of change with regard to manuals and process instructions

Manuals and process instructions are already part of compliance management. The use of these documents as global documents (see Section "6.4.6 Global documents") is a particularly valuable indicator for anticipated impacts.

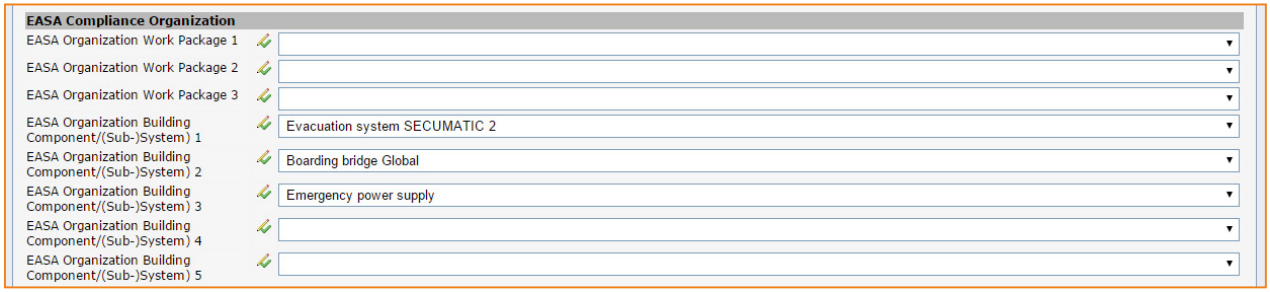
Rough analysis of the anticipated impacts of change with regard to operational and work organisations (personnel deployment, training, etc.)

The eControl TQMS training and qualification management system clearly indicates which employees are and were trained in which process. eControl qualification management enables qualifications and processes to be combined – in this way the change requirement with regard to personnel deployment and training arising from a change can be reliably defined.



Rough analysis of the anticipated impacts of change with regard to infrastructure

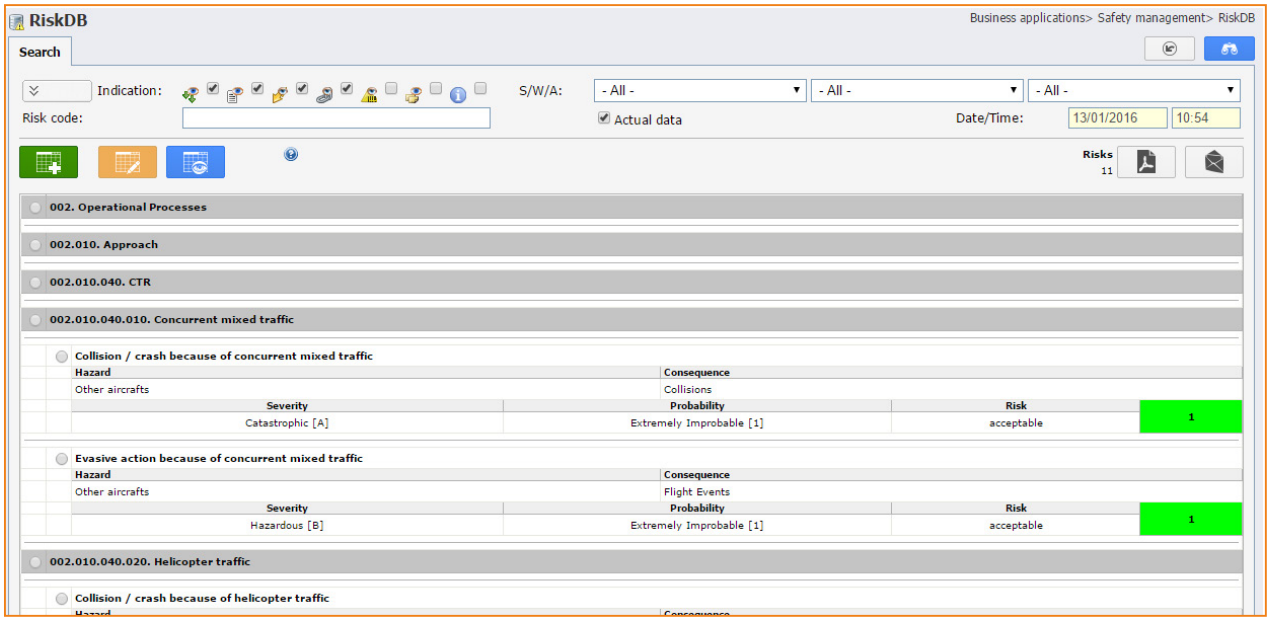
eControl can provide reference points for the impacts of change to the infrastructure, provided that assignments of processes or requirements have been based on infrastructure components. eControl flags up the issue of which requirements have to be verified in the event of a change to an infrastructure component.



The administration of compliance attributes is described on page 46.

Risk analysis / hazard identification and analysis of potential impacts

The eControl risk database or RiskDB (see Section "10. RiskDB - eControl risk database") is designed to flag up risk analyses for various change scenarios. In this way an object structure can be created for change projects, to which risks, documents, risk reduction measures and links with other processes and requirements can be attached in the system. All report and statistics functions of risk management, including the link with operational risks, are subsequently available for these risks.



A bullet point summary of the risk database can be found in Section "10. RiskDB - eControl risk database".

Safety performance monitoring

The change can lead to an alteration in the evaluation and structure of the risks in the risk database. These changes can occur when the change project risks are amended in the risk database or when existing risk assessments are updated.

eControl supports both procedures and updates the RiskDB so that the risk mitigation process can be documented and recorded. eControl has a number of other tools at its disposal for effective safety performance monitoring, not all of which can be described in this manual.

13 Training and qualification management

13.1 Regulatory requirements

The EASA and the ICAO focus increasingly on the significance of an adequate quality management for the required compliance level.

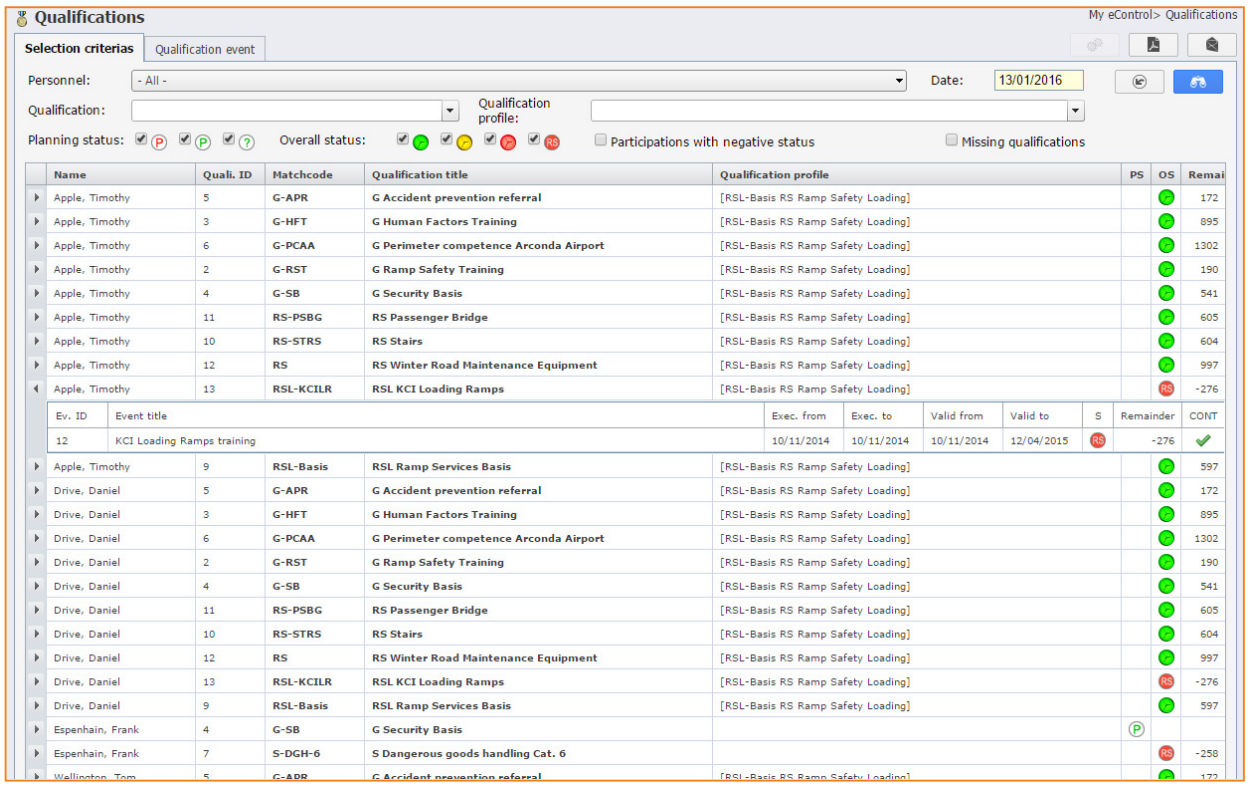
Compliance with regard to compliance management of course also requires transparent recordkeeping. The eControl qualification management offers a number of reports for the complete verification of operational qualifications.

The availability of current document versions and the control of amended documents are further services provided by eControl, which help to maintain and improve the qualification level.

13.2 Qualification status

The qualification cockpit provided by eControl helps the user to see at a glance who requires training and refresher training, where and when, in order to continue to comply with a qualification profile or be suitable for a particular assignment. eControl knows the lead times for the refreshment of qualifications, knows whether qualifications will still be needed in future according to current personnel planning and recognises which qualifications are still lacking in order to achieve the profiles allocated.

This information is available to the HR department, the line manager and of course the logged-on user.



13.3 Linking of processes or requirements with qualifications

With eControl, needs-based processes and requirements are linked with training courses.
In this way the impacts of changes to requirements (see Section "12. Change management") on the training level of the employees can be assessed.

In general the eControl process management systematically documents and structures the processes and requirements. The eControl training and qualification management ensures training and knowledge of all valid process versions and documents.

13.4 Read & Sign

Changes to processes or requirements or to the communicated documents can lead to the content of training courses becoming outdated so that qualifications have to be refreshed. In many cases the process owner comes to the conclusion that the qualifications can be maintained if the previously trained employee has taken note of and understood the changes. eControl Read & Sign provides user-friendly functions for the legally watertight signing of this information.

Before the changes take effect, the qualified employees must be informed about the changes – at the click of a button eControl sends personalised emails or PDF documents to all qualified employees and their line managers. Depending on the circumstances, the qualified employee can confirm with an encrypted email reply that he has taken note of the change. A fully automatic service then ensures in real time that the expired qualification is revived. Alternatively, process sheets and associated process documents can be directly viewed, understood and confirmed by each employee in eControl.

For further information about our TQMS module
see our product catalogue:
"TQMS - Training and Qualifications Management"

14 Competent authorities

The administration processes of the competent authorities and organisations subject to certification are closely linked and have a high degree of similarity in some areas.
The programme functions that are the focus of the competent authority are shown below in bullet point form.

14.1 General requirements

- **Traceability of all data changes**
  (see Section "6.6 History")
- **Transaction-protected and fail-safe storage of data in the data centre of the competent authorities**
- **Administration processes for the administration of any number of airports.**
  (see Section "5. Regulation (EU) No. 139/2014, AMC, CS, und GM and other regulations")
- **Individual, robust access permissions for each airport, user and compliance category**
  (see Section "7.3 Authorisation structure")
- **Flexible workflow control via attributes**
  (see Section "7.3.1 Design")

14.2 ADR.AR.A.010 Regulations

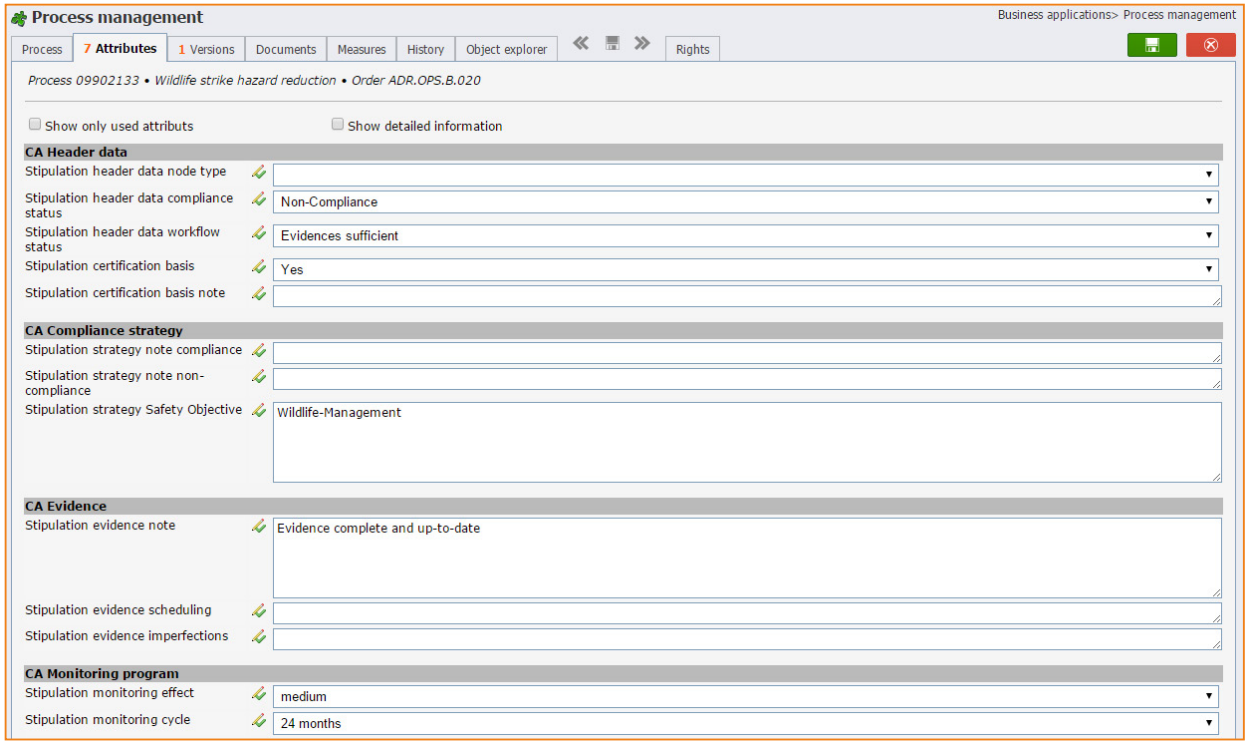
- **Provision of regulations as hierarchical structure**
  (see Section "5. Regulation (EU) No. 139/2014, AMC, CS, und GM and other regulations")
- **All regulations can be adapted as required by the competent authorities**
  (see Section "7.1.1 Flexible hierarchical structure")
- **Document archive with fully automatic version management**
  (see Section "6.4 Documents")

14.3 ADR.AR.B.020 Qualifications

- **Traceable system for the administration of the appointed personnel**
  (see Section "13.2 Qualification status")
- **Graded authorisation system for the personnel management**

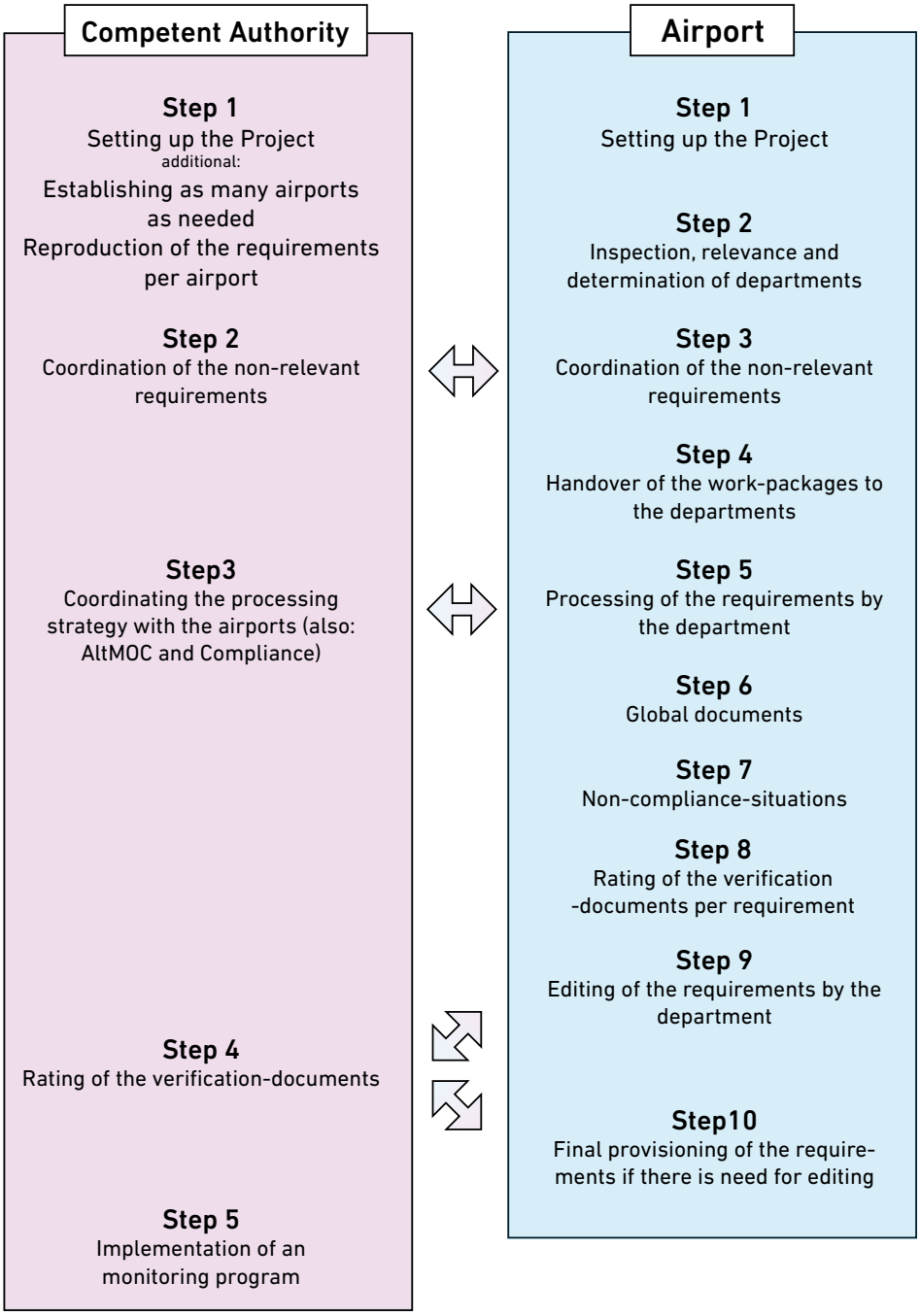
14.4 ADR.AR.B.020 certification - system for the documentation of the certification procedure

- Traceable verification documentation
- Any number of documents for each requirement and organisation
  (see Section "6.4 Documents")
- Freely configurable data fields or compliance attributes for each requirement and organisation – usable as required (see Section "7.3 Authorisation structure")
- Version management for conditions and documents
  (see Section "6.3 Versions")



14.5 Model of operational organisation

The process sequences of the organisation to be certified and the competent authorities are compared below. For the description of the process sequence of the organisation to be certified, refer to the description in Section "4. Airports - step-by-step towards compliance".



14.6 Relevant compliance attributes from the perspective of the competent authorities

The key attributes already prepared by the manufacturer for the competent authority are described below. As detailed in Section "7.2 Compliance categories and compliance attributes", the compliance attributes can be changed or updated and thus adapted to the requirements of the relevant administration processes.

14.6.1 CA Step 1: Header sata

Compliance status / value range
This process attribute stores the compliance status for each requirement and organisation.

Node type / value range
This compliance attribute classifies conditions, AMCs and certification specification, in order to make it easier to filter compliance information.

Workflow status / value range
The workflow status documents the processing progress for each requirement.

14.6.2 CA Step 2: Relevant requirements

Certification basis / value range
By means of this data field it is possible to classify whether the current condition is part of the certification basis.

Certification basis reference / value range
This attribute enables the storage of free-text information about the certification basis.

14.6.3 CA Step 3: Compliance strategy

Compliance reference / text attribute
The strategy that has been coordinated with the monitored organisations in order to achieve regulatory compliance can be stored here (also AltMoC, see Section "14.7 ADR.AR.A.015 AltMoC").

Non-compliance reference / text attribute
This compliance attribute documents the approach that has been coordinated with the monitored organisation for the potential identification of a deviation from the requirement. (see Section "14.8 ADR.AR.B.020 deviations").

Safety objective strategy / text attribute
The communicated safety objective that is targeted by the compliance or non-compliance work of the monitored organisation can be stored here.

14.6.4 CA Step 4: Evaluation of verification documents

Reference / text attribute
This compliance attribute documents the structure of the evidence from the perspective of the competent authority.

Amendment requirement evidence / text attribute
This compliance attribute should indicate the established amendment requirement.

Schedule sequence / text attribute
A schedule sequence with regard to when and what evidence must be or has been provided, can be stored in this field.

14.6.5 CA Step 5 Monitoring programme

Impact / value range
This process attribute classifies the anticipated impact on the safety status of non-compliance with the conditions.

Potential deviations / text attribute
Any anticipated deviations in the context of the monitoring programme can be stored here for the specific purpose of illustrating the controls.

Verification procedure / text attribute
The evidence required in the course of the cyclical monitoring can be documented in this compliance attribute.

Safety objective / text attribute
The safety objective documented in the course of the current requirements can be documented in this compliance attribute.

Monitoring cycle / value range
A monitoring cycle required for the monitoring of the controls is stored in the compliance attributes.

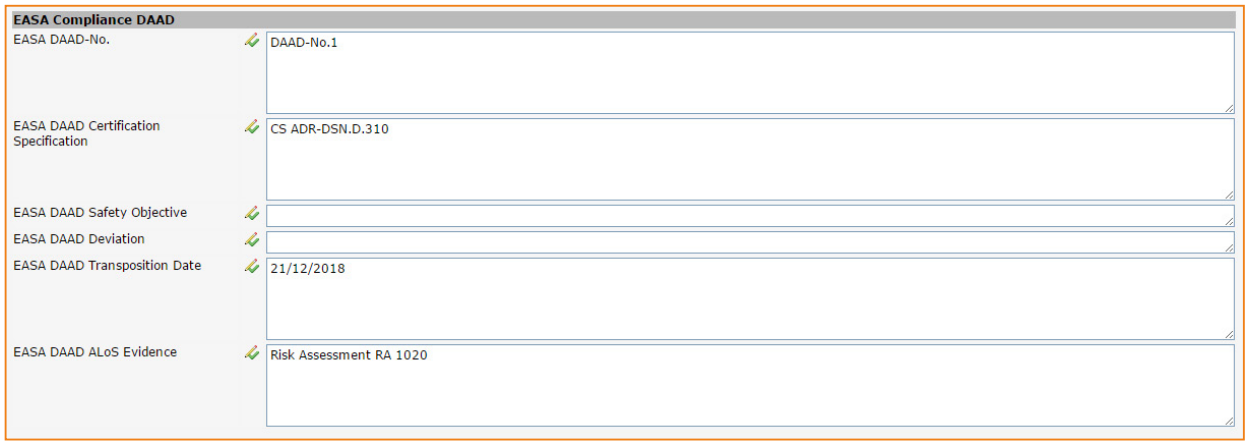
14.7 ADR.AR.A.015 AltMoC

- eControl provides a system for the regular evaluation of alternative verification procedures (AltMoC).
- Individual AltMoCs can be agreed for every condition and every aerodrome.
- Central, cross-organisational AltMoC register.

14.8 ADR.AR.B.020 deviations

- eControl provides various compliance categories for the systematic evaluation and documentation of deviations.
- Deviations are monitored for each condition and aerodrome. According to EASA regulations, compliance attributes are provided for different deviations:
  - ELoS
  - DAAD
  - SC
- Deviation information
  - Data fields for deviation information can be freely designed (see Section "7.2 Compliance categories and compliance attributes").
  - Where required, different write and read access permissions for deviations for each compliance category and monitored organisation. (see Section "7.3 Authorisation structure").
  - Specific assignment of documents to deviations.

Examples of compliance attributes are shown below, with which DAAD-specific information can be recorded.



EASA Compliance DAAD	
EASA DAAD-No.	DAAD-No.1
EASA DAAD Certification Specification	CS ADR-DSN.D.310
EASA DAAD Safety Objective	
EASA DAAD Deviation	
EASA DAAD Transposition Date	21/12/2018
EASA DAAD ALoS Evidence	Risk Assessment RA 1020

Accordingly, compliance attributes are also already provided by the manufacturer for the other deviations:

- AltMoC
- ELoS and
- SC

although all data fields can be freely designed by the customer in accordance with individual requirements.

14.9 ADR.AR.B.010 QM-System

- **Complete documentation of administration processes**
  - Storage of all process descriptions in eControl (see Section "6.4 Documents")
  - Version management (see Section "6.3 Versions")
  - Document control
  - Change, control, release
- **Read & Sign for version changes** **(see Section "13.4 Read & Sign")**
- **Linking of regulations, audits, infringements, safety instructions** **(see Section "6.7 Object explorer")**
- **Measure management** **(see Section "6.5 Measures")**

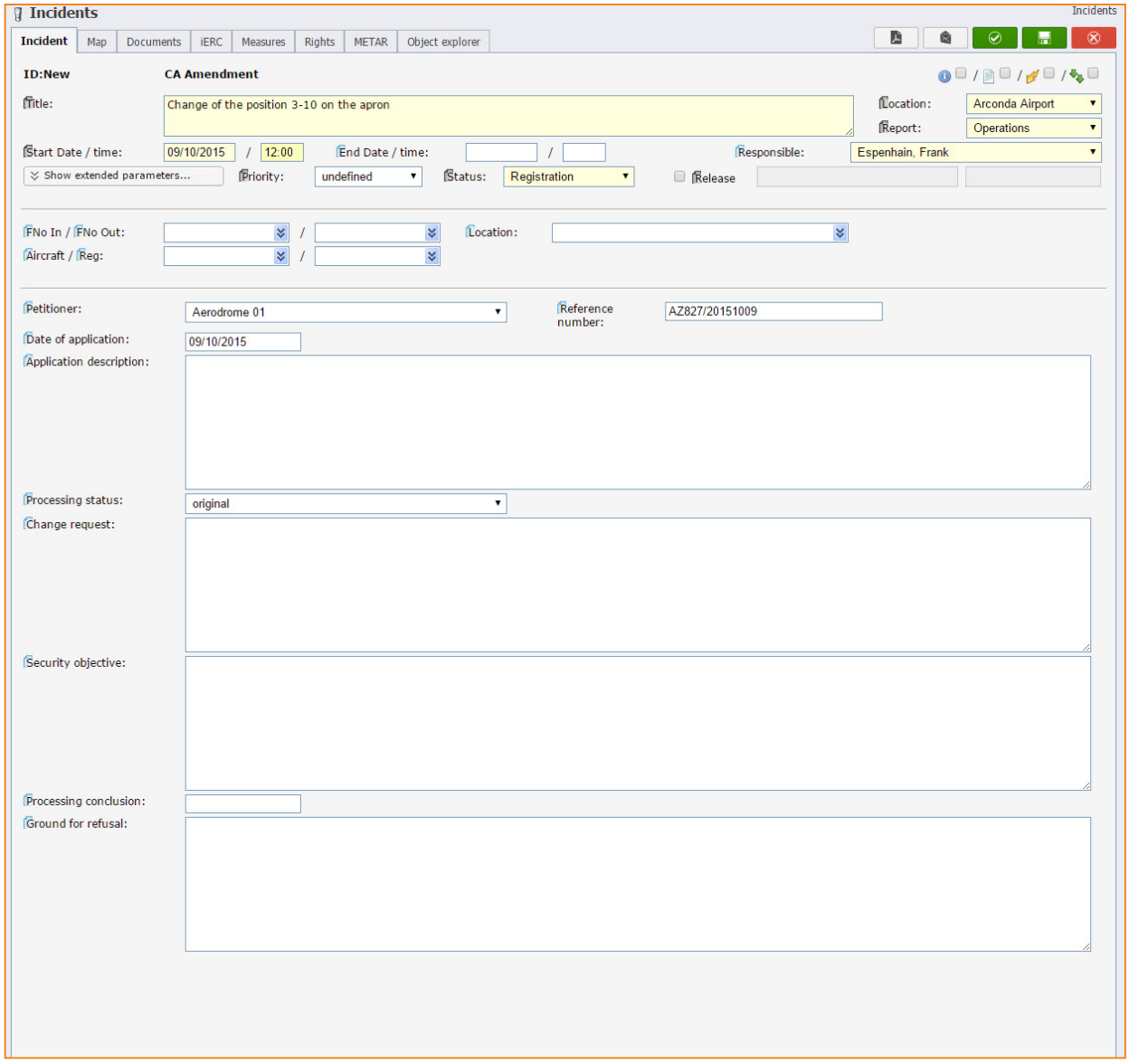
14.10 ADR.AR.B.015 Changes

- **System support of analysis of impact on the management system of changes to the regulations** **(see Section "3.2.5 Change management during the lifetime of the project")**
- **Documentation of the impact analysis conducted in the document archive, in the RiskDB, etc...**

14.11 ADR.AR.C.040 Change requests

- **Provision of a traceable software for the administration of future changes**
- **Change requests**
  - Electronic form
  - Freely definable
  - Status management
  - Differentiated authorisation control
  - Reporting for each airport
- **Document management for each change request**
- **Linking of change requests with the certification basis of the airport**
- **Regulation-based email alerts (in the system)**

An example of the form provided by the manufacturer is shown on next page. It can be amended as required by the customer with the eControl form designer.



The generation and administration of process archives based on electronic forms (eForms) is a basic function of eControl.

For further information about electronic forms (eForms) in eControl see our catalogue:
"eControl - General Product Catalogue"

14.12 ADR.AR.C.005/010 Audits

- **Preparation, planning and documentation of audits/inspections with eControl**
  (see Section "11. Audits - long-term maintenance of compliance level")
- **Traceable documentation of external audits and self-inspections**
- **Audit catalogue available for Regulation (EU) No. 139/2014**
- **Audit plan (including planning, preparation, conduct, documentation, follow-up)**
- **Complete audit catalogues or sections of audit catalogues (hierarchical structure) can be used or merged in the preparation of audits**
- **Storage of any number of documents for each test item and audit**
- **Storage of any number of measures for each test item and audit**
- **Linking for audit items with the certification basis or the requirements of compliance management**
- **Differentiated authorisation control for each audit**
- **Standardised handling**
- **Detailed reporting including statistical functions**

14.13 ADR.AR.A.030 Incidents

- **eControl provides a traceable system for the airfield-related recording, analysis and transfer of safety information**
- **Change requests**
  - Electronic form
  - Differentiated authorisation control
  - Reporting for each aerodrome
- **376/2014 – Taxonomy for the documentation of safety-related parameters [from 11-2015]**
  - ECCAIRS compatibility
  - Approx. 265 combinable parameters
- **Linking of incidents with the certification basis or requirements of the aerodromes**
  - Fully automatic dispatch of rule-based email alerts in the system

14.14 ADR.AR.A.040 Safety instructions

- **Provision of a traceable system for the generation and administration of safety instructions**
  - Electronic form
  - Differentiated authorisation control
  - Linking of safety instructions with certification basis of airports

14.15 ADR.AR.C.045 Infringements

- **Provision of a traceable system for the airfield-related recording, analysis and transfer of safety information**
- **System for the documentation and evaluation of observed infringements**
  - Electronic form
  - Differentiated authorisation control
  - Reporting for each aerodrome
- **376/2014 – Taxonomy for the documentation of safety-relevant parameters [from 11-2015]**
  - ECCAIRS compatibility
  - Approx. 265 combinable parameters
- **Linking of infringements with the certification basis of the aerodromes**
- **Fully automatic dispatch of rule-based e-mail alerts in the system**

eControl

- Process Management
- Operation Management
- Safety Management
- Audit Management
- Qualification Management
- Compliance Management
- Environmental Bird Control Management

Customers:

BADEN-AIRPARK® FLUGHAFEN KARLSRUHE / BADEN-BADEN
Flughafen Stuttgart
FBB FLUGHAFEN BERLIN BRANDENBURG
MÜNSTER OSNABRÜCK INTERNATIONAL AIRPORT
LEIPZIG·HALLE AIRPORT
ALBRECHT DÜRER AIRPORT NÜRNBERG
Beiersdorf
AIRPORT WEEZE
Dortmund Airport 21
hannover airport
Köln Bonn Airport
Schütz & Co
Da sind Sie einfach hin & weg! Allgäu Airport
DAVVL e.V.
Government of Upper Bavaria

Customers international:

Birmingham Airport
Administration de la Navigation Aérienne
Flughafen BERN BELP
PEOPLE's BUSINESSAIRPORT ST.GALLEN-ALTENRHEIN
MALTA INTERNATIONAL AIRPORT

ARCONDA.systems
Aktiengesellschaft

Sportallee 6
22335 Hamburg I Germany

Tel. (+49) 40 823 158 0
E-Mail: info@arconda.ag
Web: econtrol.arconda.ag