Understanding Authority LOI for Aviation Software

DASA Aviation Software Symposium
FLTLT Jaiden Kennedy
02 Aug 2019
Overview

• What is LOI?
• Why you need to understand Authority LOI
• Terminology
• Assessing the requirement for Authority LOI for software Aspects
• Conduct of Authority LOI for software aspects
• Delegating Software LOI
• Role of CVE vs Authority inspector for software audits
What is Level of Involvement

• **What?**
  – “Selection of the compliance demonstration activities and data that the [Authority] will investigate and the depth of these investigations during the certification process” – EASA

• **‘Involvement’ in What?**
  – In applicant assessments/Decision making process?
  – Involved in generating or compiling evidence showing compliance?
  – Involvement in the Certification Programme.
    • The Certification Programme presented to the Authority must include acceptable provisions to allow the Authority to review required Compliance Demonstration evidences.

• **How:**
  – Negotiated set of evidences and activities in the CPP, expanded in the PSAC
What is Level of Involvement

- Demonstration of airworthiness of product
- In particular compliance with certification basis

DOA oversight

- Demonstration of capabilities (organisation, procedures, competencies and resources)
- Also providing a picture of performance of the organisation
Why you need to understand Authority LOI

• Programmatic risks can arise if requirements for Authority LOI are not able to be achieved due to limitations in existing contracts.
• Assist in the ease of development and negotiation of a Certification Programme.
• Prevent misunderstandings arising from role confusion.
• Need to understand that the Authority may seek a range of evidences and time up-front in your software development.
• Sourcing software from foreign sub-contractors may often generate a requirement to send DASA Software SMEs overseas, or require a considered and informed proposal to appoint a delegate.
De-confusing terminology

- **[TAREG] Compliance Finding:** Meant different things to different people, may have referred to:
  - Authority inspections of selected evidence? – Authority Inspection delegated from the TAR/DAR
  - Assessment of CRE deltas?
  - Involvement in the Design Process?
  - Supplies Acceptance functions?
  - Assessment of future Supportability?

- **Compliance Demonstration**
  - An activity by the applicant to confirm compliance of a design to certification requirements.
  - May involve the creation, compilation, inspection or review of compliance demonstration evidences.
De-confusing terminology

- **Inspection of Compliance Demonstration Evidence (ICDE):**
  - An [Authority] Inspection of the Compliance Demonstration Evidences generated by the applicant.
  - Includes evidence submitted for (or sampled/witnessed by) Authority review during LOI, or submitted with applications for approval of a Major change (or generated internally for Minor changes).

- **Level of Involvement**
  - A review of Compliance Demonstration Evidences by the Authority during the conduct of the applicant’s Certification Programme.
  - Identified LOI must be completed prior to applying for approval of the Major change.
Assessing LOI

• The Authority is not resourced to review all affected compliance evidences for an application.

• A risk based decision made through:
  – An assessment of the likelihood of an unidentified non-compliance in an application. Considering:
    • Novelty,
    • Complexity,
    • Organisational Performance
  – The criticality (safety affect) of such a non-compliance

• The use of a risk based approach, allows the authority to focus it’s assurance role on the most important aspects of a design change.

• The LOI approach is consistent with international convention and best practice for Airworthiness regulation.

• Ensure DASA does not waste reviewing trivial compliance demonstration activities
LOI – Risk of a Non-compliance

- Step 1: Likelihood
  - Novel to who?
  - Complex to who?
  - Who assesses applicant performance?
Recall: Oversight vs LOI

- **LOI**
  - Demonstration of airworthiness of product
  - In particular compliance with certification basis

- **DOA oversight**
  - Demonstration of capabilities (organisation, procedures, competencies and resources)
  - Also providing a picture of performance of the organisation
Step 2: Criticality

*Intuition DAL A or B Software will usually always require class 3 or higher*

<table>
<thead>
<tr>
<th>Criticality (see Chap. 3.3)</th>
<th>Likelihood (see Chap. 3.2.5)</th>
<th>Very low</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Critical - DAL D</td>
<td></td>
<td>Class 1</td>
<td>Class 1</td>
<td>Class 1</td>
<td>Class 2</td>
</tr>
<tr>
<td>Non-Critical/Critical* - DAL C</td>
<td></td>
<td>Class 1</td>
<td>Class 1</td>
<td>Class 2</td>
<td>Class 3</td>
</tr>
<tr>
<td>Critical - DAL B</td>
<td></td>
<td>Class 1</td>
<td>Class 2</td>
<td>Class 3</td>
<td>Class 3</td>
</tr>
<tr>
<td>Critical --DAL A</td>
<td></td>
<td>Class 1</td>
<td>Class 2</td>
<td>Class 3</td>
<td>Class 4</td>
</tr>
</tbody>
</table>

DAL C equipment that contributes to hazardous or catastrophic failure conditions is classified as critical.
Assessing Software – LOI: Historical difficulties.

• Design is already Mature prior to submitting a CPP
• Applicant cannot provide key documentation such as the PSAC or the Change Impact Analysis that is required to undertake the assessment.
• Perception that the PSAC is ‘accepted’ without being provided to the Authority.
• Insufficient data is submitted to assess the CPP: Authority is told requested data is ‘not in the contract’, or other difficulties.
• Not understanding different roles between a CVE Inspection and Authority inspection.
• Data requested by the Authority to complete LOI is ‘not available’.
So what? What do we look at?

- Depending on the project (and certification basis), it may not always make sense to look at the same information.

<table>
<thead>
<tr>
<th>EASA Lol</th>
<th>Desktop and on-site audits</th>
<th>Document review</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of on-site audits</td>
<td>PSAC/PHAC and related SW/AEH plans</td>
</tr>
<tr>
<td></td>
<td>Planning audit (desktop)</td>
<td>Verification audit (on-site)</td>
</tr>
<tr>
<td>Class 1</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Class 2</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Class 3</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Class 4</td>
<td>As necessary *</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Upon request
LOI Typical Activities

• Why is involvement during the software lifecycle preferable:
  – Authority review may identify a requirement to generate additional evidence or undertake actions where findings or deficiencies are identified.
  – Authority Inspection is improved by a capacity to witness testing, participate in reviews and witness builds or conformity activities.
LOI Typical Activities

- As a result of these issues, it is preferable that the Authority is involved upfront and as early as possible, and at key points in the software lifecycle.
LOI Typical Activities

- There is no mandated policy on how the Authority is to achieve its audit outcomes, however where suitable the Authority will align with good international practice.
  - An alternative may be sought by the Authority or applicant, depending on the particular situation, certification requirements, or lifecycle of a software item.

- **International Practice: Stage Audits or inspections: “Stage of Involvement” or ‘SOI’**
  - Terminology used by the FAA to describe a staged auditing process
  - Originally described in the FAA Job Aid (Now historical) describes an inspection process that might be used by: ‘Authorities’, ‘Desigees’ [DERs], and ‘Applicants’.
  - Continues to be used now internationally.
LOI Typical activities: planning audit (SOI 1)

1. Assure plans and standards meet DO-178B objectives and address other applicable software policy, guidance and issue papers.

2. Assure that the processes described in the applicant’s plans meet the objectives of DO-178B and address other applicable software policy, guidance, and issue papers.

3. Obtain agreement between FAA and applicant on the plans, standards, and proposed methods of compliance.

- Note: For Software Aspects, the Authority will typically seek to achieve some or all of the outcomes prior to approving the CPP.
LOI Typical Activities – Development Audit (SOI 2)

1. Assess implementation of plans and standards for the software requirements, design, and code, and related verification, SQA, and SCM data.
2. Assess and agree to plans and standards changes.
3. Assess implementation of new technology and methods to ensure compliance to plans, standards, and agreements.
4. Assure life cycle data satisfies the certification standards objectives and other applicable software policy, guidance and issue papers.
LOI Typical Activities – Verification Audit (SOI 3)

1. Assess implementation of verification and test plans and procedures.
2. Assess completion and compliance of all associated SCM and SQA tasks.
3. Ensure software requirements are verified.
4. Ensure robustness testing is planned and is being performed.
5. Ensure analyses (including timing, memory, test coverage, structural coverage and data and control coupling) are being performed as required by the certification standard.
6. Ensure verification activities satisfy the certification standards objectives.
LOI Typical Activities – Final Audit (SOI 4)

1. Assure final software product meets the certification standards objectives and is ready for certification.
2. Address any open items.
Focus Areas

– If there are novel or more critical aspect of the software design, then the Authority will typically focus it’s review on these components. eg:
  • Thread traces will be done against affected Safety Critical Requirements.
  • Planning review may focus on design standards for novel techniques.
  • Potentially a focus on the Change Impact Analysis and regression testing where the modification to the Computer Software Configuration Item may affect existing safety critical requirements / hazards.
What else may be audited by software inspectors

- Other authority sections have differing LOI requirements
- Authority software SMEs may seek involvement in development assurance objectives and focus on requirements validation activities.
- Authority will apply LOI similar to the above for changes to safety critical Complex Electronic Hardware upgrades.
- Minor Changes to type?
- Other Authority approvals: i.e. AUSMTSO, UAS, ANSPC, may have a similar process in the future.
Outcomes of Authority LOI

• Authority will provide a minute at defined stages (perhaps linked to SOI stages) disclosing the outcomes of these involvement activities.
• Authority will provide a report once LOI is complete, advising that Authority LOI (for software aspects) has been closed.
• Applicant cannot submit a declaration of compliance to the Authority until all defined Authority LOI is executed – as the certification programme is not complete.
Outcomes of Authority LOI – Adverse feedback

• Authority may pass on Findings and Actions that will need to be closed prior to closing LOI.
• Decision to not action findings and actions will require production of an MCRI (ESF, exception) and DASA must be presented evidence that the elevated risk level has been accepted by command IAW the principles of the DASP.
• Authority may also pass on observations or issues (items related to other areas of the Certification Programme but not precluding closure of LOI)
Outcomes of Authority LOI – Adverse feedback

(What we don’t want to see)
Executing Software LOI: Historical difficulties.

• Nested documentation.
  – DASA will request a document, but the evidence targeted is in a subordinate document. Seeking the evidence then causes a delay
• Notes taken by auditor become Intellectual Property of the applicant.
• International travel.
• Form 31a submitted concurrently with evidence required to complete Authority LOI.
Appointment of other Authority Compliance Demonstration Inspector

• Authority may consider appointing an external resource, but must be satisfied that the individual is:
  – Sufficiently Competent.
    • Authority preference is that an external inspector routinely makes similar assessments for DASA or other Authorities (i.e. FAA, CASA).
  – Sufficiently independent.
    • The inspector must be demonstrably independent from the applicant: Cannot work for the MTCHO or the Design Organisation.
    • The Authority will typically not accept proposals to use DERs employed by a subcontracted design organisation.
    • The delegate must not be involved in the design in any other way.
  – Will conduct the inspection IAW authority processes, or through a system that aligns with Authority processes.
• Significant discussion with the Authority is required to achieve this process.
Audits done by Compliance Verification Engineers = LOI?

- Short answer: No
- Many CVEs may elect to follow (or follow a similar process) to the SOI concept described earlier, to achieve their assessment.
- This shared terminology can lead to significant confusion.
- DASA may elect to attend a CVE ‘SOI audit’, rather than to run our own on-site audit, to fulfil our assurance outcomes.

<table>
<thead>
<tr>
<th>EASA LoI</th>
<th>Desktop and on-site audits</th>
<th>Document review</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of on-site audits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Planning audit (desktop)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Development audit (on-site)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verification audit (on-site)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Final audit (desk-top)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSAC/PHAC and related SW/AEH plans</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SAS/HAS + SCI/HCI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Applicant SW/AEH Review report</td>
<td></td>
</tr>
</tbody>
</table>

Class 1: None None None None None None None None
Class 2: None Yes None None Yes Yes Yes None
Class 3: 1 Yes Yes Yes Yes Yes Yes Upon request
Class 4: As necessary Yes Yes Yes Yes Yes Yes Upon request

Applicant “SOI” Reports
Clarification Under DASR, FAA DER’s and CVEs

- Projects will sometimes reach back into parent companies (etc) and make use of individuals with privileges and competencies under different regulatory systems. An example of this are individuals with FAA DERs designation, while employed by a design organisation, are able to conduct Authority inspections on behalf of the FAA.
- While a DER (etc) qualified individual may be appointed as a CVE for a DASR MDOA; they are not conducting assessments on behalf of the Authority.
- No one is conducting assessments on behalf of the Authority unless they have been explicitly notified by the DASA that they are fulfilling this role.
- Intuition: When contracted as a CVE, DERs and other highly competent individuals are not exercising an Authority delegation. However, when such an individual is contracted (and this is outlined to the Authority in the CPP), this *may* result in lower Authority LOI.