Policy assessments

By creating and comparing policy assessments, you can integrate your IDERA SQL Secure policies into your existing audit process. The recommended assessment workflow is:

1. Save as draft.
2. Publish assessment.
3. Approve assessment.

Use saved assessments in an existing audit process

Your Audit Process Step	Corresponding Assessment Step
Prepare for upcoming audit.	Create a draft assessment from an existing policy or previously approved assessment.
Set up the security requirements requested by the auditors.	Update the draft assessments to address the audit requirements. You can change the security check settings, choose different audit data, and add or remove SQL Server Instances.
Get your security status and findings.	Run the draft assessment using audit data from a specific point in time.
Identify differences from last time this audit was performed.	Compare the draft assessment to a previously approved assessment.
Distribute the assessment findings to an internal team to investigate any new violations or discrepancies.	Publish the assessment and distribute to the team. To distribute the assessment, run the Risk Assessment report, and then print or save the results.
Confirm that violations were fixed.	Take a new snapshot and then run the published assessment using your new audit data.
Document any discrepancies as known issues.	Add an explanation note for each security check finding that is a known issue.
Give assessment to auditors.	Run the Risk Assessment report, and then print or save the results.
Apply feedback from auditors.	Update the published assessment to address the auditors' feedback. You can change the security check settings, add or remove explanation notes, and change which instances are being audited.
Obtain "sign-off".	Approve the assessment.