ATLASSIAN

How Atlassian ensures governance and compliance

A quick guide from our executive team to yours

GEORGE TOTEV
Head of Risk and Compliance

GUY HERBERT
Risk and Compliance Manager

BILL MARRIOTT
Trust and Security Manager

As your enterprise grows, your security, governance, and compliance protocols have to grow with it. If not, you can find yourself caught in legal matters, subject to a significant data breach, or even worse, you can threaten your brand's integrity and your customers' trust.

So what's the best way to achieve top-notch enterprise security, governance, and compliance? For starters, the tools you use and the systems you have in place are critical to success. We sat down with Atlassian's security leadership team to gain insight into how we've scaled our security and compliance practices, and it boiled down to three major themes.

1. Change and release management - *2 steps to success*

In the words of George Totev, Atlassian's Head of Risk and Compliance, "As the scale and complexity of your environment grows, so does the impact of incorrect changes."

If you have a large enterprise with integrated systems and workstreams, complexity becomes one of your biggest risk drivers, especially if you're in a highly regulated industry. Agile methodologies, which essentially break down large changes into small iterative changes, can help reduce that risk. However, in today's highly connected world, even a small change can wreak havoc at scale, especially in more complex environments.

With the increased need to streamline work and reduce risk, it's no secret there's a need for a more modern and secure approach to change and release management. Because there are so many stages throughout release management, such as initiation, requirement gathering, development, test, and production, there's more vulnerability to error. Traditionally, each of these stages would need sign-off in order to move to the next. And at the end of the full cycle, a change approval board (who may not even fully understand the context of the build), would need to sign off on the code change before it goes out to customers in production. In today's agile organization, this outdated, error-prone process doesn't work in today's world.

The key is balancing the risk of change, with the risk of avoiding or slowing down those changes. Fine-tune that balance of quality with agility!

At Atlassian, we've developed a modern approach to get our code changes to production as fast as possible. It consists of 2 simple steps.

1. Peer review
With a peer review, developers have context and understand the code and the changes to the code, along with its implications.

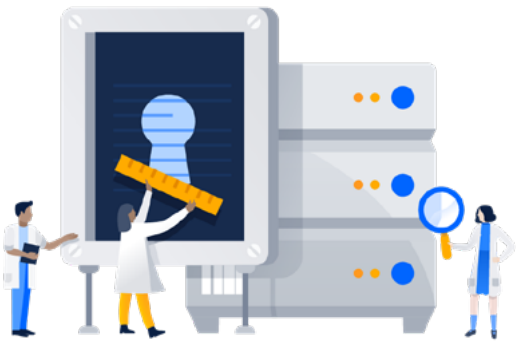
2. Build testing
Automate your testing and maintain your build tests - have the test run every time you build a commit to ensure your changes work accurately.

Having these 2 controls in place allows for faster change, iteration, flexibility, and improvement. Ultimately, it provides higher quality so you can better serve your customers.

To use these 2 steps effectively as a compliance control, you'll need a way to guarantee the build received a proper review. That's why we "system-enforced it," by baking these two requirements into our change and release management workflow within our products. Within the build itself, the system requires peer review first before pushing the branch to master, and then the build test has to successfully pass before going into production. Within the production environment they're looking for those two requirements to be met before it even accepts the change.

BONUS This also makes it easier from a compliance perspective when your auditors are manually looking through a lengthy series of individual changes. Now, they can look at the system settings and see that these changes met the 2 requirements.

In the end, auditors can approve faster, and your devs get to spend more time on meaningful work. Win-win.



2. Reducing risk with the right tools in place

Gone are the days when risk, compliance, and just about every other process for that matter, were managed in Microsoft Excel and Word. A few years ago when we were deciding on what risk management tools to use ourselves, we actually considered many external options at first, but then we looked in house, and adopted Jira and Confluence to manage our risk and compliance processes.

We use Confluence to capture our compliance policies, and Jira to capture the lifecycle of these policies. This shows us the various stages within these workflows, such as when policies are designed, approved, implemented, or signed. These two tools together make an effective document management and workflow system.

Within Jira, we create different tickets for each compliance object type, including controls or remediations, so that we can track the connection between those tickets and follow them end-to-end. This enables us to readily evaluate different standards, along with the controls, activities, and remediations that are connected to them.

Because so much of our work at Atlassian already runs in these tools, all the work associated with the compliance standard is run by the business teams. Therefore, when we have a remediation, we link it to the associated Jira ticket as part of the backlog for that particular business unit. Many of our teams end up working on compliance themes without even realizing it!

The security team uses Jira to track our security instances and investigations from start to finish. We begin with an investigation, determine it's severity, move it into an indecent if needed, and track it to completion. To add to that, we've also written a whole series of alerts to do our detections in Splunk, which we maintain inside of Bitbucket as our code repository and hosting platform. This allows us to connect our detections to our work throughout Bitbucket, Jira, and Confluence.

The product security team also uses Jira to translate findings and vulnerabilities from our vulnerability assessment platform, Nessus. These vulnerabilities become Jira tickets that we can allocate out to our teams to resolve.

BONUS By using your existing infrastructure and tools, you can save time and resources by not needing to set anything new up to manage risk and compliance processes.

3. Policy management scaled across the org, build for the future

To set up our policy management program, we document our policies and standards in Confluence across all legal, privacy, people, and technology domains. Within Confluence, you can readily view the page history at any given time. You can also enable alerting functionalities when there's a document change, or someone comments on the page with a question, which is extremely helpful as you grow. For example, within our technology domain alone, we have over 85 policies and standards documented in Confluence that need to be maintained. We then use Jira to track the policy review and completion of that review each year.

PRO TIP Create templates in Confluence for your policies so they all have the same layout and functionality, then link the the associated Jira project at the bottom of the Confluence document so you can easily reference both.

Within Jira, we suggest creating a ticket for each policy standard such as HIPPA, GDPR, and SOC2, so you can map all activities tied to these larger objectives. With the visibility Jira provides, you can always determine what the policy is, who the owner is, and what the standard is.

From there, we create and monitor all the associated subtasks to completion. You can use JQL (Jira Query Language) to filter down and show active policies, exceptions to policies, violations to policies - which we can then link to incident management tools. Having a Jira filter that shows all of those details readily available really helps when external auditors come around.

All these are housed in a master ticket which is the policy review program. So now, when your annual policy review cycle is up, just set up a subtask within each policy ticket to make sure each document gets reviewed each year. You can then easily scale these processes and systems across the org to ensure other teams use it to stay compliant too.

At Atlassian, many other teams have adopted these systems to manage their own policies and operations. The legal department uses Jira to manage their contracts and track the lifecycle of legal documents through stages of negotiation, review, and approval. This means you can look back 4-5 years to access important history and use analytics to see key information such as the last review date and track changes to important contracts. The procurement team uses Jira to manage their suppliers, their onboarding, and all the and actions associated with the account, with access to deep analytics to optimize our supplier portfolio. The human resources team uses Jira to track certain initiatives to completion by creating a specific Jira, such as employees needing to sign our annual code of conduct each year.

With these integrated systems working across the company, we were able to establish our entire business process model within Jira, not just our project management, and efficiently plan for change and scale. To build for the future, you have to start today, and having the right tools, team, and governance in place allows for efficiency as you evolve over time.

Additional resources

Atlassian Trust Center

Server vs. Data Center: what's right for you?

Support for OpenID Connect in Data Center

Self protection capabilities in Data Center blog

Advanced auditing for Data Center blog

2 minutes to upgrade using your same Server hardware blog

Data Center on AWS Quick Starts

The complete guide to enterprise user management

Want to dive deeper into security governance and compliance at Atlassian?

Watch the webinar series