Work Authorization and Requirements Integrity

Introduction

This is the second in a series of articles on how the Rational Collaborative Lifecycle Management (CLM) solution supports compliant software development. It is highly recommended you first read the article in the series before proceeding.

Business Context

This article details several options for work review, approval and formal authorization. Some regulations that impact software development, like the FDA CFR 21, part 11 require electronic signature. Others, like Sarbanes Oxley, require implementation of internal controls to prevent unauthorized changes to systems that are material to the business. One of the implications of this is organizations must have controls in place to ensure no unauthorized changes are being made to systems that deal with the *organization's* financial data (work authorization). Part of the change and development process for many software systems involves requirements: their definition, review/approval, implementation, and validation. This also involves ensuring and proving the integrity of the requirements: that approved requirements are not changed by unauthorized persons and/or that the approved version of the requirement is the one that has actually been implemented and validated (requirements integrity). Companies must also prove that the defined processes and internal controls were implemented and sufficient. There are other regulations or standards that impose similar mandates on the development, delivery, deployment, and maintenance of software systems.

Required capabilities of Requirements Integrity and Work Authorization solution

- As an approval authority, I need the ability to approve the correctness of a specific version of a requirement
- As an approval authority, I need the ability to certifiably authorize work to implement, test, deploy, etc. the approved version of the requirement
- As an auditor, I need proof that only approved and authorized versions of requirements were implemented, tested, etc. and included in a given release

Requirements Integrity and Work Authorization solution configuration(s):

Different IBM Rational products or combination of products can be used to provide a Requirements Integrity and Work Authorization solution as part of a broader compliant software development solution. These include, but are not necessarily limited to:

- Integrated Rational Requirements Composer (RRC)/Rational Team Concert (RTC): RRC is used to define, review/approve, and manage requirements. RTC is used to authorize and manage work linked to the RRC requirements.
- RTC only: Use RTC work items to capture, approve, manage, and authorize changes and work. For example, RTC User Story, Enhancement, or Defect types of work items.

- Integrated DOORS/RTC: DOORS to define, manage, and sign-off on requirements. RTC work items to manage and authorize work assignments to implement, verify, deploy, etc. the requirements in a release.
- DOORS: DOORS to define, manage, and sign-off on requirements.

Every organization will have its own criteria to decide which product(s) to use to provide these capabilities and solution. This article focuses on the RRC/RTC solution examining different ways that agreement on project artifacts can be captured and the work to proceed at a given point in the process can be authorized:

- Review and approval of a requirements collection by requirements stakeholders
- Electronic signature authorization to implement a reviewed and approved requirements collection by business authority
- Multi-level approvals of a build for release into a user acceptance testing environment

Pre-conditions for the RRC/RTC solution detailed in this article:

- CLM (RRC and RTC) v3.01
- RRC/RTC integration setup (ref. http://publib.boulder.ibm.com/infocenter/clmhelp/v3r0m1/nav/5)
- RTC e-signature enabled approval established for the work item type to be used to track sign-off of a RRC formal review/approval (in this case, a custom "work authorization" RTC work item type based on the RTC Scrum template Task work item type).
- RRC Formal Review has been created and completed (ref. http://publib.boulder.ibm.com/infocenter/clmhelp/v3r0m1/topic/com.ibm.rational.rrm.help.doc/topics/c_reviews.html)
- CLM Money that Matters sample lifecycle project setup.

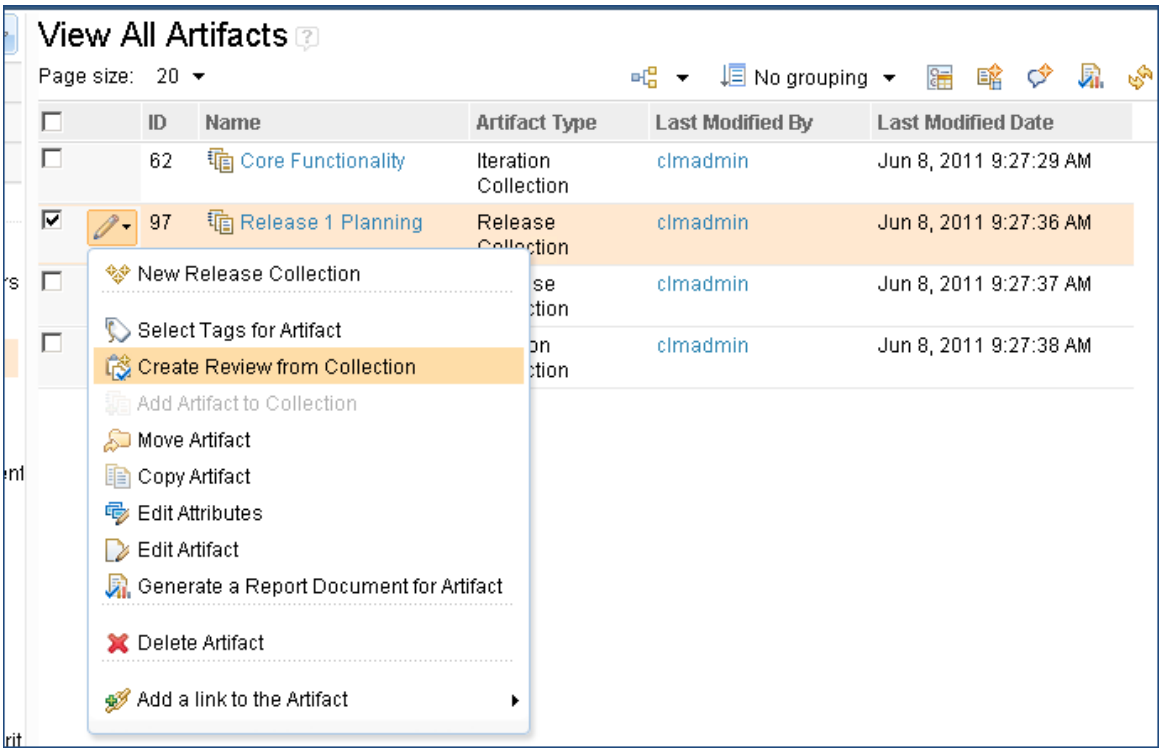
Review and Approve a Requirements Collection to ensure Requirements Integrity

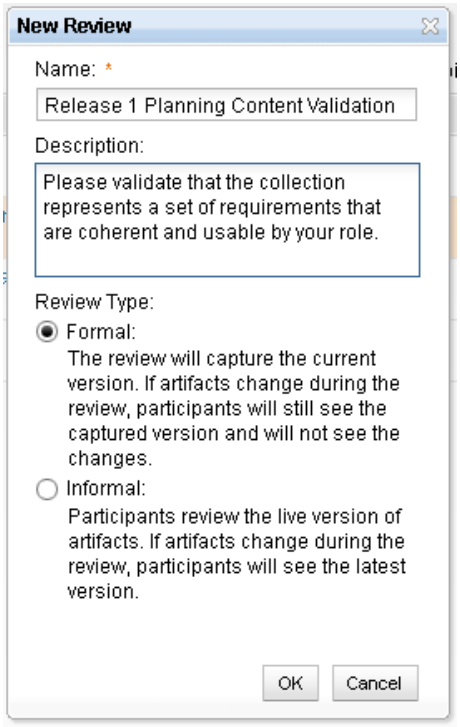
This activity mitigates the risk of having misunderstood, incorrect, or incomplete requirements implemented in a system. In this example we initiate a review and approval of a requirements collection in Rational Requirements Composer. As an approval authority, we then review, comment and approve the review to help ensure the integrity of the requirements.

Create a RRC Requirements Review from an existing RRC Collection.

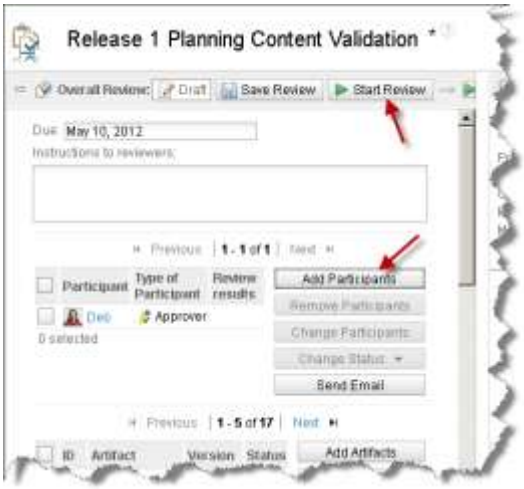
Assuming the role of Bob the business analyst, we log into RRC and from the requirements dashboard navigate to the JKE Banking Requirements project.

We then create a RRC Formal Requirements Review named “Release 1 Planning Content Validation” from the existing **Release 1 Planning** collection.

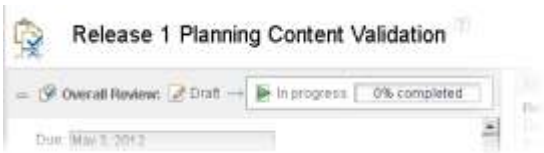




We then add another team member (Deb the developer) as an approver and then start the RRC Formal Requirements Review process. *Note: we would normally add additional team members to the review, but we are keeping it simple for this article.*

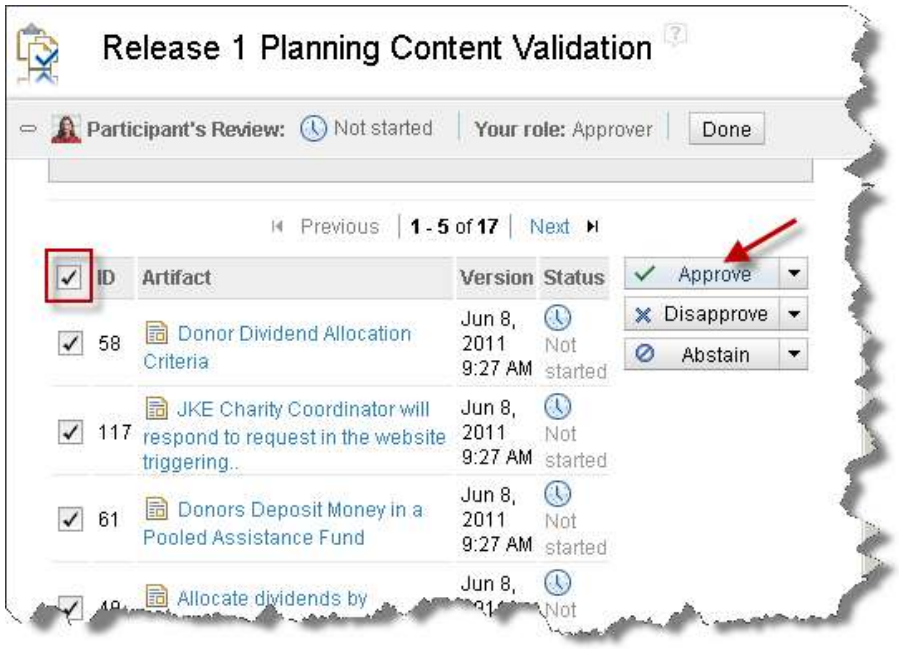


The review status will look like this:



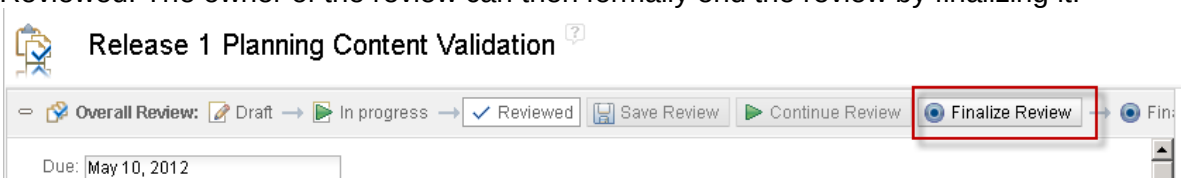
Participate in a review

As Deb, we find on her Requirements dashboard a link to the new RRC Review created by Bob to which Deb is assigned. We click on the link to the review, open up and review the requirements in the review, and optionally provide comments on the requirements under review. In this example we approve all the requirements in the review and then mark it Done.



Finalize a review

Once all reviewers have completed their reviews, the status of the overall review will be set to Reviewed. The owner of the review can then formally end the review by finalizing it.



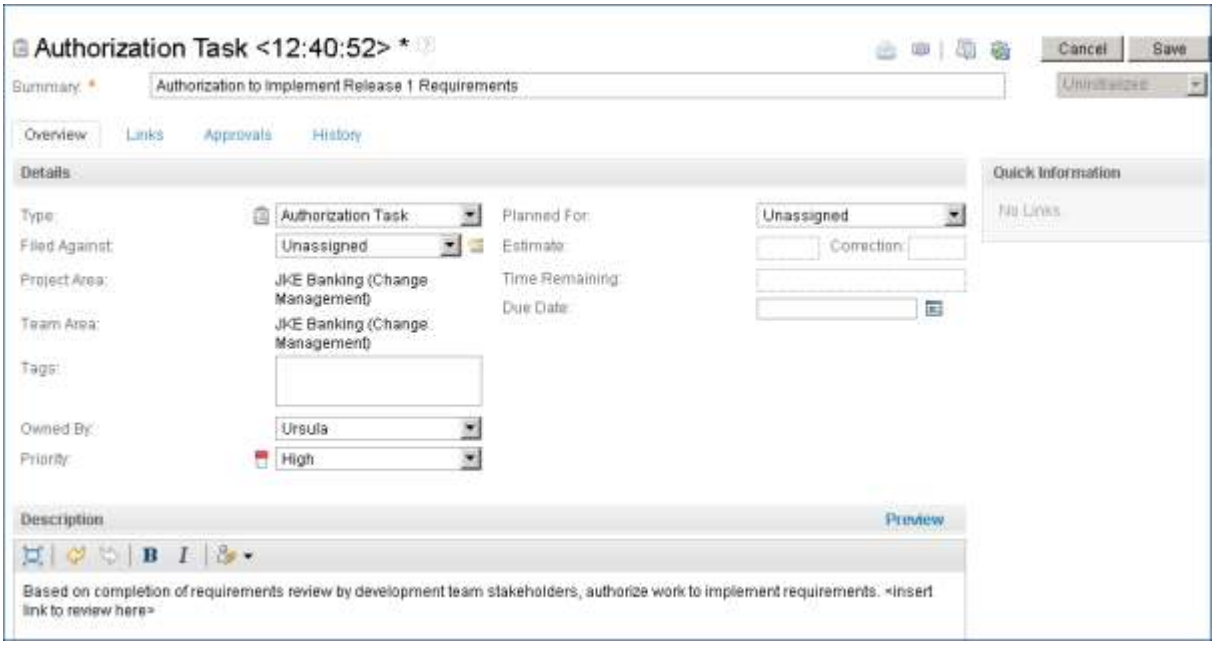
Implementing and using Electronic Signature for Work Authorization

In this section use a combination of Rational Requirements Composer and a Rational Team Concert Authorization Task. The Authorization Task is a custom RTC work item (WI) type created especially for implementing (satisfying) the corporate control “only authorized persons can authorize changes to material systems”. It is also used for creating an audit trail of electronic signature authorizations.

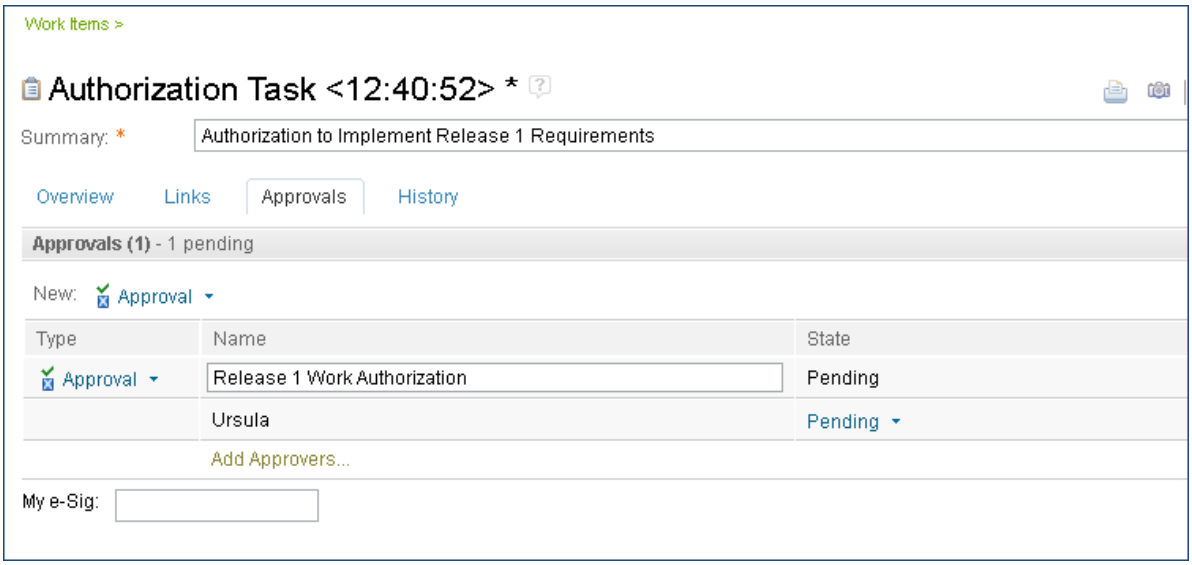
Prepare the work authorization

We have created the Authorization Task WI type within the RTC JKE Banking (Change Management) project. The first thing we do after logging into the RTC project we will use for work authorization is create a new Authorization Task.

Entering details in the Authorization Task as seen in this screen shot:



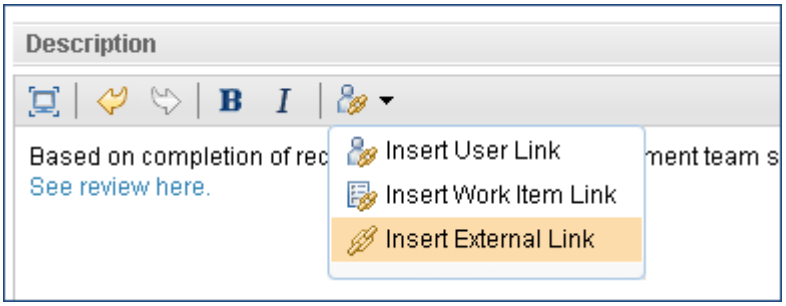
We use RTC approval and e-Sig capabilities to formally assign and capture work authorizations. In this example, we have added Ursula as a new Approver.



Link approved RRC Requirements Review to RTC e-sig enabled Work Authorization

We add to the RTC Authorization task a link to the RRC Requirements Review by opening the review within RRC and then copying and then inserting (or pasting) the URL into the RTC Authorization task.

> NOTE: We are using a URL link to the RRC requirements review so that the RTC Authorization task will have a direct link to the version of the requirements/artifacts in the collection that were reviewed and approved. This helps to ensure Requirements Integrity (that the developers and testers subsequently assigned tasks to implement and test these approved and authorized requirements are in fact working against the authorized and approved version of the requirements).



Authorize Work to proceed on Reviewed and Approved RRC requirments

The work authorization is now ready to be used by the person(s) assigned as the approver to capture their authorization via e-Sig in the RTC Work Authorization approval.

The assigned approver simply opens up the work item, transitions the WI state to “start working”, uses the link to the RRC Review to confirm that the review is finalized and meets the authorizer’s

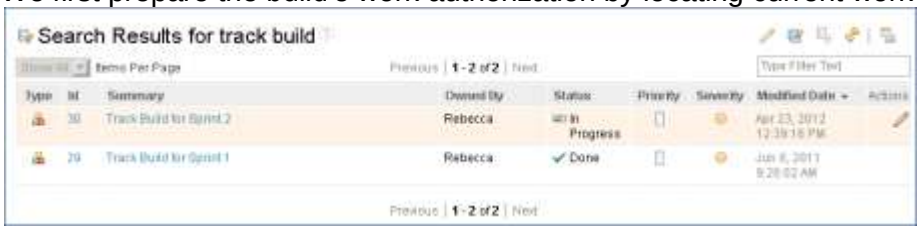
approval signified and captured by using RTC Work Authorization e-Sig approval feature, and then saving the work item in a “Completed” state.

Implementing Multi-level Work Authorizations

It is also possible to easily implement and use a multi-level approval/authorization using Authorization Tasks in Rational Team Concert. We will show in this section how this can be done using RTC work items to track, approve, and authorize a build.

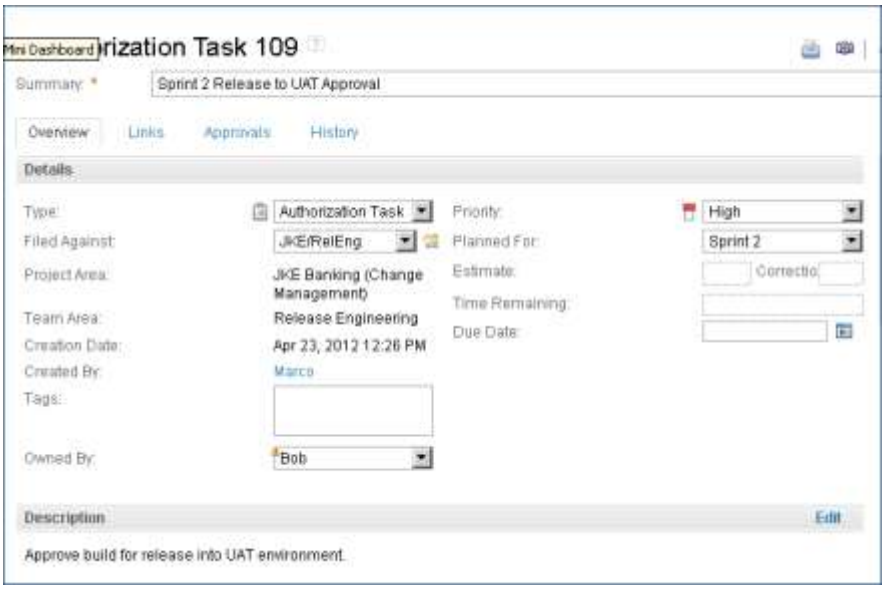
Prepare the multi-level work authorization

We first prepare the build’s work authorization by locating current work items used to track builds.



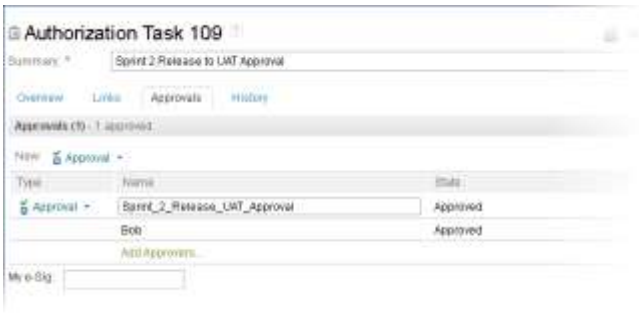
We then select and review *Track Build for Sprint 2* work item – noting the approvals on the Approvals tab are not e-signature approvals (which are required for audit purposes).

We then create a new work **Authorization Task** to capture authorization for the build to be released into the UAT environment:



We link this new authorization task to the existing *Track Build for Sprint 2* - -making it a **Child** work item of this Work Authorization task

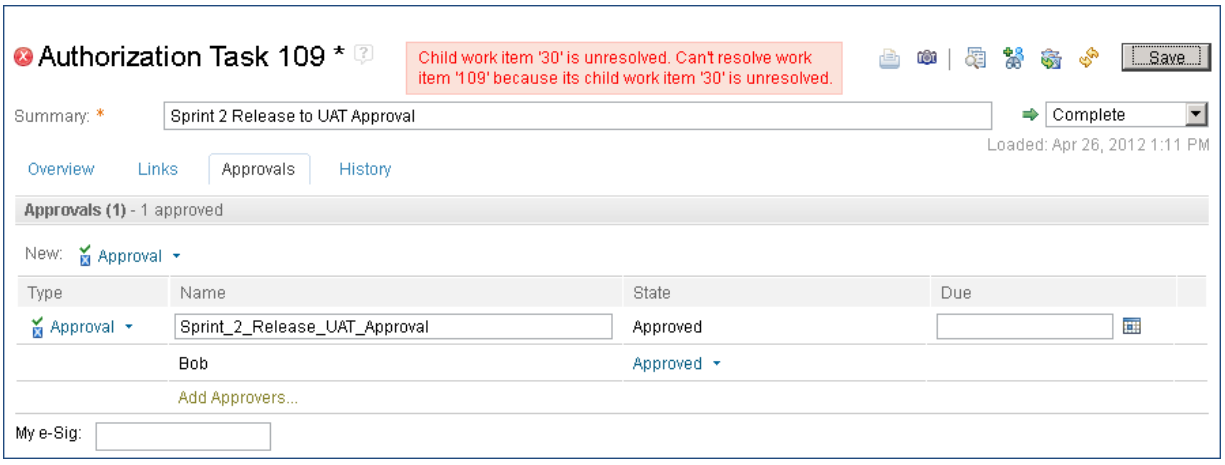
and also add an approver (Bob) and then save the new Authorization Task.



Authorize the work.

The build can now be authorized by the approver *after the child Track Build work item has been completed* by setting the new Authorization Task's approval state to **Approved** and the state of the Work Authorization to **Complete**. RTC prevents the authorization from happening until (all) linked child work items are complete.

This following shows how RTC uses the parent-child dependency between approval and authorization records to help enforce a multi-level authorization and approvals.



Summary

This article has detailed several options for work review, approval and formal authorization. Some regulations like Sarbanes Oxley, require you to implement internal controls that prevent unauthorized

changes to systems that are material to the business. Others that impact software development, like the FDA CFR 21, part 11 require electronic signature. Depending on the nature of your business, a specific project and the internal controls established by your compliance organization, you must determine the appropriate reviews, approvals and authorization formality required.