Tricentis

Test management for compliance and security: where to start and how to empower your teams

Tricentis

Test management for compliance and security: where to start and how to empower your teams

GENERAL TOPICS/SUMMARY

- In recent years, new and changing data regulations have made it more challenging than ever for companies to remain compliant.
- Collaboration between testing teams, development teams, and corporate and technical leadership is critical to ensuring data compliance, avoiding breaches and fines, and preserving customer confidence
- To meet data compliance requirements, companies should take small steps as early as possible - every effort they make now will reduce their technical debt later.
- Test management is key for meeting compliance needs: it drives collaboration across stakeholder teams, scales best practices and standardized checks for compliance, and helps establish an audit trail.

INTRODUCTION

Compliance laws have turned every industry into a regulated industry. In recent years, regulations like GDPR and the California Consumer Privacy Act have forced change across all industries, proving that the landscape for managing sensitive data is constantly changing. Meanwhile, attacks become more sophisticated each day. The earlier organizations can get ahead of these challenges, the better it will be for their products, teams, and for customers.

To meet these ever-changing challenges, it's critical to keep your teams, requirements, and delivery plans aligned. To do so, you'll need a clear view of roles and responsibilities for each team when it comes to security and compliance. Additionally, you'll need the right test management and automation capabilities to establish traceability between requirements and testing, to enforce standard checks during development, assess risk levels during release, and if needed, establish an audit trail.

HOW YOUR TEAMS CAN SUPPORT DATA COMPLIANCE AND SECURITY

Addressing data compliance and security is too important and far-reaching to be handled by any one team. To get ahead of the data compliance challenge, your organization will need to involve more than just your quality assurance leader. Data compliance also requires the collaboration of testing teams, development teams, and leadership. Let's explore how testing teams, developers, and leadership can share responsibility for data compliance.

The role of quality and test teams

If you're a QA leader, your team is under pressure to accelerate testing cycles while reducing risk. Meanwhile, new compliance requirements continue to introduce risks that you must account for in your test plans — often without the benefit of extra time to implement. Testing teams should champion data compliance and security best practices that allow your organization to scale safely, and function as a voice of reason with business and development teams to help prioritize safety and compliance considerations.

Where to start: collaborate to include security and privacy, by design

You'll need to put security at the forefront of your design phase and software development lifecycle, regardless of your industry. Start by implementing a security-by-design or privacy-by-design approach in coordination with your architecture and development teams, as well as with any other stakeholders within your organization, such as InfoSec, legal, or other leadership.

This task may seem overwhelming, but keep in mind that the best way to start is often to consider your basic requirements around data:

- Make high-level decisions about which data you'll encrypt and how.
- Decide how you'll control your perimeter and grant access once you've launched your application.
- Establish a method of detecting unusual behavior so that if someone breaches your perimeter controls, you'll be able to stop them before they access your database.
- Determine how you will demonstrate compliance – not just to determine release readiness, but as a record in event of a breach, violation, or audit.
- Understand how and when you will improve and revisit test plans as more features are delivered, and both your product and business mature.

If your product is already mature, basic testing for common use cases may be the easiest to implement while you tackle the larger challenges above. These can include (but aren't limited to):

- Operating system (OS)-specific testing
- General administrative access
- Single sign-on requirements
- Password complexity requirements
- Admin, super-admin, and user controls

Build continued collaboration between testing and development

Keep QA in lockstep with your development teams as soon as you know what the user experience will be. If your QA team can work closely with the development and business teams and see their requirements, they can avoid working at cross purposes. Later in the development cycle, there will be very few occasions when QA must request input directly from users because this input will have been included in the process all along.

Although your development teams may build a great deal of vision into your product roadmaps, they still must provide evidence of compliance. As you plan and evaluate the results of test cases, look for ways to prove that your organization is doing privacy-by-design or security-by-design. If you can design test cases that produce multiple types of evidence, you can dramatically streamline work for various teams — especially those involved in regulatory audits. When creating this evidence becomes an organic part of your processes, it will no longer feel like overhead or added work.

You'll need a system of record to document this evidence. Aim to document your test cases, steps, execution, and analysis within a test management system that integrates tightly with your development or product planning tools. The right test management solution will support real-time synchronization of requirements, test outcomes, and defects with your development and product planning tools. You'll keep your development, product, and testing teams coordinated.

Scale standard compliance and security checks with test automation and centralized test management

One of the most valuable investments testing teams can make is in centralized, well-managed test automation. Given the right tools, your testers will be able to automate most security and privacy testing, making it easier to meet requirements without sacrificing speed. Considering the current pace and volume of development, it's almost unthinkable to proceed without automating and centrally managing these tasks. Here's why:

- **Compliance- and security-specific testing expertise can be hard to find.** Automation will allow you to repeat and scale this specialized knowledge across your existing quality team.
- **Automation makes it easier to build functional testing to happen immediately after code check-in, and at the integration level.** This delivers an immediate response to the development team so they can make the right changes, sooner – this means you'll improve quality while preserving speed of development.

However, test automation alone can only take you so far. To improve security and meet compliance requirements at speed and scale, you'll need a test management solution to help you manage and scale test automation alongside manual testing. The right test management tool will:

- **Integrate easily with your specific test automation tools, support automated workflows, and work well with your CI/CD solution.** This frees your team to focus on the critical task of ensuring release readiness, instead of tracking and troubleshooting integrations.
- **Track automated testing in one place, alongside manual testing.** While test automation is important, it's often complemented by manual and exploratory testing. These results need to be tracked results alongside your automation testing in one place, rather than in a separate tool to ensure that you have a unified view of testing and coverage before a release or deployment.
- **Include powerful, flexible reporting across all your testing activities.** This helps you determine release readiness, align with other teams, and make strategic decisions to continually improve quality, compliance, and velocity.

A scalable, enterprise-grade test management solution to centralize test plans and results not only helps testing, development, and other teams stay aligned, but also helps identify problems earlier, and improve quality and compliance while minimizing the impact on velocity.

The importance of executive sponsorship

The support of executives is critical to ensuring security and data compliance. **Executive sponsorship ensures that compliance and security are taken seriously from the earliest stages of development and product maturity, so the business can grow faster, safely.** However, many executives overlook compliance and security in favor of controlling spend, or features and pace of delivery to drive business growth.

When executives fail to support data compliance from the earliest stages of their business, they set themselves up for severe consequences later, and it's harder to course correct in a mature business. But eventually, being unable to demonstrate compliance prevents companies from growing – it often blocks them from selling to larger enterprises with stringent compliance requirements, or from working with services or delivery partners that can scale the business. And the longer a company goes without achieving compliance, the greater the chance they will experience a data breach and the resulting fines and public relations fallout.

Without executive support, testers will be unable to influence the rest of the organization to meet data compliance requirements. For example, it's unlikely they will have the confidence to hold up a release candidate for not meeting regulatory requirements. Testers drive collaboration across teams to demonstrate a company has met regulatory requirements. **Empowered with executive support and a broad understanding of the regulations that apply to their industry and organization, the impact of testers on the health and continued growth of the business can be huge.**

TRICENTIS QTEST HELPS SUPPORT GROWING COMPLIANCE NEEDS

For fast-growing, enterprise teams, test management is critical to meeting compliance and security requirements. Test management drives collaboration across testing, development, and stakeholder teams to build compliance testing throughout the software development lifecycle. The right solution can also reinforce best practices around handling user data, and help establish an audit trail to meet growing compliance needs.

Tricentis qTest is a test management solution to help you collaborate, plan, track, and improve testing as you work towards improving quality and meeting security and compliance needs.

With qTest, you can:

- Establish a central repository for testing, reusing test cases to scale standards and specialized knowledge like compliance testing across the organization
- Provide a source of truth for test projects, cases, steps, execution, approvals and outcomes, helping build an audit trail for the organization
- Integrate with planning tools such as Jira or Azure Boards for real-time test/development collaboration, and establish seamless traceability to requirements
- Integrate with any third-party testing or DevOps tool like Jenkins or Azure DevOps to accelerate testing with automation and within CI/CD pipelines
- Share powerful, customizable analytics and reports across the organization for faster, more strategic decision-making with the team

CONCLUSION

As you strive to keep your applications and data in compliance, there's a lot to do. Plan to implement a shared responsibility model across testing, development, executive leadership, and other departments. Make sure your model provides ways of managing, training, and deploying your engineers effectively to be sure they're following best practices and implementing proper controls to help you increase software quality at scale. The earlier you start implementing controls within a project and the more you can automate the process, the less technical debt you'll incur later, and the faster the business can grow – safely.

ABOUT TRICENTIS

Tricentis is the global leader in enterprise continuous testing, widely credited for reinventing software testing and delivery for DevOps and agile environments. The Tricentis AI-based, continuous testing platform provides automated testing and real-time business risk insight across your DevOps pipeline. This enables enterprises to accelerate their digital transformation by dramatically increasing software release speed, reducing costs, and improving software quality. Tricentis has been widely recognized as the leader by all major industry analysts, including being named the leader in Gartner's Magic Quadrant five years in a row. Tricentis has more than 1,800 customers, including the largest brands in the world, such as Accenture, Coca-Cola, Nationwide Insurance, Allianz, Telstra, Dolby, RBS, and Zappos.

To learn more, visit www.tricentis.com or follow us on LinkedIn, Twitter, and Facebook.

AMERICAS

2570 W El Camino Real,
Suite 540
Mountain View, CA 94040
United States of America
office@tricentis.com
+1-650-383-8329

EMEA

Leonard-Bernstein-Straße 10
1220 Vienna
Austria
office@tricentis.com
+43 1 263 24 09 – 0

APAC

2-12 Foveaux Street
Surry Hills NSW 2010,
Australia
frontdesk.apac@tricentis.com
+61 2 8458 0766

v. 0222