ATLASSIAN

To Protect and Serve

Atlassian Cloud Security Approach and Practices

Most challenges – large and small – are solved not by individuals, but by teams. So it's been our mission to unleash the full potential of every team, across organizations of all sorts throughout the world. In recent years, we've witnessed the growth of one of the most significant tools for team collaboration ever developed: the Cloud. And we've embraced it wholeheartedly. Our cloud products enable teams to collaborate and innovate more effectively, scale quickly, and focus more time and energy on their core mission.

The cornerstone of our cloud applications and services is security – our mission depends on it. So we're committed to ensuring the unfaltering safety and security of your company's data and to providing you with the information you need to understand and evaluate our security practices and policies for yourself.

This white paper outlines how the Atlassian team keeps our cloud systems secure, the many steps we take to build security into our products, and the role your organization plays in keeping your work environment secure. Our aim is to help your team take full advantage of all that Atlassian cloud services have to offer with the confidence that your organization's security is ensured.

It starts with trust

In cloud services, trust begins with security–but it doesn't end there. It also includes reliability, privacy, and compliance with industry standards and legal regulations. So, to fully earn your trust, our team is committed to these four principles:

Security

We follow extensive administrative, operational, and configuration practices to track and protect your information through a comprehensive set of security controls and practices. Our dedicated security team continuously improves our development, security operations, and threat-mitigation practices to detect and prevent new security threats, so you can rest assured that your data is safeguarded.

Reliability

Organizations run mission-critical projects and operations on Atlassian products – that's why we are committed to delivering products, applications, and networks that are stable and secure at scale. Our products are built on best-in-class core technologies and our business continuity, disaster recovery, and data backup programs ensure the impact on our customers is minimized in the event of a disruption to our operations.

Privacy

Your data is our responsibility, and we're committed to protecting it from unauthorized access and supporting your organization in meeting data privacy obligations around the world. We provide information and governance controls to help you make the right decisions for your organization. Additionally, we've invested heavily in GDPR, Privacy Shield, and stringent privacy safeguards to keep your data private and in your control.

Compliance

We encourage you to inspect and verify our security and privacy practices and operations. Our products regularly undergo independent third-party audits and certifications against global standards such as SOC2, ISO 27001, ISO 27018, and PCI DSS. Additionally, our service providers undergo regular SOC1, SOC2 and/or ISO/IEC 27001 audits to verify their practices.

Below you'll find our approach and practices regarding each of these four essential principles of trust.

Security

Building security into all our products

Security isn't a destination–we see it as an ongoing, never-ending journey. We continuously strive to improve our software development and internal operations to identify, prevent, and preempt any vulnerability or threat on your behalf. We also strive to make security as simple as possible for our users, which is why we build security into the fabric of our products and infrastructure.

Security in Development

Atlassian develops software using agile development processes, and we apply the same approach to security. Just as this enables us to rapidly develop and update our software to meet customers' evolving needs, it also allows us to quickly target and fix newly discovered security vulnerabilities within strictly enforced time frames.

We believe that this agile approach to software development and security is far more effective than a traditional Software Development Life Cycle (SDLC)-based approach that checks for security only at specified development milestones or just prior to new releases.

Our agile development processes also include anticipating potential security risks and building in rigorous safeguards right from the start. So security is never an afterthought, subject only to a post-development review process. Instead, it's tightly integrated into the way we plan, build, and approve every single feature of each one of our products.

We diligently monitor each of our cloud services–across all development, staging, and production environments–so we can immediately notify our developers of any security issues. This allows us to fix most problems before the affected software is ever deployed to customers, or–in the few cases when we don't–very shortly afterwards.

We also guard against common web application attacks (XSS, SQL injection, CSRF, etc.), although not all controls are compatible with all products.

Product Security

One of the biggest challenges of software development is shipping secure products while maintaining speed to market. We constantly strive to achieve the right balance between hitting our release dates and ensuring security–after all, our own company runs on the same software we build for our customers. These are some of the most important security controls we implement to keep our products–and your data–safe.

ENCRYPTION-IN-TRANSIT

All data sent between our customers and our applications is encrypted in transit. We use Transport Layer Security (TLS) 1.2+ with Perfect Forward Secrecy (PFS) to protect data from unauthorized disclosure or modification. Our implementation of TLS enforces the use of strong ciphers and key-lengths, where supported by the browser. Find more details at our Security Practices page.

PRODUCT VULNERABILITY AND QUALITY MANAGEMENT

We take innovative approaches to building quality software. Stepping outside the traditional realm of Quality Assurance (QA), we instead follow the principles of Quality Assistance (see box). This approach allows us to introduce new features quickly and safely. We foster a more inclusive "whole team" mentality to quality, and we actively work to educate and empower developers to review their own features to ensure they meet our quality standards. Our security bug fix Service Level Agreement (SLA) defines the following time frames for fixing security issues in our products:

- Critical severity bugs (CVSS v2 score >= 8, CVSS v3 score >= 9) to be fixed in product within 4 weeks of being reported
- High severity bugs (CVSS v2 score >= 6, CVSS v3 score >= 7) to be fixed in product within 6 weeks of being reported
- Medium severity bugs (CVSS v2 score >= 3, CVSS v3 score >= 4) to be fixed in product within 8 weeks of being reported
- Find more details at our Security Bug Fix Policy page

PRODUCT SECURITY TESTING

We use both internal and external testing to track down, prevent, and patch product vulnerabilities. We utilize industry-leading vulnerability scanners, container scanning software, and static code scanners to identify security bugs and vulnerabilities in our Services and Products. One of our external programs–our bug bounty–helps us find and correct any errors in our software by incentivizing a large crowd of competing "good-guy" bug hunters and hackers. These programs yield the additional benefit of increasing the cost to the "bad guys" (in terms of time and resources) of finding and exploiting original vulnerabilities, making such malign ventures far less attractive. Learn more at our Security Practices page.

Penetration Testing

We use specialized security consulting firms to conduct targeted penetration tests on high-risk products and infrastructure. Such tests generally include:

WHITE BOX

Testers are provided with design documentation and briefings from our product engineers to support their thorough evaluations.

CODE-ASSISTED

Testers are given full access to the relevant code base to help discover and diagnose any unexpected system behavior and to identify potential targets.

THREAT-BASED

Testing focuses on a particular threat

scenario, such as a compromised instance, and testing lateral movement from that starting point. To ensure intensive and exhaustive testing of our products, we provide our testers with extensive access to our proprietary information and assets. When possible, we make these reports available for customers. We also publish quarterly reports from our Bug Bounty on our External Security Testing page.

Physical Infrastructure Security

We limit physical access to our data centers where customer data is hosted to authorized personnel only using biometric measures for verification. Additional defenses include on-premise security guards, closed-circuit video monitoring, man traps–and more. We rely on our data center hosting partners (AWS, NTT) to manage the physical and environmental security concerns of our data centers.

Network security

Atlassian implements controls at each layer of the stack, dividing our infrastructure by zones, environments, and services. We control access to our sensitive networks through the use of virtual private cloud (VPC) routing, firewall rules, and software defined networking. All connectivity is encrypted by default.

Staff remote connectivity requires device certificates, multi-factor authentication, and use of proxies for sensitive network access. We also deploy advanced intrusion detection and prevention systems in our office networks to identify potential security issues.

What's more–in keeping with our commitment to continuous improvement–our approach to secure access is shifting to a "Zero Trust" device-based system that goes beyond the traditional firewall-based "in vs. out" approach. Instead, Zero Trust denies or permits access based on whether a specific device (a laptop, phone, etc.) has been, and is currently, authorized–regardless of its "within the firewall" vs. "outside the firewall" status. This approach enables both tighter security in general and simpler access for authorized users.

How we use our own stack

Our customers often ask us what applications we use in our own stack, especially as it pertains to responding to security incidents. We use a mix of our own products along with a few other best-of-breed tools. Sharing information across the organization–and with partners and customers–is a top priority, so, naturally, we make sure our stack is harmonized for this purpose. Here's how our own products work in our stack:

COMPREHENSIVE DETECTION AND ANALYSIS

We use Splunk, a big data analytics platform, to query our logs, events, and alerts and apply heuristic analysis and anomaly detection, based on policies established by our security intelligence team. These policies are based on both historical and theoretical incidents. Our Security Intelligence Team also performs frequent 'hunts' to determine if there are indicators of compromise in the environment. These 'hunts' are translated to alerts so we can be notified of future suspicious activity.

AGILE COMMUNICATIONS LOOP

We address problems that require quick and simple fixes immediately, and then log them. For more serious or complex issues, we first record incidents in Jira, then share them in Slack, to broadcast the information widely throughout the company.

CONNECTED CONVERSATIONS

Alerts that we receive from customers or partners via Jira Service Desk go to Opsgenie in order to notify the right people. These alerts are also sent to Jira, and then Slack, to ensure transparency and broad awareness.

KNOWLEDGE CAPTURE AND TRANSFER

Many of our playbooks are stored in Confluence, so if we need to use them as guides in response to an incident, we can reference them in the Jira ticket. Relevant email conversations are also logged in Jira. And whenever an incident is updated in Jira, that information is also communicated through Slack. We've set up our tools and processes to make it easy for people to provide input via whichever tool makes the most sense for them. That way, information and communications are always widely disseminated and never siloed.

People

Any comprehensive discussion of security must reckon with the central role people play in the development and maintenance of products and systems. After all, trusting any organization begins with trusting its people.

So, at Atlassian, we invest in experts, processes, and practices to ensure that we safeguard your business and customer data around the clock. This begins with hiring the very best talent available–whether they're employees or contractors. Everyone working at and with Atlassian is required to sign a confidentiality agreement prior to starting with us, and subsequently–during the on-boarding process–we provide security awareness courses to all new talent.

New-hire and ongoing training and awareness

Our security and awareness program is built on the premise that security is every employee's responsibility–not just of those in our security team. These responsibilities are grounded in our internal Security Policy Program, and our training and awareness program effectively communicates these responsibilities to our entire workforce.

And this program doesn't just check compliance boxes. We've developed a comprehensive curriculum that helps raise awareness of the most hazardous security mistakes and vulnerabilities with the goal of driving widespread adoption of security best practices.

In keeping with our principle of continuous improvement, we regularly spread the word about relevant security issues, like newly-discovered and publicized threats, through company-wide email messages and blog posts. These updates cultivate an environment of sustained awareness and vigilance, reinforcing the importance of always following security best practices.

Security champions

Like many organizations, Atlassian is brimming with bright and talented people. And not all of these bright, talented people work in our security team. So, we actively reach out to people from all across the company for innovative ideas about enhancing security.

One of the ways we do that is through our Security Champions program. A major goal of this program is to embed security into each and every team at Atlassian–to further "build security in." Another goal is to demystify security issues by providing people across the organization with core security training, enabling them to knowledgeably consider and anticipate a wide spectrum of security threats–and then devise creative defenses. This program is about taking subject matter experts with a passion and aptitude for security and drafting them into the team on a part-time basis and to be our advocates in the rest of the company

Red team

The Atlassian Red Team focuses on full-scope adversarial emulation. We employ our Red Team to hack our own systems, just as if we were targeted by a malicious entity.

The Red Team acts like the attackers that are most likely to target the company and does their best to infiltrate and compromise critical systems. If they succeed, they notify everyone involved and work together to implement long-term solutions to the security vulnerabilities and gaps that were discovered.

The goals of the Red Team are to:

- Measure and improve the effectiveness of the security intelligence function by evading detection
- Create positive change in Atlassian security posture and capabilities
- Increase understanding of our vulnerability and ability to respond to real-world attacks

Compliance

We adhere to widely accepted compliance standards and regulations. Our Service Organization Control (SOC) Reports–which are certified by third parties–describe how we comply with common controls and objectives. These reports detail for you and your auditors how the controls we've established support operations and compliance at Atlassian.

Common controls framework

It's easier to build security into all your products and processes when you have a set of standardized tools to work with. Atlassian's products–like those of many industries–are guided by several international control standards for product development and operations.

Like any skilled artisan or builder, we carefully consider the range of tools (control standards) available to us, then precisely select and utilize the ones we think are best-suited to realizing our goals and our vision.

You can find a detailed list of the standards we apply–and how and where we apply them–in our Atlassian Common Controls Framework. This helps us show how we meet the requirements of many of our customers across many different industries.

Compliance tracking and policy development system

We've also built our own unique system for managing controls compliance and policy development – with Atlassian's own products. Using Confluence for documents and Jira for work flow mapping and tracking, we created an extremely powerful compliance management tool that's very tightly integrated. And, as an added benefit, it costs us and our customers nothing – because the only tools needed are Jira and Confluence.

External compliance and certifications

SOC2

Atlassian's Service Organization Control (SOC) Reports are certified by a third party and demonstrate how Atlassian achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the controls established to support operations and compliance at Atlassian.

Atlassian has achieved SOC2 certifications for:

- Bitbucket Cloud (Type II)
- Confluence Cloud (Type II)
- Jira Cloud (Type II)
- Trello (Type I)

> A copy of the SOC2 report for Jira, Confluence, Bitbucket, and Trello Cloud is available here.
>
> A copy of the SOC3 report for Jira and Confluence Cloud is available here.
>
> A copy of the SOC3 report for Bitbucket Cloud is available here.

ISO27001/ISO27002 and ISO27018

ISO/IEC 27001 is recognized as the premier information security management system (ISMS) standard worldwide. ISO/IEC 27001 also leverages the comprehensive security controls detailed in ISO/IEC 27002. The basis of this certification is the development and implementation of a rigorous security management program, including the development and implementation of an Information Security Management System (ISMS). This widely-recognized and widely-respected international security standard specifies that companies that attain certification also:

- Systematically evaluate our information security risks, taking into account the impact of security threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls to address security risks
- Implement an overarching audit and compliance management process to ensure that the controls meet our needs on an ongoing basis

The scope is Atlassian Cloud offerings Jira Cloud, Confluence Cloud, and Bitbucket Cloud–including the micro services used to deliver these applications. Also, Corporate functions including Legal, Talent, Policy, Privacy, Procurement, Risk & Compliance, Security, Workplace Experience and Workplace Technology teams.

View the Atlassian ISO/IEC 27001 Certificate

PCI

We care about the security of your credit card and we despise fraudsters. When you pay with your credit card for Atlassian products or services you can rest assured that we handle the security of that transaction with appropriate attention. We are a Level 2 merchant and we engage with Qualified Security Assessor (QSA) to assess our compliance with PCI DSS. We are currently compliant with PCI DSS v3.2, SAQ A.

View or download our PCI Attestation of Compliance (AoC)

- Jira, Confluence, Bitbucket and LearnDot
- Trello
- Statuspage

Cloud Security Alliance

A CSA STAR Level 1 Questionnaire for Atlassian is available for download on the Cloud Security Alliance's STAR Registry web site.

The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping customers assess the security of cloud providers they currently use or are considering contracting with. Atlassian is a CSA STAR registrant and Corporate Member of the Cloud Security Alliance (CSA) has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). The latest version of the CAIQ, aligned to CSA's Cloud Controls Matrix (CCM) v.3.0.1, provides answer to over 300 questions a cloud customer or a cloud security auditor may wish to ask of a cloud provider.

Our Atlassian CIAQ entry covers our Jira and Confluence Cloud and Bitbucket Cloud offerings.

We will continue to evaluate other industry-recognized frameworks for certification in the future. For more information, and to download relevant certificates, see our Atlassian Compliance page.

Our Service Providers

We hold our service providers to very high standards. Data centers, co-location, and managed service providers undergo regular SOC1, SOC2 and/or ISO/IEC 27001 audits to verify their practices.

We review the results of these audits annually, at a minimum, as part of our vendor management program. In the event these audits find present risks to us or our customers, we work with the service provider involved to understand any potential impact to customer data and track their remediation efforts until the issue has been resolved.

Shared responsibility: We're on the same team

While there are many security benefits to cloud software, it's still critical to take steps to ensure the security of your cloud applications. As with most things that are mission-critical, security is a shared responsibility. There are a number of links in that chain of responsibility, and if any one of them is compromised, the whole chain is weakened.

As we've discussed, people are the foundation on which trust and security are built. We consider security everyone's responsibility, and we actively engage our entire workforce in that critical mission. But the people who develop, monitor, and maintain software are just part of the equation. After all, software is intended to be used, and how it's used plays a significant role in the security of the work it enables.

If someone creates a confidential document, then grants access (either intentionally or inadvertently) to unauthorized viewers, unfortunately, there's not much our team can do to prevent a security risk. So, there's another critical group of people who are essential to maintaining security: software users.

The granting of authorized access and specified permission levels are in the hands of our users–specifically, those with admin privileges. But this, of course, introduces new openings for abuse or errors that create security vulnerabilities. That's why the security of your data on our systems is a joint responsibility.

> This notion of shared responsibility in security management is addressed in greater detail in our white paper ***"The Atlassian Cloud Security Team (You're part of it) ."***

At a high level, Atlassian handles security of the applications themselves, the systems they run on, and the environments that host those systems. We ensure these systems and environments are compliant with well-known and relevant standards, including PCI DSS, ISO27001, CSA STAR, and SOC2, among others.

You–our customers–manage the information within your accounts, the users accessing them (and their related credentials), and the apps you install and trust. You ensure your organization is meeting its compliance obligations when using our systems.

In brief, there are a few key decisions we would like our customers to consider when setting up our products. These decisions have a significant influence on the way security is implemented:

All products: Domain verification and central management

You can verify one or multiple domains to prove that you or your organization owns those domains. Domain verification allows your organization to centrally manage all its employees' Atlassian accounts and apply authentication policies, including password requirements and SAML.

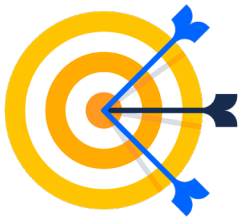
After verifying your domain, all users with existing Atlassian accounts under that domain will receive an email explaining that they are transitioning to a managed account. Anyone signing up to a new Atlassian account with that domain will see that they are getting a managed account.

Bitbucket: Public vs. private repositories

You designate whether the repositories are public, meaning that anyone on the internet can view those repositories; or private, meaning that access to those repositories will be limited to those who have permission to access them.

All products: Granting access

Our products are designed to enable collaboration–and collaboration requires access. But you do need to be careful about granting permissions to other users (and third-party apps) to access your data. Once you grant such permissions, we will not be able to prevent those users from taking the actions allowed under those permissions, even if you don't approve of those actions. So, carefully consider the permission level you grant each user, and be sure to change permissions, when necessary, in order to minimize risks.



Reliability

We recognize that for organizations that run mission critical-projects and operations on Atlassian, products like Jira and Confluence become indispensable to your daily operations.

For this reason, it is all the more important that your team has uniform reliability and uptime–and we can definitely relate. Our own business operations are heavily dependent on our cloud product suite, so we know first-hand how crucial product reliability and data recoverability are to our customers.

Platform-wide availability and redundancy

We utilize trusted cloud hosting partners to help us run Jira, Confluence, and Bitbucket. These data centers are designed and optimized to host applications with multiple levels of redundancy built in, and they run on a separate front-end hardware node on which application data is stored.

To ensure seamless continuity in the event of regional outages, we operate multiple geographically diverse data centers. We maintain multiple regions and availability zones across East and West regions of the U.S. as well as the European Union and APAC. Our platform optimizes where customer data is located based on origin of access, ensuring more reliable performance and reduced latency.

Uninterrupted availability of your data and services is our top priority. We devote immense effort and attention to product resiliency, by strictly applying standards and practices designed to minimize downtime. We implement controls at every point of the development life cycle using SOC2, ISO 27002 and ISO 22301 standards and practices. We also utilize industry-verified quality control processes, such as chaos engineering, staging environments, and internal dogfooding, enabling us to proactively identify issues.

Key principles guiding our Disaster Recovery (DR) Program include:

CONTINUAL IMPROVEMENT
We continually enhance resiliency by implementing new operational efficiencies, ever-increasing automation, the most up-to-date technologies, and the latest proven practices.

ASSURANCE THROUGH TESTING
We only know it works if we test it. Our continuous regimen of testing and improvement ensures that our DR Program is always operating optimally.

DEDICATED RESOURCES
Our dedicated teams constantly monitor and update our customer-facing products to ensure we maintain and maximize the effectiveness of our DR Program. Our dedicated field specialists advise and support our steering committee–and execute and deliver regularly updated risk assessments, organizational impact analyses, and comprehensive testing.

In addition, our data center hosting partners are SOC2 and ISO27001 certified for security and availability, to ensure that physical security, network and IP backbone access, customer provisioning, and problem-management are controlled in accordance with our rigorous standards.

Backups

Application data is stored on resilient storage that's replicated across data centers. In addition to platform-wide resiliency, we also have a comprehensive backup program for our Atlassian Cloud offerings. Restore and recovery of these backups is provided on our own Atlassian Cloud platform.

Application database backups for Atlassian Cloud occur at the following frequencies:

- Daily automated backups are performed and retained for 30 days
- Daily manual snapshots of the standby RDS instance are sent to the secondary region and are retained for 30 days
- Snapshots of cross-region replicas enable data restoration in the event of AWS region loss or cross-region replica loss
- All snapshot and backup data are unencrypted
- For more information on our backup system, see our Security Practices page.

Quality assistance: Optimizing for quality in development

You are likely familiar with the concept of "quality assurance." We, however, follow a different model called "quality assistance"–a practice and term introduced by Professor of Software Engineering, Cem Kaner, in his paper "The Ongoing Revolution in Software Testing."

Following the principles of quality assistance, we deliberately educate and empower developers to test their own features to production-quality standards. We encourage this practice, in part, by keeping the ratio of testers to developers low–not because of resource constraints, but to force the adoption of a "whole team" mentality towards quality. As developers adopt the habit of building quality into their features from the start, it becomes deeply ingrained in their regular work flow. Rework is reduced, and the team achieves both faster and safer delivery of features and products.

While traditional quality assurance calls for a team of dedicated testers to carefully pore over newly developed code and put it through its paces–with the goal of ensuring flawless performance under all circumstances–quality assistance strives for the same goal using different, more efficient means.

When bugs are discovered through a traditional QA process, product release is often delayed as developers set out to rework existing code. Sometimes, these delays force an unpalatable choice between shipping a flawed product quickly or shipping a safe one late.

Quality assistance, on the other hand, focuses more on helping development teams achieve error-free code from the start, reducing both errors and product delays.

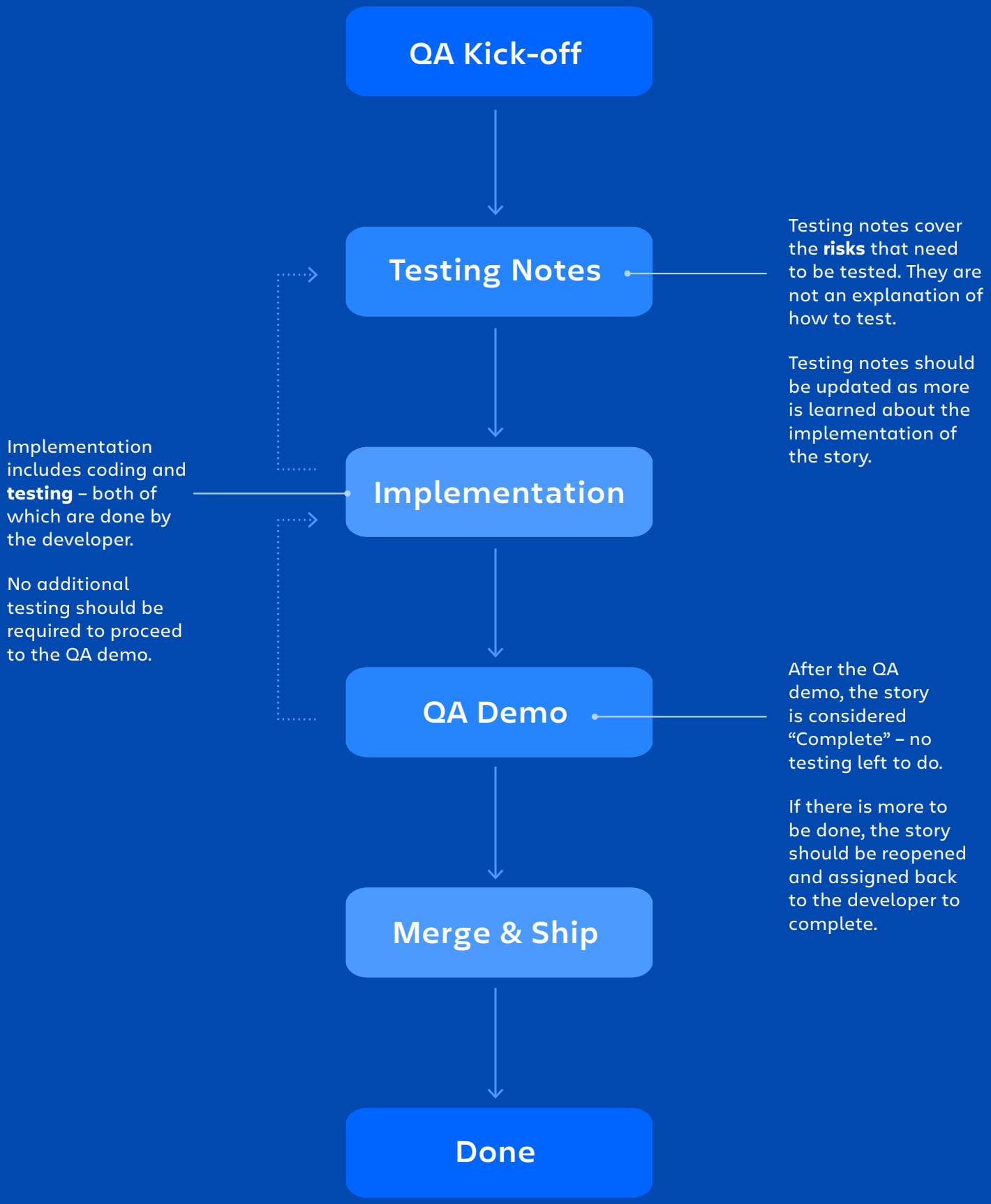
Here, then, are the guiding principles of quality assistance:

QUALITY
Development teams should always do their utmost to deliver software that works under all conditions. They should not expect other teams to find problems in their products, nor expect customers to find their bugs.

SPEED
Development teams should be able to ship their features to production in as short a time as possible. They should not write code that does not get shipped, and they should minimize the need for rework.

INDEPENDENCE
Development teams should be able to write features, test those features, and deliver them to production themselves. They should not create additional bottlenecks by relying on QA or other teams to help them deliver features and products that function as expected.

EXPERIMENTATION
A successful quality assistance approach requires the flexibility and resourcefulness to devise and apply innovative solutions that address the specific needs and challenges of every unique team and project. So teams are expected to adapt these processes to best suit their particular circumstances–and then to validate the results of those adaptations.


QA Kick-off
Testing Notes
Implementation
QA Demo
Merge & Ship
Done
Testing notes cover the **risks** that need to be tested. They are not an explanation of how to test.
Testing notes should be updated as more is learned about the implementation of the story.
Implementation includes coding and **testing** – both of which are done by the developer.
No additional testing should be required to proceed to the QA demo.
After the QA demo, the story is considered "Complete" – no testing left to do.
If there is more to be done, the story should be reopened and assigned back to the developer to complete.

Privacy

At Atlassian, we believe privacy should be clear, easy, and accessible – whether you are a company trying to decipher and comply with the GDPR and other global privacy laws, or you are a privacy-conscious end user that needs to know who has access to your data. That is why we commit to meeting the highest bar for personal data privacy, and support you and your organization in keeping your data secure and in your control.

Privacy Shield

Atlassian and our subsidiaries strictly comply with the EU-US Privacy Shield Framework and the associated Privacy Shield Principles for the collection, use, and retention of personal information transferred from the European Union to the US.

Government and Law Enforcement Requests

Transparency underpins our approach to responding to government and law enforcement requests for customer data. As part of our commitment to earning and maintaining your trust, we publish an annual Transparency Report with information about government requests for data. Atlassian will scrutinize every request for legal validity, and if required to comply, we will respond as narrowly as possible to the specific request.

Additionally, we have developed comprehensive Guidelines for Law Enforcement Requests to inform law enforcement officials seeking customer account records and customer content. To protect customers' data privacy and rights, we only provide customer information to law enforcement when we reasonably believe there's a legal requirement to do so and after careful legal review to ensure that they are in compliance with the law.

Access to Customer Data

Access to customer data stored within our applications is restricted on a "need to access" basis. We adhere to stringent controls over all customer data, and we train all new hires and contractors on the most up-to-date best practices for handling and protecting customer data.

Within Atlassian, only a tightly controlled group of authorized employees can access customer data stored within our applications. Authentication is established via individual pass phrase-protected public keys, and the servers we use accept incoming SSH connections only from Atlassian and internal data center locations.

We treat unauthorized or inappropriate access to customer data as serious security incidents and address them accordingly. Our incident management process includes notifying affected customers whenever we discover a breach of policy.

For more information, take a look at our Privacy Policy.

GDPR

We appreciate that our customers have requirements under the GDPR that are directly affected by their use of Atlassian products and services. That's why we've devoted significant resources toward helping our customers fulfill their requirements under the GDPR and local law.

Below are several GDPR initiatives that have been implemented for our cloud products:

1. We've made significant investments in our security infrastructure and certifications (see more at our Security and Compliance sections on our Trust website).

2. We support appropriate international data transfer mechanisms by maintaining our Privacy Shield certifications–and by executing Standard Contractual Clauses through our updated Data Processing Addendum.

3. We offer data portability and data management tools, including:

    - Profile deletion tool: We help customers and end users delete personal information, such as names and email addresses. We help customers respond to user requests to delete personal information, and we also help end users with Atlassian accounts–as well as people without Atlassian accounts–delete their personal information
    - Import and export tools: Customers may access, import, and export their Customer Data using our tools

4. We've made required updates to relevant contractual terms.

5. We ensure that Atlassian staff who access and process personal customer data have been trained to handle that data to maintain confidentiality and security.

6. We hold any vendors that handle personal data to the same data management, security, and privacy practices and standards to which we hold ourselves.

7. We have committed to carrying out data impact assessments and consulting with EU regulators where appropriate.

Learn more about our approach and investment in GDPR on our Atlassian GDPR Compliance page.

Keep up-to-date on our latest security enhancements

We're committed to remaining vigilant against ever-evolving and newly emerging threats. And our customers expect no less. Stay connected to the latest information on the security, reliability, privacy, and compliance of Atlassian products and services at our ***Trust site.***

Want to dig deeper ?
www.atlassian.com/trust

ATLASSIAN