EASA

European Union Aviation Safety Agency

Continuing Airworthiness domain

Guidelines on the use of electronic documents, records, and signatures

Issue no.: 1

Date: 4 MAY 2023

Table of contents

1. Introduction and objectives ... 3

2. Definitions ... 4

3. Electronic signatures: general considerations ... 7

4. Scope: situations considered ... 9

4.1. Applications sent to the Authority for approval / acceptance / authorisation ... 9
4.2. Expositions and other documents made available for use within an organisation ... 9
4.3. Certificates electronically signed by individuals acting independently ... 10
4.4. Certificates electronically signed on behalf of an approved organisation ... 10
4.5. Internal flow management tool for approved organisations ... 11
4.6. Interoperability of flows ... 13
4.7. Use of blockchain for tracking life of serialised parts and aircraft ... 13
4.8. Certificates/documents issued by national competent authorities ... 14

5. Implementation of an internal flow management tool ... 15

5.1. Project plan for the change ... 15
5.2. Implementation team ... 15
5.3. Exposition update ... 15
5.4. User functions and rights ... 15
5.5. Training of users ... 15
5.6. IT involvement ... 16
5.7. Internal assessment and monitoring ... 16
5.8. Competent authority role during implementation and continuous oversight ... 16

Revision record

Issue	Date of issue	Summary of changes
1	MAY 2023	First edition.

Contact name and address for enquiries:
Maintenance and Production Department (FS.1)
European Union Aviation Safety Agency
Maint_AB@easa.europa.eu

1. Introduction and objectives

Both European industry and EU Member State competent authorities have requested EASA to prepare guidelines to cover the topic of 'paperless maintenance', aiming to establish some basic standards upon which stakeholders can create their systems under the assumption that these will be recognised as adequate and regulatory-compliant by the competent authorities, at least those participating in the EU-aviation system.

The applicable requirements in Commission Regulation (EU) No 1321/2014[1] are flexible in regards of the format, paper or electronic, to be used for the issue of certificates or other records, or to provide evidence that a process has been followed by the regulated organisations or individuals. Therefore, stakeholders can use electronic means as long as they contain the required information and provide the same guarantees/functionalities as the traditional means (paper), i.e., traceability, integrity, authenticity, possibility of correction of errors and certain degree of prevention of tampering. Regulation (EU) No 910/2014[2] ('eIDAS regulation') obliges for recognition within the EU of the documents electronically signed, when fulfilling certain standards. Therefore, this Regulation and its implementing rules provide a valid reference for these Guidelines when it refers to electronic signatures within the EU. It is also aimed that the electronic signatures issued in compliance with this regulation are given the same recognition by third parties outside the EU.

The use of electronic means (tools, records, certificates, etc.) is permitted by the rules but it is expected that the competent authority accepts its use before a stakeholder transitions from a paper based to electronic based system. When referring to approved organisations, the organisation's Exposition referred in the Regulation (EU) No 1321/2014 should describe the use of electronic tools, electronic forms and electronic signatures, functions of key personnel including those responsible for the electronic means, initial and recurrent related training for its users, dedicated internal audits, etc.

These guidelines intend to address the functionalities and guarantees that electronic processes should satisfy. It does not intend to provide means to approve the hardware and software means used in support of the electronic processes, but it describes sample checks for the assessment of the new electronic means, that interested parties and competent airworthiness authorities should conduct to verify compliance with the applicable continuing airworthiness requirements. For a smooth transition to the use of electronic means, any concerned stakeholder should contact its competent authority before transitioning to share a common understanding of the implementation process and expectations.

[1] Commission Regulation (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks. Also referred in these Guidelines as Regulation (EU) No 1321/2014.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

2. Definitions

eIDAS – Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

eIDAS definitions:

electronic identification – means the process of using person identification data in electronic form uniquely representing a person.

Note: In the context of electronic relationship, electronic identification is an electronic means for a person (or organisation) to prove that they are who they say they are and therefore gain access to information or services available online. This is achieved by using identification data in electronic format which uniquely represent this person (or organisation). Before the electronic identification can take place, it is required that the identification data is issued to the person (or organisation) by a recognised body.

electronic identification means - means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service.

person identification data – means a set of data enabling the identity of a person to be established.

authentication – means an electronic process that enables the electronic identification of a person, or the origin and integrity of data in electronic form to be confirmed.

electronic signature – means data in electronic form which is attached to or logically associated with other data in electronic form which is used by the signatory to sign.

electronic signature creation data - means unique data which is used by the signatory to create an electronic signature.

advanced electronic signature (AES) – means an electronic signature that:

- it is uniquely linked to the signatory;

- it is capable of identifying the signatory;

- it is created using *electronic signature creation data* that the signatory can, with a high level of confidence, use under his sole control; and

- it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

qualified electronic signature (QES) – means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

electronic signature creation device - means configured software or hardware used to create an electronic signature.

Note: 'Qualified electronic signature creation devices' are certified by an authority body, require higher recognition of the service provider that generates or manage the creation data and higher guarantees about the confidentiality of the creation data.

certificate for electronic signature - means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.

Note: A 'qualified certificate for electronic signature' contains validity period of the certificate, the Member State of establishment and identification of the service provider that issues the certificate, and information of the location of the services that can be used to enquire about the validity of the certificate.

validation – means the process of verifying and confirming that an electronic signature or a seal is valid.

electronic seal - means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

electronic time stamp - means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

Note: Competent authorities willing to support their aviation industry may decide to become trust service providers for the purpose of verification of identity prior to the issuance of electronic identification tools (a.k.a. registration authority), creation of certificates and/or validation. This competent authority providing these trust services, not necessarily being considered a qualified trust service provider, would provide stronger recognition of AES from its stakeholders.

Other definitions/explanations:

Signing electronically a record/certificate/any electronic data: it is the process by which a person, representing themself (or an organisation), electronically signs (i.e. logically associates *electronic data that can be later used to validate the identity of signatory) to* the electronic record being signed by means of a software (and sometimes also a hardware) tool(s) (i.e. a creation device) and using their electronic ID (creation data).

Different electronic processes exist that fulfil the intention of electronic signature. Depending on the relevance and consequences of potential misuse, various processes should be considered. In alignment with eIDAS there are three levels of electronic signature: 'basic', 'advanced' (AES) and 'qualified' (QES). The stronger methods use cryptography to provide authentication, integrity and non-repudiation, and higher standards to control and oversight the process/actors involved in the activity.

Integrity: the record was not altered since it was signed. Advanced and Qualified electronic signatures, for their corresponding assurance levels, ensure the integrity of the signed document or record, as any subsequent change in its content would invalidate the signature, being such fact automatically made evident.

Non-repudiation: the person that signed the document cannot deny having signed that record, due to the authentication and integrity properties.

Electronic seal: An electronic seal is associated to a legal entity (business or organisation). An electronic seal can serve as evidence that an electronic document was issued by a legal person ensuring certainty of the document's origin and integrity. Only the person(s) legally entitled to sign/decide/act on behalf of the entity would be in possession of the means required for using the electronic seal. eIDAS defines, similarly to signatures, advance electronic seals (AESe) and qualified electronic seals (QESe).

Document verification by signature validation – Validation that any third party can independently trigger to assess authentication and integrity of electronically signed documents.

PKI (Public Key infrastructure) – Procedures, software and hardware that allows the registration and issuance of certificates that registered persons can use to sign electronically. It provides compliance with some of the higher electronic signature levels considered in eIDAS by means of asymmetric cryptography using private and public key concept.

Blockchain –A decentralised and distributed digital ledger consisting of records called blocks that are used to record actions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively.

3. Electronic signatures: general considerations

A signature is used for validating the contents of a document or attesting an action by a person. Depending on the needs, more simple or more complex means can be used and provide different levels of assurance and integrity.

Assurance levels characterize the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level of a signature must match the criticality of the document and reflect the needs of the receiving party or of a yet-unknown third party to validate the authenticity of the signatory without being over-burdensome on administration.

In the aviation environment, it is not always necessary to use the highest assurance levels. The principle is that a simple attestation of a process within an organisation (e.g. sign-off of a task card or conducting an incoming inspection of a spare part received at a Part-145 organisation or any internal processes in a CAMO) does not need to provide assurance to third parties and it is unlikely that a person not related to the organisation would need access to this information or would try to breach this internal process, since it would not provide any advantage (see point 4.2).

On the contrary, some certificates, including those issued by the competent authority, are given high relevance by third parties. Therefore, for these later cases stronger methods for signature, as AES or QES in eIDAS, should be considered (see points 4.3, 4.4 and 4.8).

Also, thanks to the fact that most aviation actors are already recognised by means of approvals or certificates granted to organisations or individuals in accordance with the European civil aviation rules, the required means for electronic identification in the relations between two approved organisations could be established differently if agreed by both parties (see point 4.4). However, in this case it should be considered whether these means would also be considered adequate by other stakeholders that could be affected at a later stage (e.g., aircraft lessor or aircraft potential new owner).

A requirement to sign electronically a document is that the person signing has a digital identity with certain credentials. This is achieved in a process that includes a check that the physical person to whom the credentials are assigned is the actual person. This happens when a person receives a username and password in an organisation. This could be sufficient for certain internal purposes in such organisation and may be compliant with the most basic understanding of an electronic signature in accordance with eIDAS regulation when the record generated by this process appends the electronic data indicative of the signatory to the record being signed.

For additional guarantees, described in the eIDAS regulation as AES or QES, different solutions, typically based on PKI, are needed. PKI is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in an electronic communication and/or signing a record as well as its integrity.

For electronically signing under a process based on PKI, the first step is that a user (potential signatory) obtains a certificate for electronic signature once that the physical identity of the user is verified. The certificate contains the user's name, etc., in addition to the public key that pairs with a private key that the user also gets in the same accreditation process and should never share.

When this user wants to sign a document, the user’s private key is used in an automatic process to encrypt the document being signed and appends the result of this encryption (signature) and the user’s electronic certificate to the document being signed.

Thanks to the public key contained in the certificate for electronic signature attached to the signed document, it is possible for a third party to automatically check that the certificate is genuine, decrypt the signature appended to the document and automatically verify that the decrypted record matches the original record, therefore guaranteeing that this precise document was signed by the owner of the certificate (signatory).

This process requires stronger guarantees for QES than for AES.

4. Scope: situations considered

4.1. Applications sent to the Authority for approval / acceptance / authorisation

In general, applications to the authority for an approval should be made in the form and manner established by the competent authority. These guidelines propose that competent authorities accept any application (or request for approval) referred to in Regulation (EU) No 1321/2014 which is electronically signed in compliance with eIDAS QES or AES or correspondent seals. Each competent authority can accept other forms of electronic applications.

The same approach is recommended for all documents that, in accordance with Regulation (EU) No 1321/2014, are submitted seeking an authority approval, e.g., a maintenance programme for which authority approval is sought.

4.2. Expositions and other documents made available for use within an organisation

4.2.1. The organisation Exposition must contain a statement signed by the accountable manager in accordance with the applicable regulation (e.g., 145.A.70(a)(1)). If the statement is signed electronically, it should be done i.a.w. eIDAS AES or QES.

4.2.2. The approval by the authority of the Exposition may be done by means of signing electronically a letter referring to the Exposition or by electronically signing the Exposition itself. Refer to 4.8 for the authority electronic signature.

4.2.3. Future amendments of the Exposition should follow the same approval principles (except in the case of indirect approval, e.g., 145.A.70 (c), that does not require authority approval). When the indirect approval would be permitted, the version of the Exposition approved by the authority should also contain the description of the electronic approval process for cases of indirect approval.

4.2.4. The current Exposition should contain a log with the list of revisions/issues.

4.2.5. The Exposition electronically signed corresponding to the version approved by the authority, and any later signed version of it, can be submitted (e.g., using email) with any person or organisation that needs to know/use it (*); and/or, be made accessible on the internal IT network (intranet) of the organisation (**).

4.2.6. (*) The notification of this submission should inform the recipients that they will receive any future update by electronic means insofar they are not notified of being removed from the distribution list. The organisation should keep record of the list of recipients and notify them whenever they are excluded from the distribution list.

4.2.7. (**) The authority may accept the use of an internal IT publishing system (e.g., intranet) containing the approved Exposition, as a single read-only file or by means of different files containing individual chapters of the Exposition. In this later case, the publication process (upload of the document) should provide the same documental management guarantees, i.e., approval, revision number, applicability dates and the uploading process, which should be also described in the Exposition. The organisation should be able to provide evidence of the publishing time for each published content.

4.2.8. In both cases, (*) and (**), the organisation should be capable to retrieve all Exposition signed versions containing the competent authority approval (when applicable) and evidence of the timely submission to affected parties (if applicable) or the dates of upload of the publication.

4.2.9. Alternatively, to the use of electronic signatures, an Exposition with wet signatures (accountable manager statement and/or authority approval) can be also scanned and scanned copies be distributed by email or published in the company network as described in 4.2.5. to 4.2.8, if permitted in the organisation Exposition. In this case, the records to be kept for traceability and verification of compliance purposes would be the wet-signed versions of the documents (i.e., paper originals).

4.3. Certificates electronically signed by individuals acting independently

Where Regulation (EU) No 1321/2014 permits the issue of certificates by individuals, they should be entitled to use the electronic signatures. This is possible, for instance for Certificates of release to service (CRS) and Airworthiness Review Certificates (ARC) issued by Part-66 independent certifying staff/airworthiness review staff. The same applies for other records that would normally be signed, e.g., declaration of a maintenance programme by an aircraft owner.

Any individual person entitled by Regulation (EU) No 1321/2014 to issue a certificate may sign it electronically in compliance with eIDAS QES. This electronically signed certificate has the same legal value as one signed by traditional means and should not be rejected by any actor in the EU aviation system. The electronically signed certificate should permit its validation in accordance with eIDAS. The certificate signed should explicitly contain both the reference of the approval under which the certificate is issued (e.g., Part-66 licence number) and name of the signatory, unless this information is contained in the electronic certificate attached to the signed document.

Individuals signing electronically should retain for the periods established by the applicable regulations, the records of all the documents signed for which they have referred their approval number and show them to the authority upon request.

Printed copies of the electronically signed document which contain a reference for online verification of the certificate can be considered acceptable for compliance with record keeping requirements, as long as the online verification is possible by any party.

4.4. Certificates electronically signed on behalf of an approved organisation

Examples of signed documents covered by this point are, for instance, an aircraft maintenance programme or an ARC issued by a CAMO or a CRS issued by a Part-145 organisation.

Any organisation entitled by Regulation (EU) No 1321/2014 to issue a certificate may sign it electronically in compliance with eIDAS AES or AEseal, or a higher standard. The organisation should only provide means to issue electronic seals to personnel authorised to issue the certificates on behalf of the organisation as per Regulation (EU) No 1321/2014 and its Exposition; when using AES, the declaration statement on the certificate should state that the individual person is signing on behalf of the organisation. This electronically signed/sealed certificate is as valid as a certificate signed/stamped by traditional means, and it should not be rejected by any actor in the EU aviation system. The electronically signed certificate should be recognised when presented either in electronic format or in paper format (print-out), if it permits, in accordance with eIDAS, an online verification by any third party of validity of the signature, the personal data of the signatory and integrity of the document signed.

Also, electronic seals produced by the approved organisation should be recognised as certificates issued under Regulation (EU) No 1321/2014, if the system used allows, in accordance with eIDAS, an online verification that the seal data contains name and approval number of the organisation and of the integrity of the document signed. The Exposition of the organisation should have a list with the name of all staff having permission to sign on behalf of the organisation (or to use the seal on behalf of the organisation), how those rights are revoked (when needed), and keep record of all documents signed (or sealed) on behalf of the organisation, as required by the retention periods established in the applicable regulations. Whenever seals are used, the organisation should be able to trace the person that issued the seal.

4.5. Internal flow management tool for approved organisations

4.5.1. General

Point 4.5 addresses tools for handling activities within an approved organisation on which Regulation (EU) No 1321/2014 and the associated AMCs expect that some attestation is made as evidence of completion of different steps of a process, for instance the different sign-offs aiming to support the release to service in a base maintenance scenario. In this scenario, an approved organisation (e.g., CAMO, AMO) uses a commercial-off-the-shelf software or a software developed/tailored to their needs.

This point does not cover the signature of any certificate issued by an approved organisation to a third party (refer to § 4.4 for this case), that could, for instance, attest the proper completion of all the steps of the internal process described in § 4.5. Nevertheless, both processes may be integrated within a single software/hardware solution, if the final certificate also fulfils the requirements of § 4.4.

Major functionalities of the tool (managing the flow of the processes, providing access to relevant information to identified staff, electronically attesting each step of the process, and generating electronic records) should be described in the organisation’s Exposition to the level required to demonstrate compliance with the applicable continuing airworthiness requirements and to these guidelines.

The management and release of new software versions and updates should be explained in the Exposition, but this does not need to be considered as a change requiring prior authority approval if the main functionalities (managing the flow of the processes, providing access to relevant information by different staff, attesting completion of different steps and generating electronic records) are not affected.

The company developing the software should not be considered as a subcontractor and does not need to be audited by the compliance monitoring function of the approved organisation required in Part-145, Part-CAMO or Part-CAO. However, the organisation should be able to demonstrate to its authority that the key features identified in this guideline for the tool are met.

4.5.2. User identification and attestation by signature

For the purpose of person identification to access to information provided by an internal-only tool and/or to provide attestation of steps completion, it is sufficient that user identification is achieved by means of a combination of username and password. To prevent possible misuse, usernames and passwords should be provided to users in a way that is securely controlled by the organisation.

At every log in in the tool, the user should be provided with information on the last time that (s)he logged in. The user should report internally any anomalous access detected.

When the use of the tool relies on means not directly controlled by the organisation (e.g., hardware hosted by a third party, open internet connections) the organisation should consider stronger identification assurances such as one-time password or double factor authentication.

4.5.3. Records

Each step of the flow which is attested by electronically signing should generate a record that is identified with a unique code automatically assigned.

This record should provide a detailed description of the conditions at the time of the signature: referenced documentation, completed steps of the flow, step attestation, time of attestation, attestation person.

The tool should allow each user to access at any time any record that attests a step performed by the user.

Records should be printable on paper or visible with a software tool that can show non-editable read-only files. These records will have time information of when the step was attested and when the record was generated. Printed versions should contain a statement about potentially not being current. They may include a web address to verify electronically their validity.

Records may be sent outside the organisation. Organisations should be aware that records signed using a basic electronic signature cannot be authenticated by third parties.

4.5.4. Corrections

The system should allow corrections for cases where unintended incorrect inputs on the steps of the internal flow (see § 4.5.2) were already attested with a signature.

Corrections will require a new signature by a person authorised to attest such. The correction should not prevent the possibility to read the original (uncorrected) entry if needed.

For sequential flows, a correction will temporarily invalidate any step that sequentially followed the original incorrect input. This would be indicated in all records related to those steps as from when the first step was corrected (or declared incorrect), as longs as the new steps are not sequentially reconfirmed. It is required to reconfirm any later steps of the flow with new signatures by suitable personnel to re-validate the complete flow.

4.5.5. Connectivity with using wireless terminals (e.g., tablets)

If the tool relies on real-time communications between different terminals allowing that the same data is presented in each terminal, these should clearly indicate situations when the connectivity is lost or prevents data sharing.

When signing at a terminal, the tool should provide feedback to the signatory when the step attested with the signature has been processed by the tool/system.

The process to be followed in cases of lost connectivity should be described in the Exposition and be part of the training of the concerned personnel.

4.5.6. Back-ups

Any data loss should be prevented in consideration of any foreseeable reasonable occurrence. Such prevention could be considered as achieved by establishing a robust and frequent back-up (or twin) system that would allow recovery of all information, flows and records of the system. Policy for backs-up should be described in the Exposition.

4.6. Interoperability of flows

Sometimes the flow of a process involves more than an approved organisation. It is important to assess these cases from the perspective of the roles and responsibilities of the concerned approved organisation that seeks recognition of the tool. For instance, if an e-TechLog is used for the certification of maintenance carried out on an aircraft, the tool should only permit that the signature is provided by the authorised certifying staff of the 145-organisation.

For cases when the tool of an organisation for the management of a signature flow is not deployed for use by a second involved organisation (for instance an operator using an e-TechLog that does not permit the signature of an approved maintenance organisation that conducted maintenance at an occasional line station or at an unforeseen location due to aircraft unserviceability), it is possible that the first organisation electronically signs on the flow tool (e-TechLog) attesting that the step (e.g. maintenance release) has been completed by the second organisation, when the first organisation is in possession of a record duly signed (on paper or electronically) by the second organisation that adequately reflects the step performed, and the reference number of such record is captured in the flow tool. The process for the signature of the record by the second organisation should be described in the Exposition.

4.7. Use of blockchain for tracking life of serialised parts and aircraft

A Blockchain platform[3] customised for aviation and available only to the required actors would have the potential of providing reliable information of the historical records associated to the

[3] If such platform would be of interest to the aviation industry and jointly decide to create it, EASA, when invited, would participate as observer on its development to provide its point of

life of a serialised component or aircraft, therefore adding value to this asset, i.e., component or aircraft.

4.8. Certificates/documents issued by national competent authorities

Electronic signatures/seals of certificates (e.g., CoA, ARC, Part-66 licenses, organisation approvals) and electronically approved documents (e.g., Expositions, AMPs, Exemptions) should be, as a minimum, in compliance with AES / AESe.

QES / QESe have the equivalent legal effect of a handwritten signature and benefit from automatic mutual recognition within the EU; their international acceptance is also expected to be higher.

Printed copies of the signed documents/certificates should contain a reference for online verification of the certificate by any third party and its appearance should be similar to the forms contained in the rule.

Online access to the certificates should permit to verify their status (e.g., current, suspended, revoked) by any party.

view as European authority responsible for the continuing airworthiness standards and would update, if needed, such standards to adapt them to this new tool in the spirit of the regulations. Currently EASA participates on a research project to understand the potential of such developments.

5. Implementation of an internal flow management tool

5.1. Project plan for the change

The competent authority should be informed sufficiently in advance about the intention of an approved organisation to transition from paper-based to electronic-based internal flow management, including a project plan addressing the transition's key steps and a target date for its 'go-live'.

5.2. Implementation team

It is recommended to create an implementation team composed of future users covering all user-profiles to assess that the tool can provide all expected functions, prior to declaring 'ready for implementation' to the authority. Management should be informed about the milestones achieved and difficulties found during the implementation.

5.3. Exposition update

The Exposition needs to be revised to describe the new process. All existing procedures should be revisited to identify the required changes. The description of the tool in the Exposition will identify the names of the staff responsible for assigning credentials and monitoring the proper functioning of the tool.

5.4. User functions and rights

Credentials for the internal tool should be provided individually to each user and the user should provide formal confirmation of receipt.

The profile of each individual user should be tailored to their roles and attributions within the organisation.

The system will record the additions and deletions of users in the tool as well as any changes to their privileges.

The organisation should keep the right to revoke the privileges of each user. The person nominated for this role should be declared in the Exposition.

5.5. Training of users

Training should be provided explaining the tool and the detailed processes for each involved user of the tool. Personnel requiring accessing the records generated by the tool should also have received training to the required level.

The training should contain the process to follow in normal conditions and in conditions when the tool is not available or downgraded (e.g., communications failure; end-user device inaccessible; total system failure) and alternative procedures to be followed in these cases.

The training should explain the meaning of the electronic signature, its legal validity and consequences, considerations that each user should take to prevent misuse of their electronic identity and means for e-signature. Training should also involve understanding the authenticity aspects and how to verify the authenticity and integrity of a record.

The training should explain how to get help and report malfunctions of the relevant tools.

5.6. IT involvement

In case of an externally provided tool, in-house IT specialists (or IT specialist form a subcontracted organisation that provides the service of the daily administration of IT resources) should have a general understanding of the requirements, architecture, working methods and characteristics of the tool and be trained for the daily administration of the tool.

5.7. Internal assessment and monitoring

The implementation team will keep record of all reported malfunctions during the first weeks after implementation.

Within three months of use, an internal audit should assess the tool functioning, assessing samples and interviewing users. This would allow to eliminate glitches of the tool and improve or complement the related procedures and training material.

5.8. Competent authority role during implementation and continuous oversight

Before approval, through the assessment of the applicable guidelines, authorities can predetermine if the tool/system/process fulfil the intent of these Guidelines and comply with Regulation (EU) No 1321/2014. In addition to the verification of the compliance matrix (see Appendix), the authority should have a good understanding of the tool and covered scope by means of witnessing its functioning at the company site and interviewing company staff as needed. It is not expected that authorities will audit the software itself, but by means of sampling, the authority should understand it and be reasonably convinced that it will fulfil the applicable aviation safety requirements and these guidelines, as declared in the compliance matrix.

Once approved, by reviewing organisation-declared changes to the process/tool and by challenging the results of internal audits and finding closures, the authorities can be guaranteed that the tool/system/process remains compliant.

APPENDIX

COMPLIANCE MATRIX to support implementation of an internal flow management tool (§ 5)

Item / Reference in this document **(relevance)**	**Description**	**Comments**	**Fulfilled? (organisation assessment)**	**National Competent Authority notes/resolution**
Shared planning / § 5.1 (recommended)	Notify in advance the competent authority about the intention to change the internal process to rely on electronic means.			
Implementation team / § 5.2 (recommended)	Create an implementation team with staff representing affected functions to participate in the definition of the tool, anticipate difficulties, participate on testing of prototypes, facilitate tool implementation, contribute to training, support peers after tool deployment, etc.			
Exposition / § 5.3 145.A.70 (or similar) (mandatory)	The Exposition, and relevant internal procedures, describe the electronic processes. *Note: approval of the corresponding revision of the Exposition implies that permission to operate using the electronic means there described. This should be only done after the compliance with all items has been achieved and verified.*			

Users / § 5.4 145.A.30(e) or 145.A.35(b) (or similar); (mandatory)	1. Each staff member performing functions for which the electronic tool is needed, has been assigned with credential that identifies her/him and can only be used by her/him 2. The tool entitles each user to only attests the process/steps for which the organisation has qualified her/him in accordance with the Exposition. 3. Tool administrators can monitor the list of all users registered in the tool and their privileges and add/modify/remove to keep alignment with the Exposition.			
Training / § 5.5 (mandatory)	Users are trained. Training covers, depending on the role of the trainee, electronic tool standard processes, dedicated processes for super-users (e.g. granting tools credentials) and in-house IT support activities. Training covers both the use of the tool and the understanding of different roles and the assigned responsibilities.			
IT support / § 5.6 (mandatory)	Establish and qualify a group of IT specialist for the daily management of the tool.			
Acceptance by the competent authority / § 5.8	Provide extensive explanations about the functioning of the tool, how compliance with the intentions of this Guideline is achieved and demonstration of real cases to the			

(mandatory)	competent authority inspector. Address concerns by the inspector.			
Post-implementation assessment / § 5.7 (recommended)	Improve the tool/internal process as needed after gaining some experience with the tool. Keep the authority informed prior to incorporating the required changes.			