

RapiCover Tool Qualification for DO-178C

Tool qualification is essential in the development of critical embedded systems, and should be a key consideration from the earliest stages of DO-178C projects.

Our comprehensive tool qualification solution provides the resources and expertise you need to qualify RapiCover for use in DO-178C projects. Adopting our approach to qualification early on in your development process means you will benefit from:

- Early access to our expertise and experience in defining advanced tool workflows, and communicating with certification authorities.
- Comprehensive documentation and support that allows you to refine your qualification workflows and evidence ahead of time, as well as coordinate with your certification authority to reduce potential delivery delays.
- A flexible, collaborative approach to qualification that works for your project and organization and reduces costs and effort.

For background information on DO-178C and its objectives, see *About DO-178C and tool qualification* on the next page.

Qualification Kit

A Qualification Kit is a comprehensive documentation package that provides evidence that RapiCover meets the guidance given in DO-330 for commercial off-the-shelf (COTS) products. Our Qualification Kits include two sets of documents: Developer Documents and Tool User Documents. They also include checklists against which to check your compliance with DO-330 tool user objectives.

Developer Documents contain DO-330 tool qualification evidence, including a summary of the requirements, test plans and test results demonstrating that RapiCover complies with its requirements as per DO-178C (Figure 1 right).

Tool User Documents are template versions of documents that must be provided by a tool user to support their qualification of a COTS tool (Figure 2 right). These are pre-filled with cross-references to our Developer documents, further reducing the effort needed to complete your DO-330 tool qualification evidence.

The documentation and processes we use to produce our Qualification Kits for RapiCover follow the guidance in DO-330 for a TQL-5 COTS tool. DO-330 complements DO-178C by providing specific guidance for tool qualification, and defines the Tool Qualification Levels (TQL) 1-5.

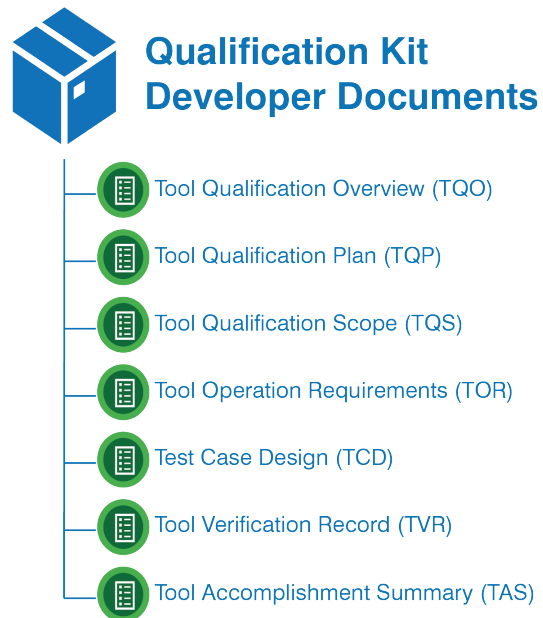


Figure 1. Qualification Kit Developer Documents

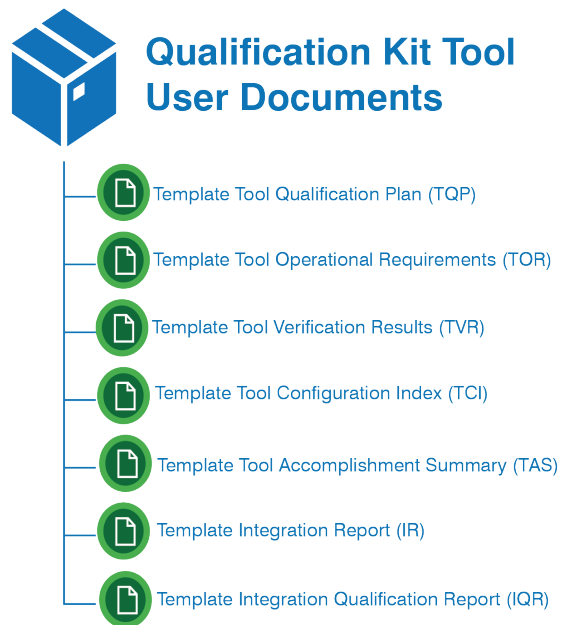


Figure 2. Qualification Kit Tool User Documents

Qualified Target Integration Service

To meet DO-178C guidance, you must provide evidence (in addition to our Qualification Kit documents) showing that the tool has been correctly installed and integrated into your specific development and target environment. To support you in this, we also offer a *Qualified Target Integration Service*.

Our Qualified Target Integration Service is delivered by Rapita Field Application and Software Quality Assurance experts, and includes comprehensive reporting, tests and expected results demonstrating that the integration works correctly.



Qualified Target Integration Service

- Expert engineering service
- Completed Integration Qualification Report (IQR)
- Comprehensive tests and expected results

Figure 3. Qualified Target Integration Service

Combined with the documentation provided in our Qualification Kits, the materials generated during the Qualified Target Integration Service complete the evidence you need for tool qualification.

Delivery process

A Qualified Target Integration Service is delivered in three stages, as shown in Figure 4:

- Preliminary assessment
- Testing and interim reporting
- Final delivery

Note: See the *RapiCover Tool Qualification for DO-178C Order Information sheet* for a more detailed version of this process, including key milestones and responsibilities.

Preliminary assessment

Rapita engineers review your integration and produce:

- A repro: An in-house integration that replicates your instrumentation and export settings as closely as possible.
- On-site tests: A suite of tests that exercise the integration in your specific build and target environment.
- A test oracle, which shows the expected output of the tests when run on your configuration.
- Preliminary Integration Qualification Report (IQR): A report which documents any issues that may affect the qualification of the tool.

Testing and interim reporting

Rapita engineers work with you to configure your integration and obtain correct results from the onsite tests. During this

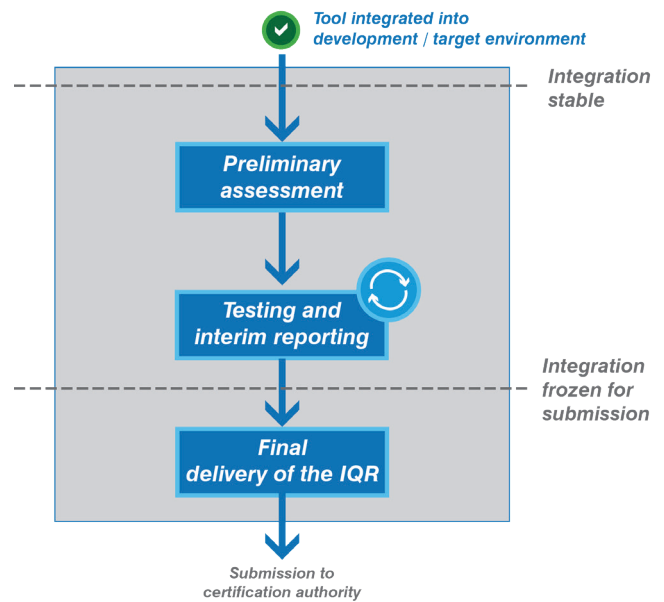


Figure 4. Qualified Target Integration Service - delivery process

stage, we may produce one or more iterations of the IQR and the onsite tests. The number of iterations, and the length of time it takes to reach the final stage, depends on the complexity of your integration and whether your configuration changes during the process. Before moving to the final stage, your integration is frozen for submission, so no more changes can be made to it.

Final delivery

We deliver the final version of the Qualified Target Integration Service deliverables, including the final IQR.

About DO-178C and tool qualification

DO-178C contains guidelines that deal with safety-critical software in airborne systems. Certification authorities (including the FAA in the US, and EASA in Europe) use DO-178C to assess these software systems.

According to DO-178C, you must qualify the software tools used in your project if:

- The tool could potentially insert an error or fail to detect an existing error.
- The tool's output will not be verified or confirmed by another verification activity.
- Processes necessary for certification are eliminated, reduced or automated by the tool.

You are responsible for qualifying the software tools you use in DO-178C projects. This means you have to provide detailed evidence not only that the tools meet their functional and robustness requirements, but also that they have been correctly integrated into your development and target environment.

Our Qualification Kits, along with our expert Qualified Target Integration Service, reduce the costs and effort required throughout the process.

Qualification options

We offer a flexible qualification approach for RapiCover, as shown in Table 1 below. We recommend you choose our comprehensive qualification solution (Option 5); however you may choose to undertake some of the qualification work yourself.

We can only provide a Qualified Target Integration Service if we have first integrated RapiCover into your development and target environment, via a Target Integration Service (TIS). See the *Target Integration Product Brief* for more information.

If you have undertaken the target integration work yourself, contact us to discuss your options.

Table 1. Qualification options

	Tool	Qualification		
		RapiCover tool	Target Integration Service	RapiCover Qualification Kit
Option 1	Rapita	Customer	Customer	Customer
Option 2	Rapita	Rapita	Customer	Customer
Option 3	Rapita	Customer	Rapita	Customer
Option 4	Rapita	Rapita	Rapita	Customer
Option 5	Rapita	Rapita	Rapita	Rapita

Key features

Clear qualification guidance

Our qualification kits include clear guidance on what to do during your tool qualification, including a qualification timeline.



Figure 5. Qualification timeline

Tool User Documents

Template Tool User Documents reduce the effort needed to develop your DO-330 tool user documents for RapiCover qualification. These are pre-filled with cross-references to RapiCover DO-330 Developer documents in the Qualification Kit.

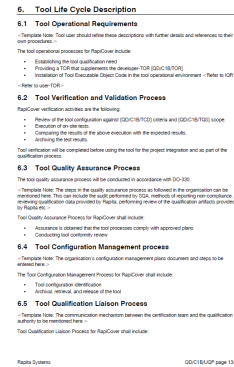


Figure 7. Tool user documents

Compliance checklists

Checklists are included in our qualification kits that help you check your compliance with DO-330 tool user objectives in each step from planning to approval.

Table T-0 - Tool Operational Processes

Objective	Details	Completion
T-0-1 The tool qualification need is established.	{{See developer TQP [QD/C1C/TQP 3.1.4] section 6 "Qualification Considerations."}}	
T-0-2 Tool Operational Requirements are defined.	{{Cross-reference developer TOR [QD/C1C/TQP 3.1.4] for individual requirements.}}	
T-0-3 Tool Executable Object Code is installed in the tool operational environment.	{{Cross-reference to the Integration Report.}}	
T-0-6 Tool Operational Requirements are correct and sufficient.	{{Reference your criteria. Also use TQS [QD/C1C/TQS 3.1.4] to scope the review.}}	
T-0-7 Software life cycle needs are met by the tool.	{{See developer TQP [QD/C1C/TQP] section 6 "Qualification Considerations."}}	

Figure 6. Compliance checklists help you check your compliance progress

Streamlined qualification material

The documentation, requirements and tests included in our qualification kits are custom depending on your specific development environment, helping you minimize your review effort.

Qualified instrumenters

The instrumenters used by RVS tools are qualified, so there's no need to manually qualify them.

Assurance issue notification

We notify you when we discover any assurance issues that might cause false positive results or introduce functional changes to your software. We keep you updated with the status of assurance issues regularly.

Announcement date: 10/26/2018, 00:00:00.000
Tracking number: +183801
Status: Resolved
Filed in: RVS 3.10
Products and versions affected:

- RapiCover product
 - Versions of RVS from 3.2 up to 3.9 and all versions of RPF are affected
 - Primitives that include function exists (cov_118_saa_a, cov_118_saa_b, cov_118_saa_c and cov_118_saa_d with --start=CBRT1181181181)
 - C, C++, Ada (all versions)

Summary of circumstances where the issue appears:

- Unreachable explicit returns

Problem report:

The return statement explicitly exits from a subprogram. The end of the subprogram is an implicit return. If there is an explicit return, we hide the unreachable explicit return. If there are unreachable explicit returns, this is usually an error in the code and needs to be addressed. RapiCover should mark these as potential exits, even though they are normally unreachable. In the affected versions, it fails to report the unreachable explicit return.

Example:

code:

```
void test3 (int A) {  
    return;  
    Rp_Ask1();  
    return;  
}
```

export:

```
/*  
  // 0 - verified, 1 - Unverified (justification)  
  // Function (F - covered) | S - not covered  
  // Position (A1 - covered | B - not covered)  
  // Data (C - covered | D - not covered)  
  // Statement (S - covered | S - not covered)  
  // LOOP (L - covered) | R - not covered  
  // Details (* - missing MC/DC condition) */  
19 | 0 | 1 | 1 | 1 | void test3 (int A) {  
20 | 0 | 1 | 1 | 1 |     return;  
21 | 0 | 1 | 1 | 1 |     Rp_Ask1();  
22 | 0 | 1 | 1 | 1 |     return;  
23 | 0 | 1 | 1 | 1 | }
```

In this example, the instrumenter fails to identify that the unreachable explicit return at line 22 requires function exit coverage. Thus RapiCover does not report "Function exists" in the third column at line 22 as shown in the export.

Recommendation:

If you suspect that your source code and integration are affected, or are in any doubt:

- We recommend manual analysis of unreachable explicit returns.
- Upgrade to RVS 3.10 or later.

Figure 8. Example assurance issue



Rapita Systems Inc.
41131 Vincenti Ct.
Novi, MI 48375

Tel (USA):
+1 248-957-9801

Rapita Systems Ltd.
Atlas House, Osbaldwick Link Road
York, YO10 3JB
Registered in England & Wales: 5011090

Tel (UK/International):
+44 (0)1904 413945