



Using RPA to Best Effect in Software System Acquisitions and Modifications – Can RPA Save Cost and Schedule?

FLTLT Justin Diamond

SCI1B





Introduction

- **Discuss in context of the expanded Recognition of Prior Acceptance (RPA) Regulations - TARREG 2.2.7**
- **Applicability and Application to Systems with focus on Software System Acquisitions and Modifications**
- **Contribution to savings on Cost and Schedule**
- **What it is not – Quantifying Potential Savings**





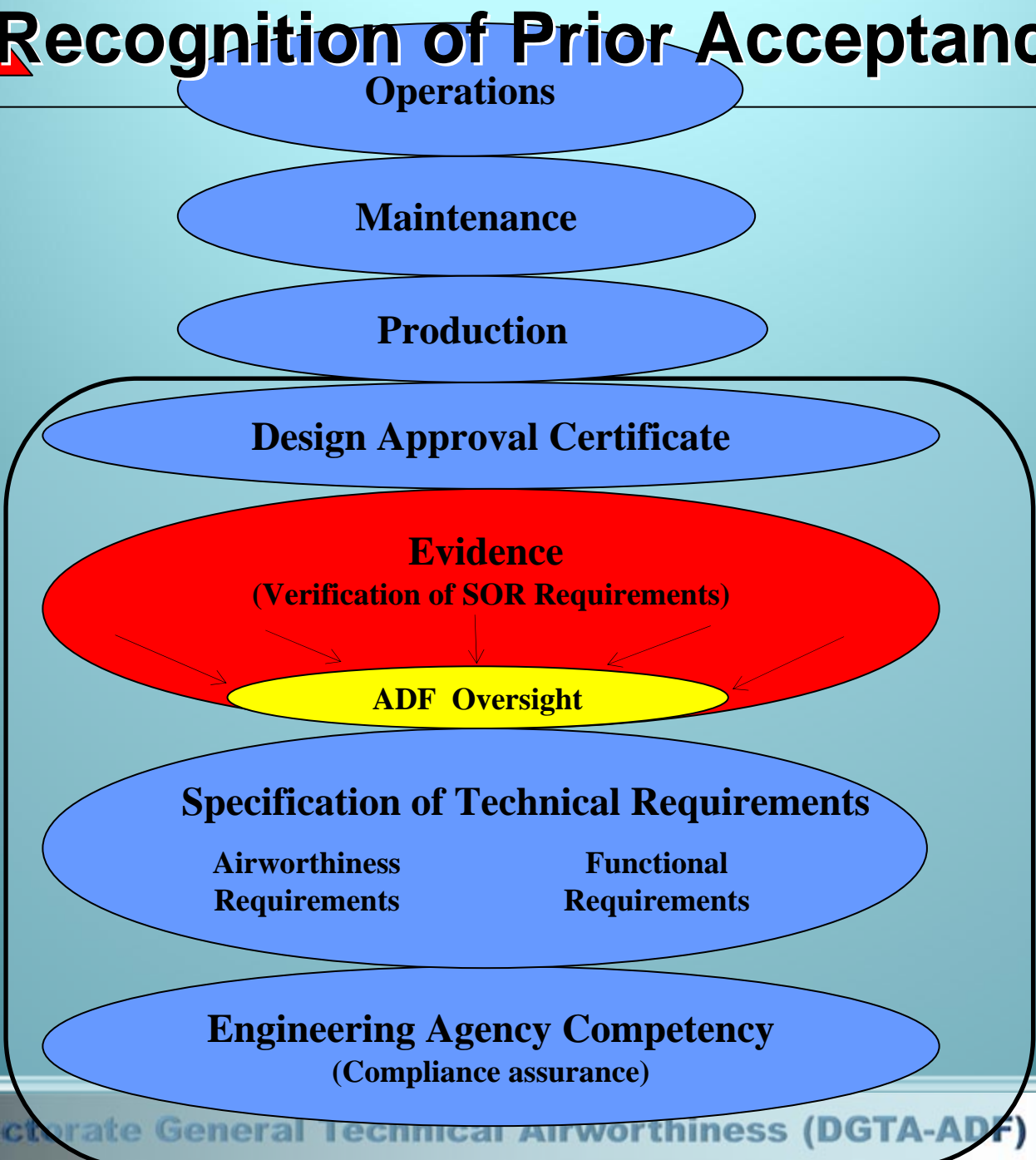
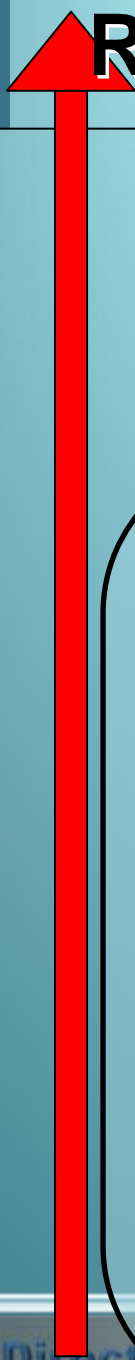
Recognition of Prior Acceptance (RPA)





Recognition of Prior Acceptance (RPA)

Airworthiness Confidence Meter



Design Acceptance





Recognition of Prior Acceptance (RPA)

- Aim is to substantially reduce the ADF's cost, schedule and technical risk
- Scopes the ADF's level of oversight required
- The ADF's role in reviewing evidence produced by designers depends fundamentally on involvement of another NAA
- Can RPA contribute to a significant reduction in cost and schedule for software systems?
 - Yes **BUT**, must be managed appropriately to ensure ADF's Design Acceptance Obligations are satisfied





RPA

- As mentioned previously, Certifying Aviation Software requires *considerable and useful Planning*
- If RPA is to be a cornerstone of the Design Acceptance Strategy it must be scoped and agreed early in the program (Ideally pre-first pass approval, at the latest prior to Contract Signature)
 - Documented and agreed with TAR via endorsement of the PDAS





Fundamentals

- **Responsibility of an NAA to assess an aircraft or modification to aircraft design is appropriately safe for flight**
- **Achieved via:**
 - **Prescription** of airworthiness requirements
 - **Evidence** that design complies with the requirements
- **For software airworthiness requirements:**
 - System/Software Safety Programs determine what the Appropriate behaviours of the system should be.
 - Software Assurance provides the confidence that software complies with those designed behaviours.





Fundamentals

Why do we review evidence?:

- We review evidence to confirm airworthiness and functional/performance requirements meet our specification.
“Ultimately, the TAA must be satisfied that compliance with the certification basis has been adequately assured before recommending an AMTC/STC for new or modified aircraft.”
- Other Reasons:
 - Acceptability of deliverable for milestone payment
 - Provide greater understanding of design
 - Assurance that evidence provides adequate foundation for through-life support
 - Good corporate governance





Fundamentals

What constitutes “evidence” wrt CF?

- NOT just contractual (DID) deliverables
- Also Includes:
 - Design documents, test reports, etc, that were not DIDs
 - ADF inspections
 - ADF witnessing of testing
 - ADF testing (e.g. AOSG reports)
 - ADF involvement in key meetings (e.g. design reviews)
 - Minutes of key meetings (e.g. system safety working groups)
 - Discussions with designers (documented)
 - IV&V assessments, ISA outcomes
 - etc





Compliance Findings – What are they?

A compliance finding is an engineering decision that an aircraft design satisfies an airworthiness requirement.

- based on relevant *evidence*,
- achieved by a competent agency
- must be relevant to the *Configuration* being offered for acceptance and the *Role* and *Environment* in which the aircraft will be employed





Fundamentals...cont

- **Many factors affect scope of Compliance Findings**
- **Depends on:**
 - Involvement of NAAs (if any)
 - CRE understanding of NAAs (if any)
 - CRE understanding of design agency
 - abilities of design agency
 - scope of modification
 - airworthiness implications of particular CB entry
 - extent of 'similarity' application





Design for ADF aircraft without NAA oversight

Compliance finding process:

- DAR/DGTA decide the relative importance of the compliance finding
 - CFA obtains a sound understanding of the relevant standard in the certification basis
 - Early in project, CFA plans how he/she will make compliance finding
 - Contractor presents evidence, asserts compliance with CB item
 - CFA assesses the evidence presented by the contractor to support the assertion of compliance
 - CFA decides whether the evidence presented supports the contractor's assertion
 - Where evidence doesn't seem to fully support the assertion, CFA seeks further information/insight/evidence
 - CFA updates PEM/DAR, and ultimately makes compliance finding
- Ultimately, the TAR must be satisfied that compliance with the certification basis has been adequately assured.*





For Software

- **Compliance Finding Process Overview**
 - **Establish the Basis**
 - The system safety program drives software assurance requirements.
 - The certification basis should identify the relevant software assurance standard.
 - Is it implicitly identified? (e.g. FAR 2x.1309)
 - What software level? (Look to consequences of failure or partial performance as identified by the system safety program.)
 - **Plan the Compliance Finding**
 - Determine the Level of Involvement.
 - Risk based approach to resource allocation.
 - Identify the objectives to be satisfied.
 - Identify the required evidence.
 - Impact on contract (what must we pay for) and compliance finding schedule
 - How will the compliance finding activities be conducted? (On site audit/appraisal/review, desktop review, combination)
 - When will the compliance finding activities be conducted?
 - Who will conduct the compliance finding activities?
 - Identify the focus of the compliance finding.
 - Document the compliance finding plan.





For Software...cont

- Review 1: Planning (*Assume Highest Level of Assurance Required e.g. RTCA/DO-178B Level A*)
 - Goal
 - Verify that the developer has sufficient and appropriate plans in place to achieve certification.
 - When
 - As soon as possible after contract signature, but plans need to be in place.
 - Objectives
 - Table A-1.
 - Tables A-8 and A-9 as appropriate.
 - A-10-1 and A-10-2.
 - Evidence
 - PSAC, SDP, SVP, SCM Plan, SQA Plan
 - Software Requirements, Design and Code Standards
 - SQA Records, Software Verification Results
 - Tool Qualification Data
- Review 2: Requirements
 - Goal
 - Verify that software requirements have been developed and verified.
 - When
 - At the end of the software requirements process but prior to the software requirements review.
 - Objectives
 - A-2-1 and A-2-2
 - Table A-3
 - Tables A-8 and A-9 as appropriate.
 - Evidence
 - Software Requirements Data, Software Verification Results





For Software...cont

- Review 3: Design
 - Goal
 - Verify that the software architecture and software design have been developed and verified.
 - When
 - At the end of the software design process, but prior to the software design review.
 - Objectives
 - A-2-3, A-2-4 and A-2-5.
 - Table A-4
 - Tables A-8 and A-9 as appropriate.
 - Evidence
 - Design Description, Software Verification Results
- Review 4: Code
 - Goal
 - Verify that the source code has been developed and verified.
 - When
 - At the completion of the software coding process but prior to the test readiness review.
 - Objectives
 - A-2-6 and A-2-7.
 - Table A-5.
 - Tables A-8 and A-9 as appropriate.
 - Evidence
 - Source Code, Software Verification Results





For Software...cont

- Review 5: Test
 - Goal
 - Verify that software behaviours have been adequately explored and verified as correct.
 - When
 - At the end of the software testing process but prior to formal release of the software.
 - Objectives
 - Tables A-6 and A-7.
 - Tables A-8 and A-9 as appropriate.
 - A-10-3.
 - Any other objective that is still outstanding.
 - Evidence
 - Software Verification Cases and Procedures, Software Verification Results
- Finalise the Compliance Finding
 - Has each objective been satisfied?
 - Satisfied
 - Not yet established
 - Not satisfied
 - Does the software comply with the standard?
 - Compliant
 - Non-Compliant
 - Non-Compliant but Acceptable
 - Retention of Risk
 - Unless risk has been referred and retained through a defined mechanism (e.g. Issue Papers), by making a finding of “Non-Compliant but Acceptable” the compliance finding agency is retaining the risk associated with any shortfalls.





RPA

- **Typical ADF RPA Scenarios:**
 1. Leveraging off previous NAA certifications for **extant aircraft designs**
 2. Leveraging off previous NAA certifications for **extant equipment/system design**
 3. Engaging an NAA to oversight the design of **ADF-specific modifications**
- ***All these scenarios are representative of the guidance in Annex D to Sect 3 Chap 12 of the TAMM (to TARREG 2.2.7)***





Application of RPA #1: Extant aircraft design

- **Examples:**
 - C-17A, F/A-18F*, B737, B300
- **Relatively straightforward:**
 - Assumption that NAA has performed or will perform competently in the role as Type Certification authority
- **Primary ADF role, in general is to ensure the NAA discloses:**
 - what their certification does/doesn't cover
 - the Certification Basis + assumed Role/Environment
 - any risk treatments applied (e.g. retention, workarounds, etc)
- **Provided all satisfactorily disclosed, ADF accepts the aircraft is adequately safe for the original Role & Operating Environment (R&E)**
 - i.e. R&E assumed by designers and agreed by NAA



- For Aviation software:
 - ADF's Design Acceptance process primarily focused on ***assessing compatibility of design with ADF's proposed Role + Operating Environment***
- ADF must via the compliance finding process:
 - Obtain an understanding of original R&E
 - Obtain an understanding of ADF's proposed R&E
 - highlight incompatibilities, so shortfalls or risks can be treated
 - assess risk treatments approved by NAA (Most important as ADF risk appetite can be substantially different to other nations)
 - assess applicability and acceptability of those risk treatments
 - Develop further risk treatments as required
 - Refer risk to appropriate authority (last resort) – Typically via Issue Paper





Application of RPA #1: Extant aircraft design (cont)

- **Software specific Challenges:**

- Minimal if design is compatible with ADF R&E
- 'Minor' changes to extant design can have dramatic impacts (F/A-18F) and therefore reduce reliance on RPA and increase ADF required oversight
- If identified late in program then large impact on schedule resources.
- Important to identify any changes up front identify CFA resources required throughout program
- Prior Certification by NAA, Establish the extent of RPA:
 - Determine the baseline from which the ADF version will be derived.
 - Identify that that baseline was certified.
 - The ADF baseline needs to be derived from a certified baseline if RPA is to apply.
 - Identify the basis of assessment.
 - Was it accepted at a lower software level?
 - Determine what risks were retained.
 - Some NAA risk appetites are higher.
 - Determine what procedures and workarounds were required.
 - Did they need to treat some risks to within acceptable bounds through procedures and workarounds?



- **Software specific Challenges (cont):**
 - **Determining Non-Interference if we do modify:**
 - **Goal:** To demonstrate that the ADF unique modifications have not negatively interfered with those aspects of the software to which RPA applies.
 - Requires re-verification of unchanged software.
 - Did we break it when we tried to improve it?
 - Aspects to re-verify determined by dependencies:
 - Functional
 - Code
 - Control
 - Data
 - Timing
 - Memory
 - Processor
 - **It is more than a regression test!**





Application of RPA #2: Extant systems design

- **Examples:**
 - AP3C Autopilot, C-130J- 30 Block Upgrades
- **Greater oversight by ADF required:**
 - Determine the role the NAA (Military or Civilian) has performed or will perform in the role as Type Certification authority (See Next Slide)
- **Primary ADF Design Acceptance focus is *assess compatibility of design with ADF's Configuration, Role + Operating Environment***
- **The ADF is required to:**
 - comprehensively assess impact of configuration deltas
 - comprehensively understand original R&E, and compare against our proposed R&E.
 - Manage identified deltas
 - assess risk treatments approved by NAA:
 - assess applicability and acceptability
 - confirm we are fully aware of all treatments
 - Develop further risk treatments as required
 - Refer risk to appropriate authority (last resort)





Application of RPA #2: Extant systems design

- Equipment/systems certified by **civilian NAA:**

- **Advantages:**

- Simple to apply (standards information readily available + system will meet standards)
- Application of Technical Standard Orders (TSOs) can assist
 - Requires judicious use, a TSO'd piece of equipment means that an item meets minimum applicable performance standards - still required to establish compatibility with our aircraft.

- **Disadvantages:**

- Certification only relevant to civilian R&E.
- Specific Mission systems receive little oversight, lesser standards acceptable
- STCs generally of limited benefit.

- Equipment/systems certified by **military NAA:**

- *** Only applicable if we confirm military was acting in the capacity of an AA*

- **Advantage:** Good potential to contribute to Design Acceptance, since role and operating environment often similar to our own

- **Disadvantages:**

- Access to detailed information on standards + tailoring
- Access to key NAA assessments
- Disclosure of risk treatments (e.g. limitations, mitigations, retention, etc)



- **Software specific Challenges:**
 - Integration Issues
 - Over-reliance or poorly scoped reliance on inappropriate RPA will lead to significant shortfalls in Design Acceptance and an increased level of risk being referred to higher authorities potentially impacting operational capability and/or reduction in safety margins
 - As per RPA #1 (See next Slides)



- **Software specific Challenges:**

- Prior Certification by NAA, Establish the extent of RPA:
 - Determine the baseline from which the ADF version will be derived.
 - Identify that that baseline was certified.
 - The ADF baseline needs to be derived from a certified baseline if RPA is to apply.
 - Identify the basis of assessment.
 - Was it accepted at a lower software level?
 - Determine what risks were retained.
 - Some NAA risk appetites are higher.
 - Determine what procedures and workarounds were required.
 - Did they need to treat some risks to within acceptable bounds through procedures and workarounds?



- **Software specific Challenges (cont):**
 - **Determining Non-Interference if we do modify:**
 - **Goal:** To demonstrate that the ADF unique modifications have not negatively interfered with those aspects of the software to which RPA applies.
 - Requires re-verification of unchanged software.
 - Did we break it when we tried to improve it?
 - Aspects to re-verify determined by dependencies:
 - Functional
 - Code
 - Control
 - Data
 - Timing
 - Memory
 - Processor
 - **It is more than a regression test!**





Application of RPA #3: Engaging an NAA to oversight ADF-specific design

- ADF's strong preference is for NAA involvement in aircraft modifications
 - Design Acceptance can be based largely on NAA's assessment of design
 - Examples: ARH, AEW&C
- **NAA advantages:**
 - Many NAAs are experienced in aircraft certification programs`
 - NAAs should have access to a wide range of certification specialists
 - NAAs are often local to design organisations
 - NAAs probably have previous relationships and experience with the design organisations (and vice versa)
 - NAAs don't have to rely on contract law to enforce requirements

NAAs can substantially reduce the strain on ADF resources (both project and specialist agencies)





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont)

We can rely on NAAs to provide oversight of specific designs provided:

- The ADF is able to assess the NAA as being a competent AA
 - Specified in current TAMM release
 - NAAs may be added after an assessment
- We assess them as suitable to oversight the ADF mod
 - (see next slide)

=> INFORMED Recognition of Prior Acceptance





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont)

An NAA is assessed as 'suitable' provided:

- Experienced in the subject certification issue
- Evidence exists that they are fully committed to the task
- Effective mechanisms in place to enforce their requirements on the designer
- They are aware of all ADF specification requirements for the design change
- They have a clear understanding of our proposed CRE
- We are fully aware of what they are/aren't attesting to





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont)

Civilian vs Military NAAs - preferences ?

- Both have their advantages and disadvantages
- Both acceptable provided shortfalls are managed
- **Generally:**
 - a civilian NAA is well suited to modifications that are civilian-like (i.e. modifications with parallels in civil aviation)
 - A military NAA can be well suited to military-unique modifications, particularly developmental modifications
- **New Tamm regs + annex on RPA is essential reading! (DGTA WEBSITE NPRM 02-09)**





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont)

Civilian NAAs:

- Advantages:
 - Extensive experience with complex modifications
 - Well-established level of oversight
 - Access to a wide network of technology specialists
 - No undisclosed risk retentions (systems must meet defined standards)
- Disadvantages:
 - Designs must meet NAA's own standards
 - Unlikely to allow ADF involvement in certification effort
 - No flexibility to trade off safety for mission-effectiveness
 - Unlikely to consider ADF's CRE
 - Will not assess whether system is fit-for-service (ADF Service)





Civilian NAAs (cont):

Assessed in
Compliance
Finding

- **ADF's Software Design Acceptance focus:**
 - Fully understand extent of CRE considered by NAA, and assess deltas across CB
 - Provide AA oversight for systems the NAA refuses to oversight
 - Provide oversight for design of mission systems
 - Confirm aircraft meets mission requirements
 - Obtain recommendations from NAA to enable ADF CFs
 - Provide corporate governance oversight of NAA efforts (?)
- **There will be shortfalls that the ADF must address**





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont)

Military NAAs

- **Advantages:**

- Flexibility to trade off safety for mission effectiveness
- Can consider ADF CRE
- Can assess whether system is fit-for-service
- Opportunities for ADF to be involved in certification effort

- **Disadvantages:**

- Level of AA oversight needs to be comprehensively pre-agreed (otherwise may fall substantially below ADF-accepted levels)
- Risk treatment decisions may be made without our agreement
- Difficulties in obtaining comprehensive standards information or data

**** While FMS has advantages, it has numerous pitfalls**
- need to manage carefully





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont)

Military NAAs (cont):

- **ADF's Software Design Acceptance focus:**
 - Confirm military will provide formal AA oversight
 - Confirm military oversight will be comprehensive (ie ADF-equivalent)
 - Ensure NAA's CBD is acceptable to ADF
 - Ensure NAA fully assesses compatibility with our CRE
 - Ensure ADF will receive CF recommendations from NAA
 - Ensure ADF obtains comprehensive insight into risk treatments agreed by NAA, and has a right of veto (if possible)
 - Provide corporate governance oversight of NAA efforts
 - (Ensure production oversight is satisfactory)
- **Where the Military NAA doesn't comprehensively cover any item, the ADF must overcome the shortfall**





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont

- **Software focus using FMS with USG**
 - **Establish the Basis**
 - The basis is the assurance objectives achieved by the USN, US Army or USAF to satisfy themselves that the software is safe.
 - What were the assurance objectives?
 - The ones that are inherently satisfied through correct application of their documented plans.
 - Be warned: USN, US Army and USAF verification activities do not finish with the developer, there is usually substantial flight testing involved. (How does this affect ADF acceptance?)





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont)

- Plan the Compliance Finding

- **Goal:**
 - Someone acting in the capacity as an Airworthiness Authority has evaluated the life cycle data against the relevant set of assurance objectives for the ADF CRE.
- What evidence is required to demonstrate equivalent rigour?
- What activities are required to overcome disclosure of evidence limitations?
- How will we identify the risks that were retained on our behalf?
- When will the activities occur?
- Does the FMS case provide access to the necessary evidence and enable the required activities?
- If the ADF cannot acquire the evidence, can we acquire access to it?
- If the ADF cannot acquire access to the evidence, can we obtain evidence (direct or indirect) that processes were correctly completed?
- If not, can we gain access to the development process and generate our own evidence that processes were correctly completed? e.g. participation in milestone reviews, test witnessing, etc.





Application of RPA #3: Engaging an NAA to oversight ADF-specific design (cont)

• Equivalent Rigour

- Did the USN, US Army or USAF apply the same level of rigour to the development of ADF software that they would have applied to their own?
- Requires evidence of:
 - Milestone satisfaction
 - Review completion
 - Absence of tailoring
- Did they have full insight into the ADF CRE?
- Did they have suitable test assets available?



- **Risk Retention**

- Did the USN, US Army or USAF retain any risks that the ADF would not have retained?
- Was the retention of any risks based upon workarounds or procedural mitigations?
- Could involve inspection and analysis of:
 - problem report databases,
 - certification evidence,
 - limitations of service release,
 - flight manuals,
 - procedures,
 - hazard logs,
 - etc.

- **Finalise the Compliance Finding**





RPA - summary

Summary:

- Expanded TAREG 2.2.7 and guidance in Sect 3 Chap 12 - **Essential Reading**
- In general the ADF's preference is for external agencies to act in the capacity of an NAA
- Where NAAs are involved, informed RPA can substantially reduce our CF efforts and thus subsequently reduce the resource requirements (cost/schedule)
- Failure to identify appropriate reliance on RPA early in program will lead to serious shortfalls in Design Acceptance = Cost/schedule Pressure





RPA - summary

- **Can it save cost and schedule?**
 - YES – But the application of RPA must be carefully managed and used appropriately. It does not absolve an organisations or individuals responsibility to conduct reasonable engineering practice
- **Engineers do not make decisions based on opinion.**
- **Engineers make decisions based on evidence and standards.**





Further Information

- AAP 7001.053 Technical Airworthiness Management Manual Section 2 Regulation 2.2.7 *Recognition of Prior Acceptance*
- Guidance in AAP 7001.053 Technical Airworthiness Management Manual Annex D to Section 3 Chapter 12 *Informed Recognition of Prior Acceptance*





Questions ?

