Workzone Compliance

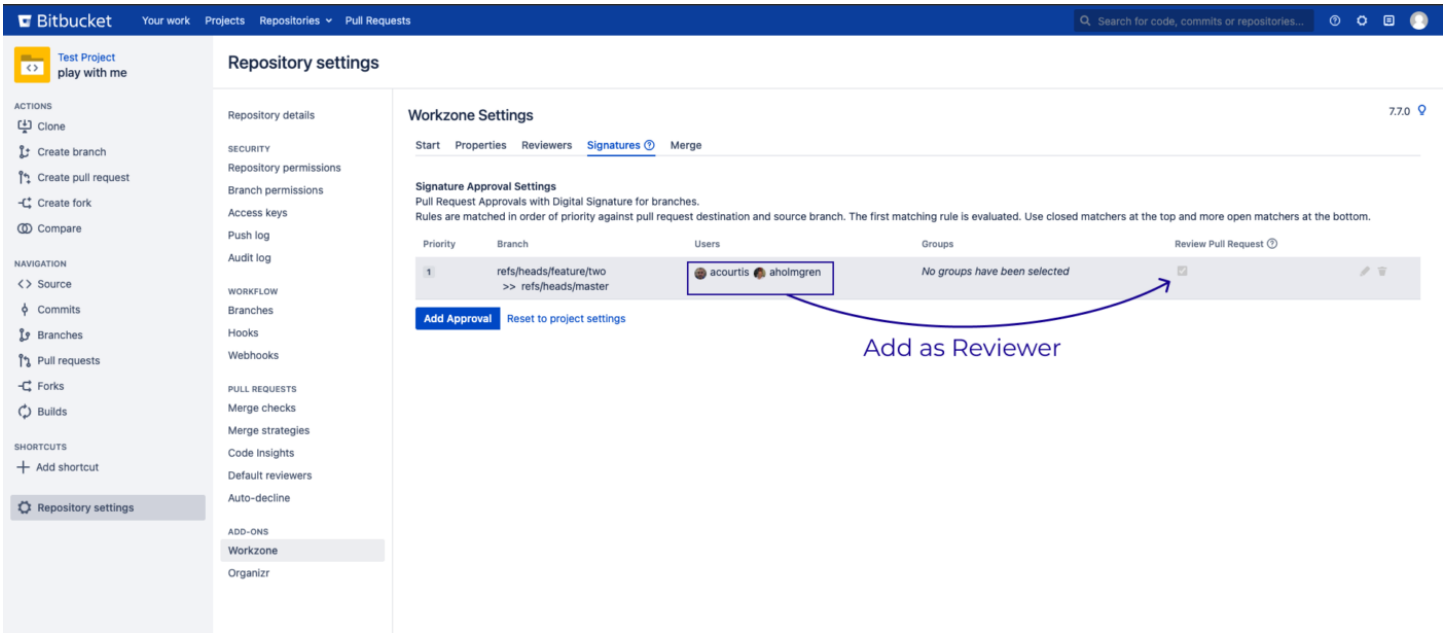
Feature Guide Workzone · https://izymes.com/docs/workzone-workzone-compliance/

How to enforce compliance with digital signatures

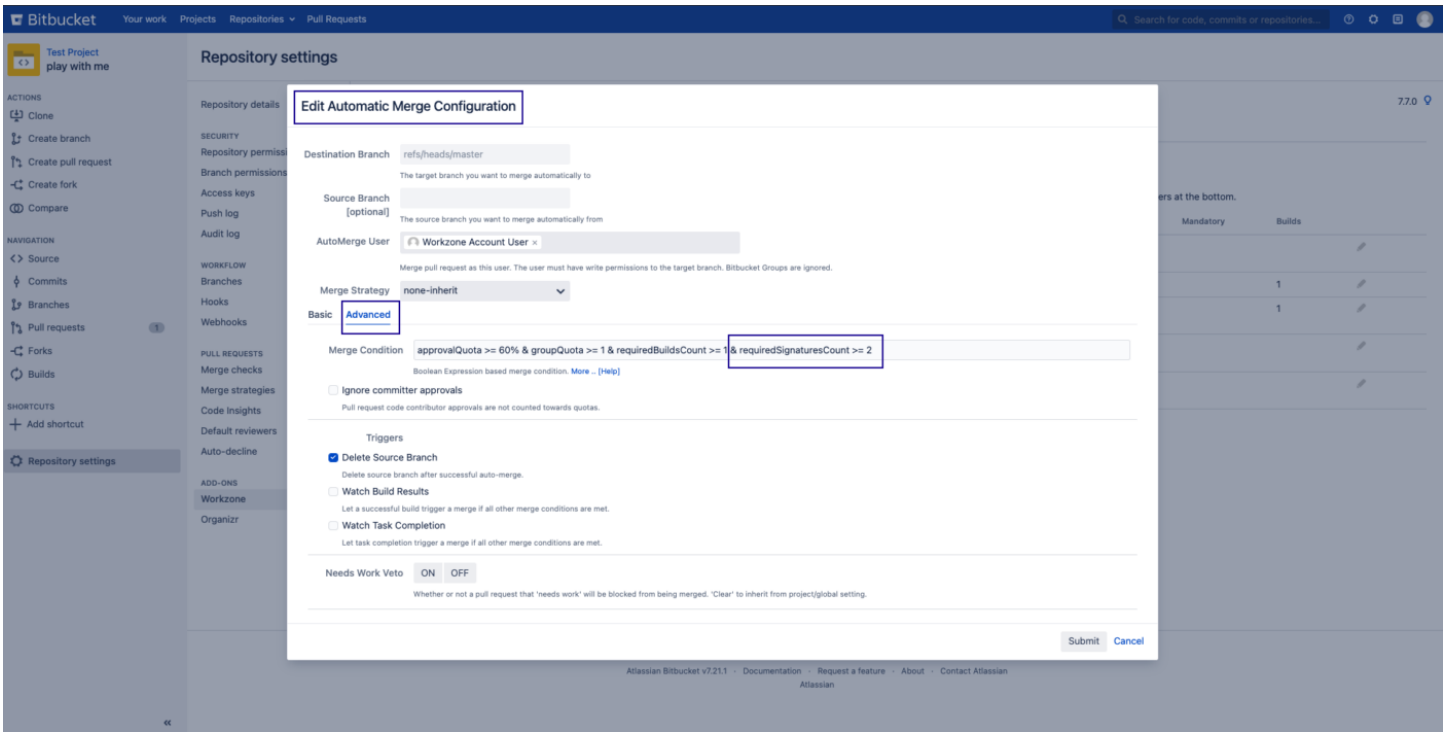
Merging pull requests in Bitbucket is comparable to merging documents. Just as documents can be signed for approval, Workzone lets you **digitally sign** pull request approvals using a username and password.

You can even set the configuration to only allow a merge to take place if a required amount of approval signatures are present.

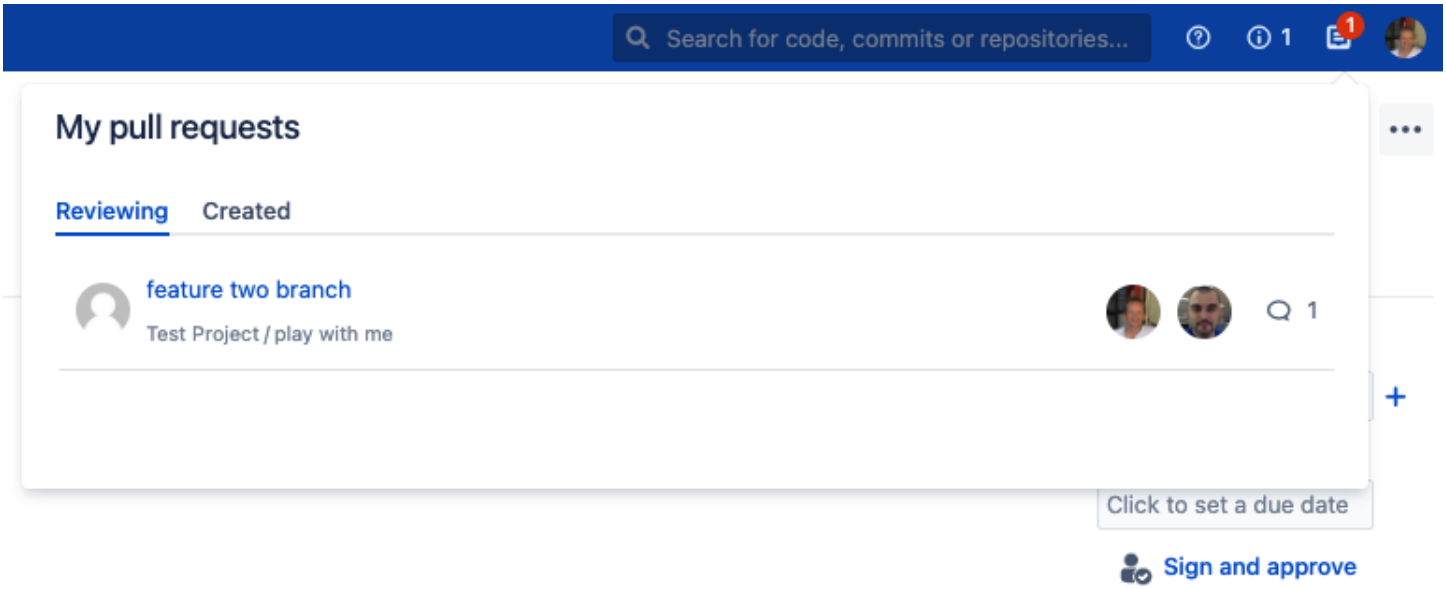
Let’s say Acourtis and Aholmgren release managers at ACME. ACME is a CFR compliant / ISO 900x certified company. In order to merge code for their new intensive care unit device update they need to digitally sign off changes.



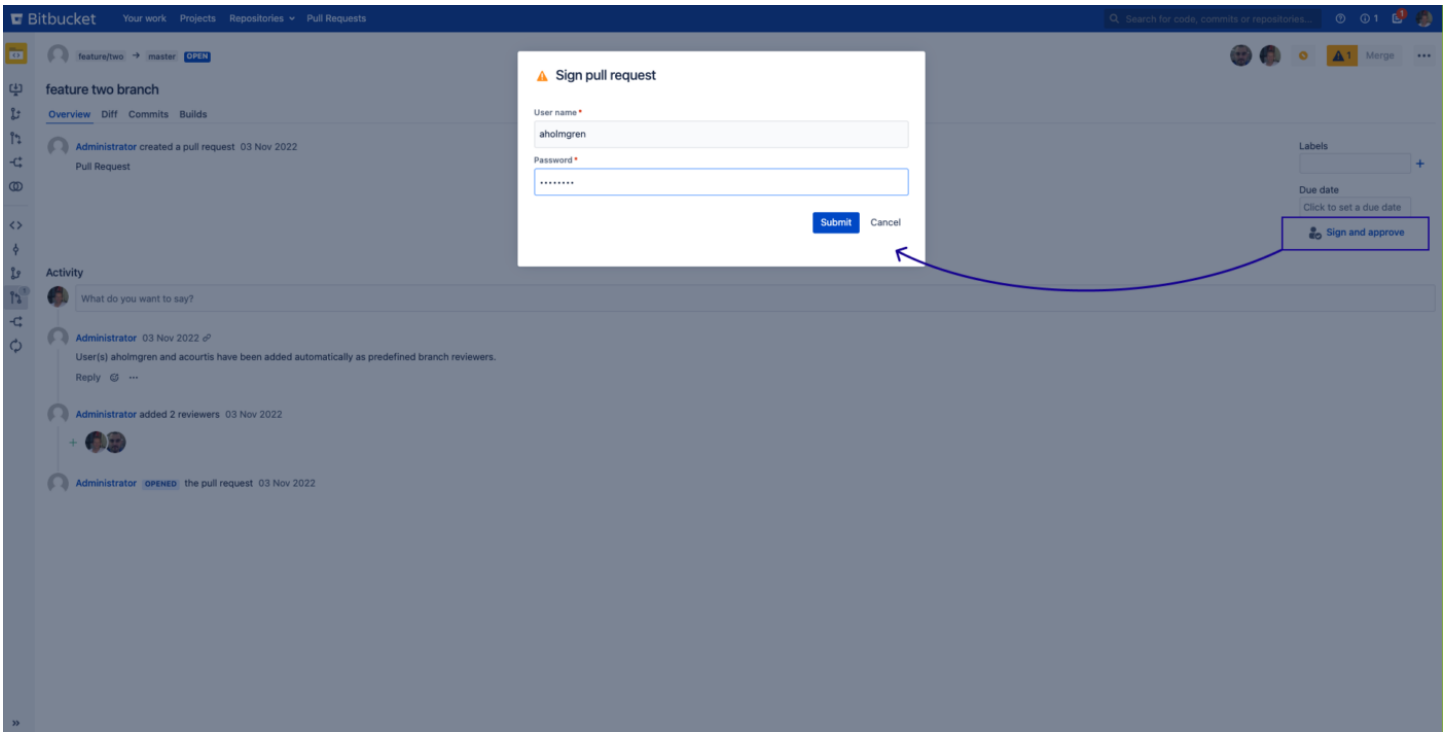
ACME’s CFR policies enforce 2 digital signatures before the code can be merged. Workzone’s auto-merge configuration is set up to require 2 signatures.



Acourtis and Aholmgren are notified of the pending Pull Request that requires their signature.

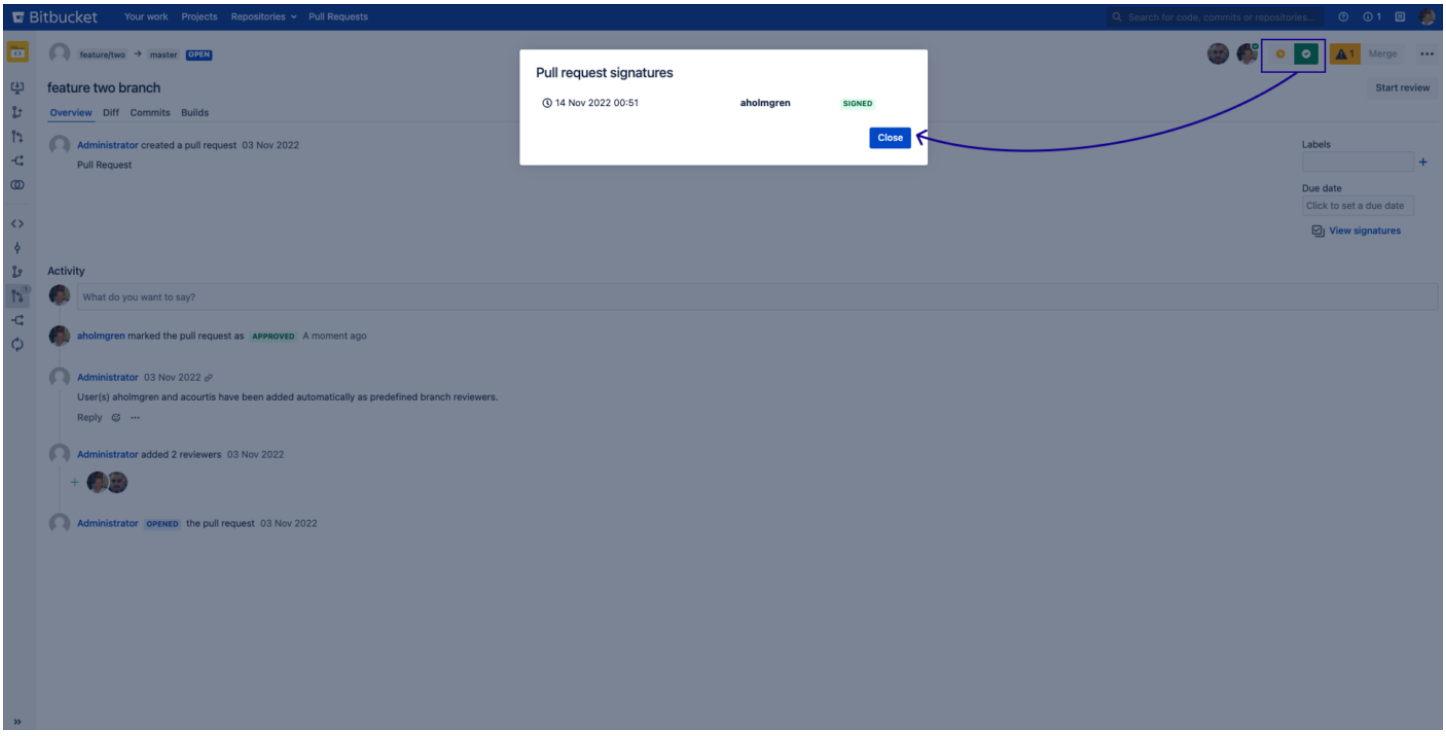


When Acourtis and Aholmgren approve the PR, they need to enter their username and password to digitally sign their approvals.



Once Acourtis and Aholmgren have digitally signed the Pull Request is automatically merged or merge restrictions are lifted if the Pull Request is merged manually.

The merged Pull Request Overview shows the signature trail.



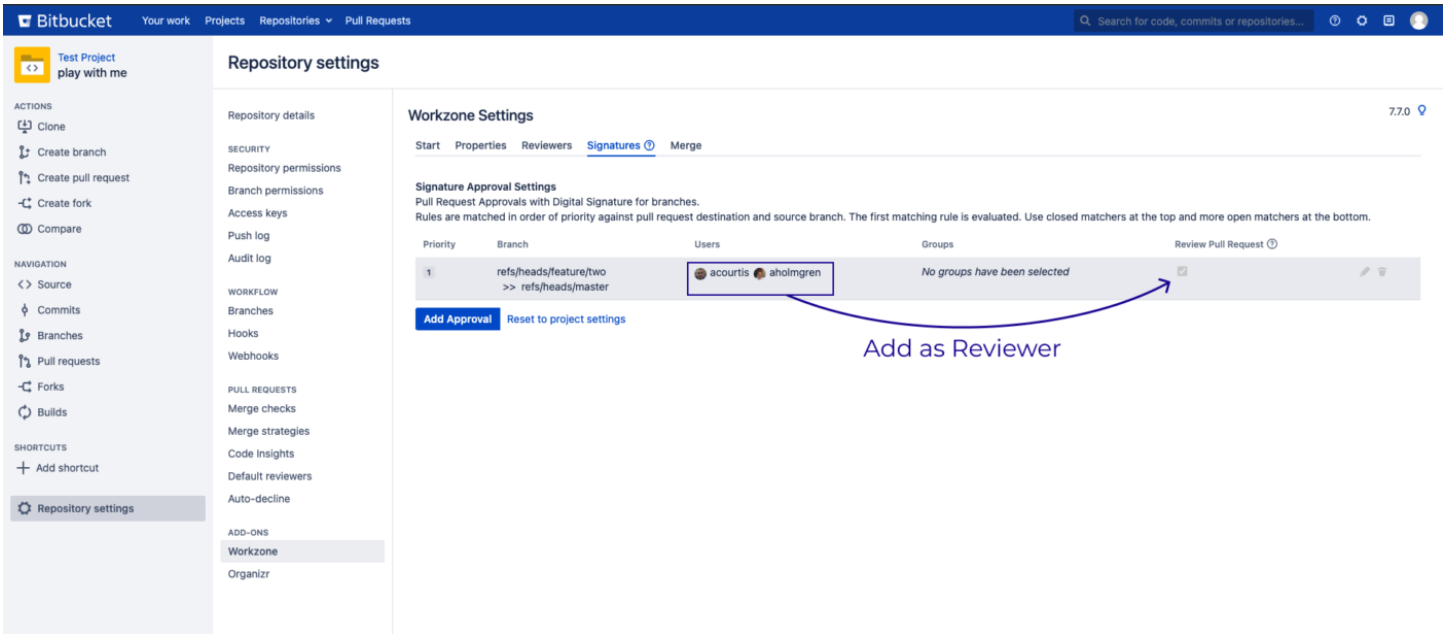
ACME, Regulatory bodies and agencies can now track each digitally signed Pull Request as signed approvals are stored in Bitbucket's database. Workzone Digitally Signed Pull Request Approvals

makes your Bitbucket Server instance CFR Part 11 compliant.

Approvers Configuration

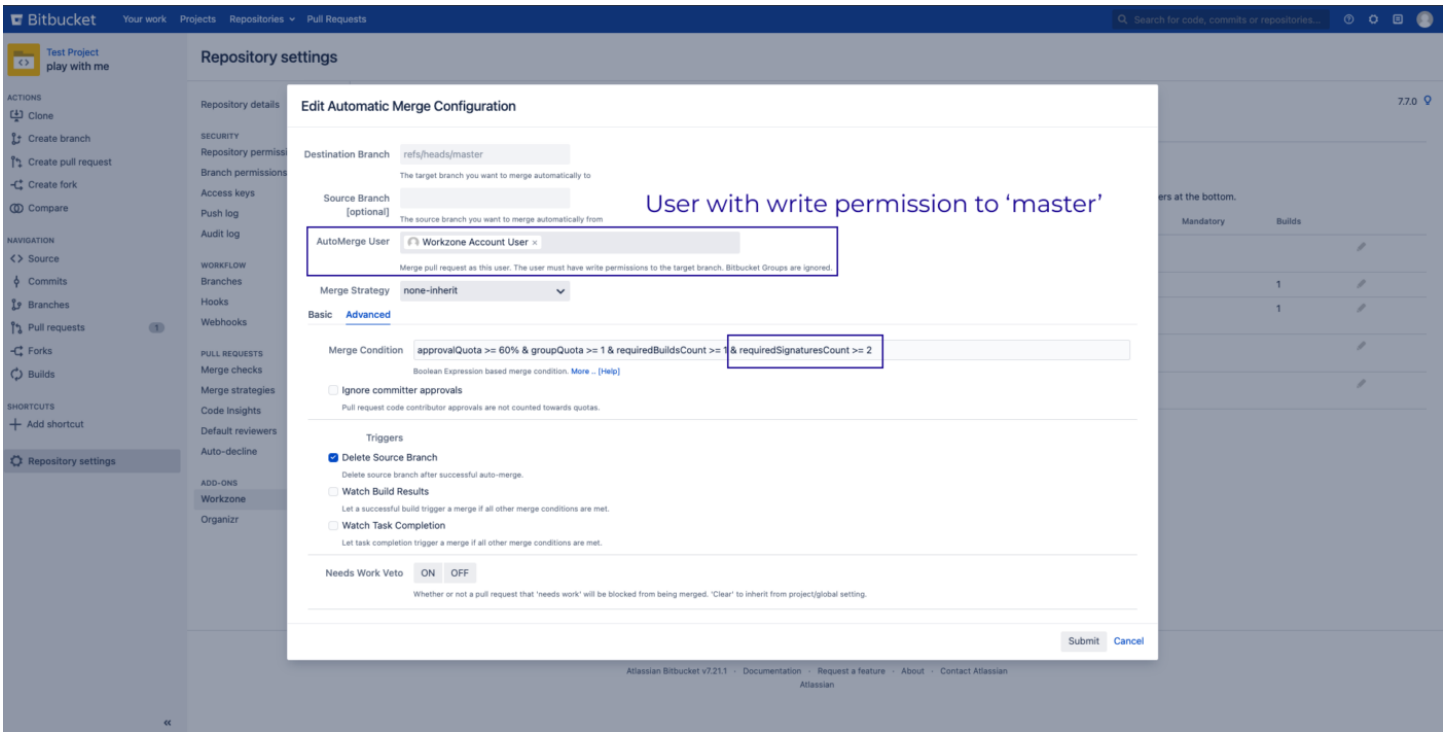
Configuring digitally signed approvals follows the same pattern as with ‘normal’ reviewers.

Define a target (and optionally a source) branch (pattern) and add approvers as users or groups. It is best practice to let Workzone add them as pull request reviewers as well so approvers get notified.



Merge Configuration

To enforce digitally signed pull request approvals a *requiredSignaturesCount* parameter can be configured in the (auto) merge configuration. Together with write restrictions to the pull request’s target branch and/or globally enforced Workzone merge conditions pull requests can now only be merged when the *requiredSignaturesCount* condition is met by reviewers approving a pull request with their digital signature.



Types of Compliance



FDA Title 21 CFR Part 11 compliance.

Ensure CFR Part 11 certification compliance for your software change management process

- Digitally sign pull requests with e-signature

- Enforcement, validation, audit trail, and secure record retention: Prevent merging pull requests without signature, signature audit trail reports for compliance.
- Smart approver/signer selection: nominate individuals or groups to sign off on pull requests.



FDA Title 21 CFR Part 11 compliance.

Ensure ISO/IEC 27001 / ISO 900x certification compliance for your software change management process

- Digitally sign pull requests with e-signature
- Enforcement, validation, audit trail, and secure record retention: Prevent merging pull requests without signature, signature audit trail reports for compliance.
- Smart approver/signer selection: nominate individuals or groups to sign off on pull requests.



Validate data security standards and operations, SOC 1 and SOC 2

Code Review for SOC 2 Compliance

Protect your applications and customers by implementing a custom change management process that works the way you want it to.

- Secure Your Codebase: Provide guardrails with automated code review assignment and requirements.

- Native Integration: Built around Git and Bitbucket, employees can review code with built-in tools and leave an audit trail.
- Smart reviewer selection: Use targeted reviews to notify only relevant reviewers when a PR is ready for them.



Code Review for SOX Compliance

For public companies and those preparing to IPO, Workzone can help implement internal SDLC controls to meet the requirements of Sarbanes-Oxley Act of 2002, Section 404.

- Custom Workflows: Address Section 404 with specific Workzone workflow rules and requirements for change management.
- Native Integration: Built around Git and Bitbucket, employees can review code with built-in tools and leave an audit trail.
- Secure your codebase: Enforce pull request merge controls by limiting permission to merge to a system-account.



Code Review for PCI Compliance

Satisfy PCI DSS requirement 6.3.2 by implementing a code review policy that protects your codebase and your customers.

- Automate Assignment: Write the rules for who should review and when, and Workzone will automate it.
- Improve Your Codebase: Use precise reviewer selection to add context to the change and improve code over time.
- Native Integration: Built around Git and Bitbucket, employees can review code with built-in tools and leave an audit trail.



Code Review for OWASP Top 10

Develop secure applications by implementing a human code review process to catch the most common security mistakes.

- Automate Assignment: Write the rules for who should review and when, and Workzone will automate it.
- Improve Your Codebase: Use precise reviewer selection to add context to the change and improve code over time.
- Native Integration: Built around Git and Bitbucket, employees can review code with built-in tools and leave an audit trail.



SAFe Transformation

Use dynamic project or repository reviewer groups for implementing Agile, Lean, and DevOps practices at scale.

Try Workzone!