Our way to ISO 27001

Alexandre Aubert

Published Jun 7, 2023 (Edited Jun 7, 2023) • Validated Sep 28, 2024 • 4 min read

our way to ISO 27001 certification

Introduction

In this article, i will share the steps we've gone through in Piano Analytics teams to implement ISO 27001 requirements in our CI (continuous integration) and development practices.

From defining the goals to being successfully certified, let's open the box and share how everyone has successfully contributed to this great success !

First step : let's have a plan !

We needed first to **consider the requirements**, evaluate the initial gap and **define a plan** to fill it properly and fast to be on time for the real audit ! This journey has

started beginning of 2022, let's review the main

1. Consider the requirements

Two main tracks are identified to be fully compliant to ISO 27001 requirements

Doing the things right	Being able to prove it
Security controls (S.A.S.T.)	Traceability
"4 eyes" principle	Visible practices
Structured change management process	Available processes

2. Define milestones

3 global 'milestones' are defined to be ready to be certified in November:

Second step : fill the gap !

Starting March 2022, we started the implementation by taking **concrete actions** to progressively fill the identified gaps.

1. Security controls : S.A.S.T.

S.A.S.T. (Static Application Security Testing) becomes **mandatory for all** the customer product's code base

We decide to meet this requirement by using Sonarqube **quality gates** with a progressive and gradual setup:

03/2022: « Security score = A » is required on overall code

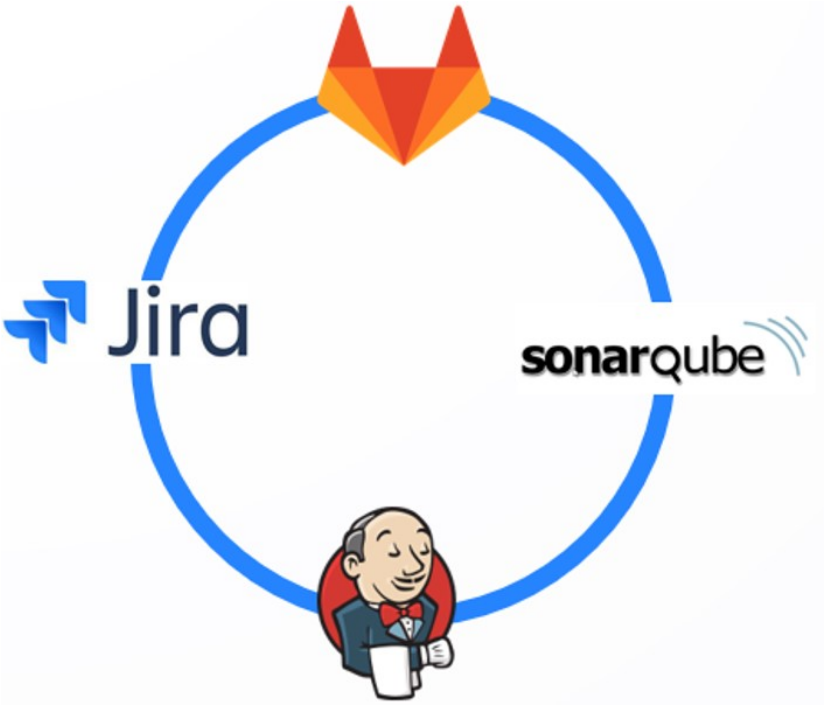
05/2022: « Security review score = A » on new code only

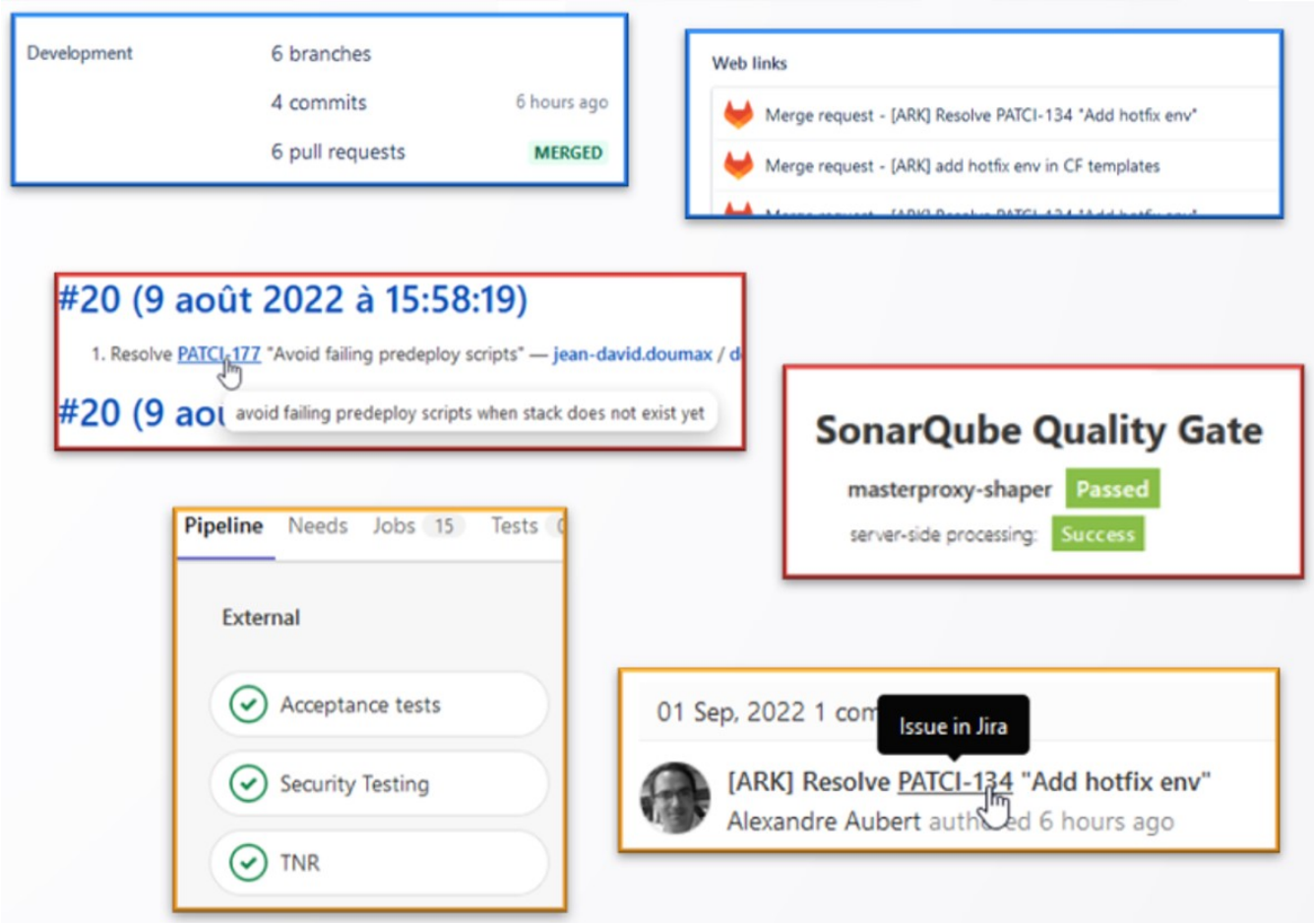
09/2022: « Security review score = A » on overall code

> *Sonar scores definition is available on sonarqube metrics documentation*

2. Traceability

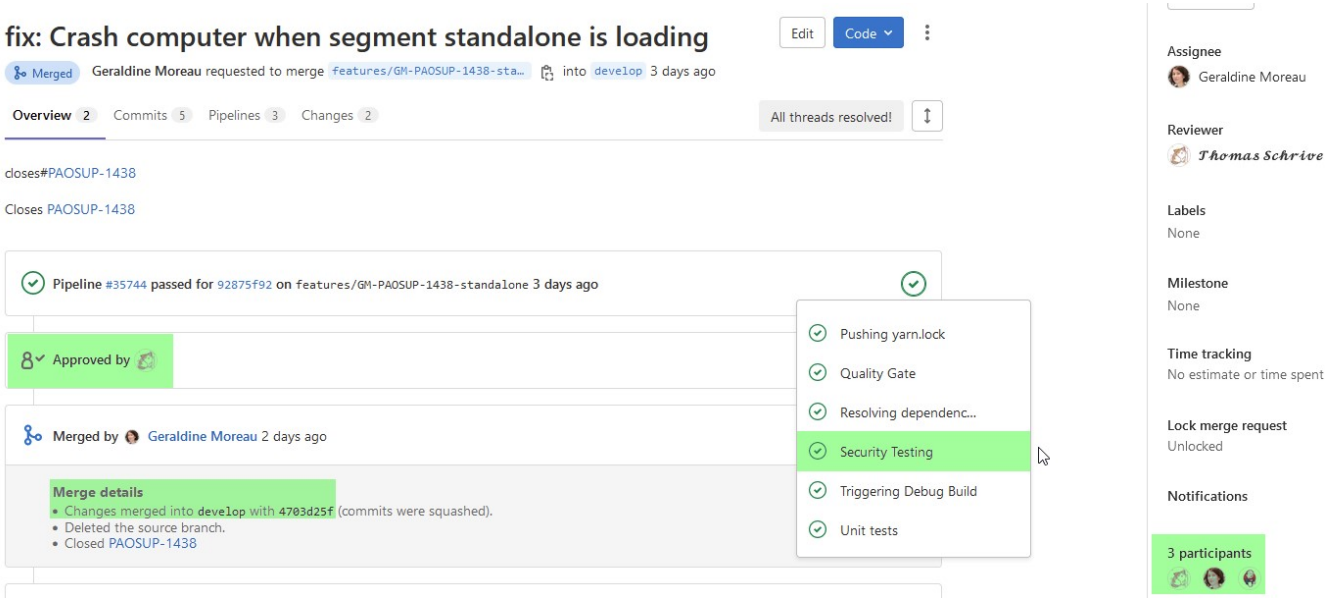
CI Tools are interconnected to **make the information available** to everyone everywhere (using plugins, configuration and available integrations for each tool)





3. "4 eyes" principle

Every code change should go through a **Merge Request** with an **identified approver**



Everyone as an actor of our success

1. Information is made available

Interlocutors are identified : @Erwan Loaec / @Alexandre Aubert

Emails describing the plan, the milestones are sent to everyone

Questions are answered, requirements clarified on demand

Confluences pages are created / extended to help each one meet the requirements:

Test strategy / SDLC lifecycle management (now in OnePiano)

[EXTENDED SECTION] Security related tests

[NEW SECTION] Rollback policy

[NEW SECTION] Merge requests and requirements

"Tools interconnection" and how to get the most of it

Tutorials / HowTos

Gitlab statuses implementation (from our Jenkins scripts)

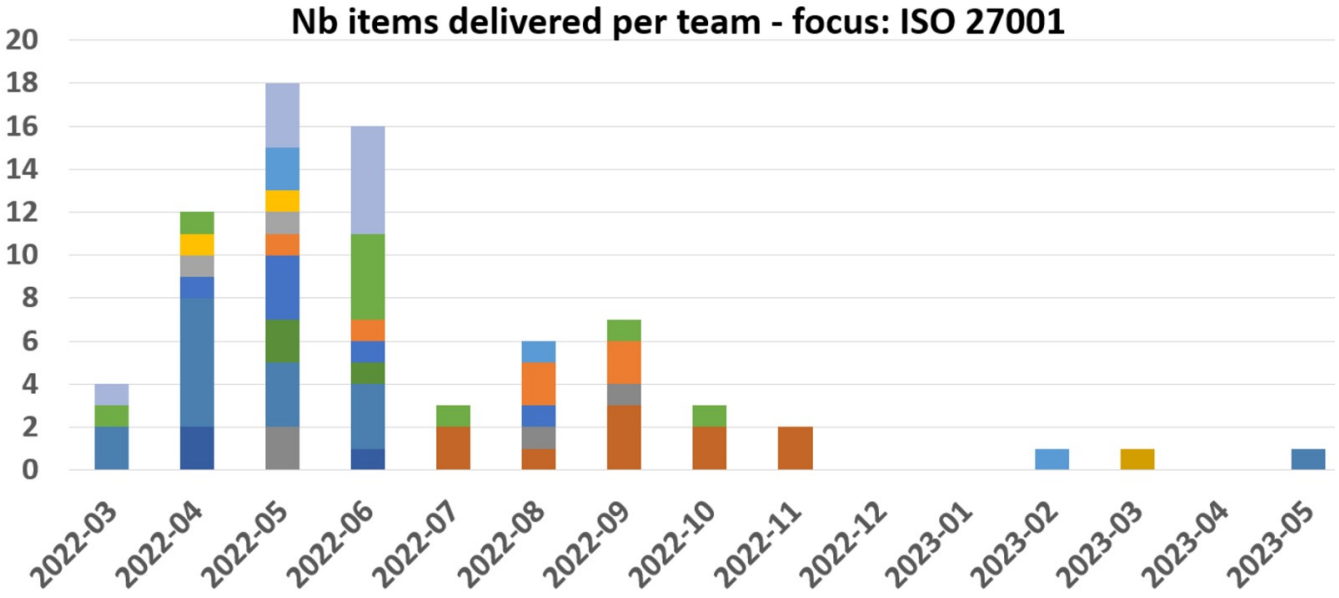
Webhooks to automatically trigger jenkins pipelines from Gitlab

Sonarqube and quality gates

and more...

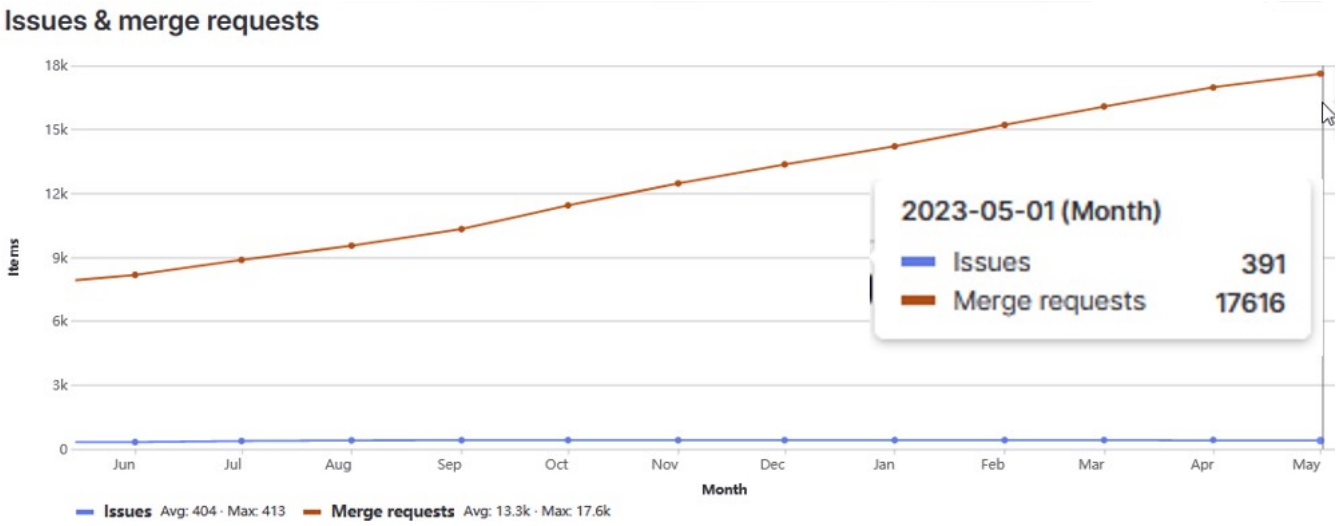
2. Engagement is global

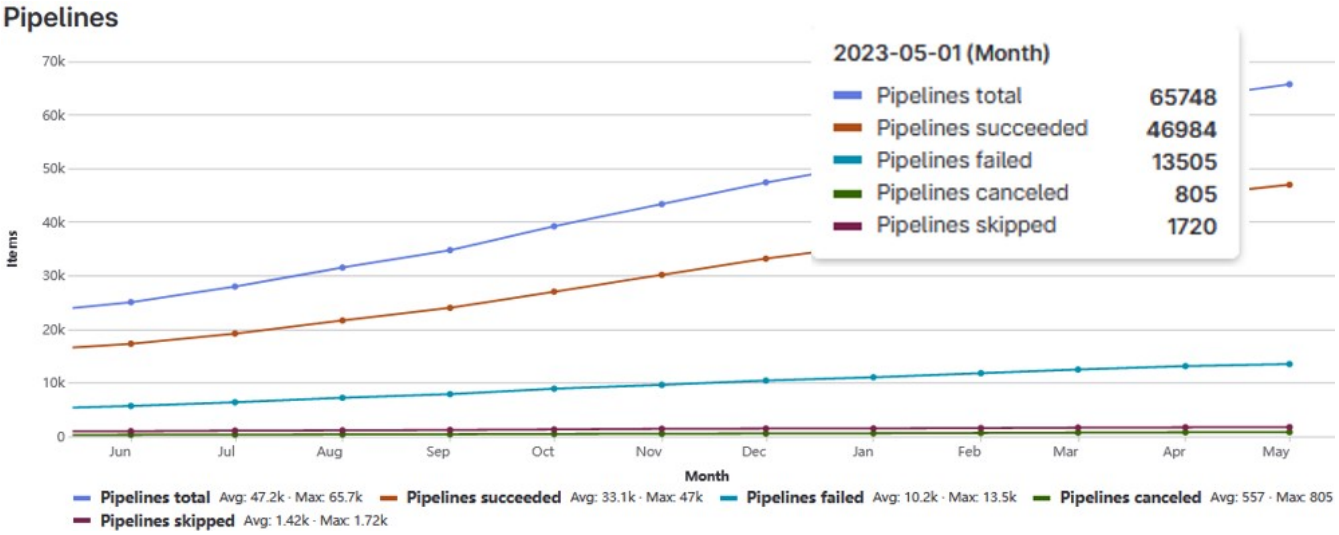
In a few weeks only, the teams have filled the gap and reached the objectives by implementing what was missing/incomplete in their CI scripts and adopting new practices in their daily work (systematic merge requests, peer approvals, quality gates...).



“First internal audit in June showed things to adjust which were fixed during summer. We were then ready for the real audit in November !”

> Merge requests and pipelines are now common practices everywhere and information is made well visible to anyone (an ISO auditor ?) in Gitlab:





Each member of the development teams has played **a significant role** in reaching the target. This project was really challenging with **a short delay** and the need to **compose with ongoing roadmap projects**. Each intermediate milestone has been successfully delivered and we reached the goal by obtaining this important certification for our business !

Ensuring ISO conformity overtime

1. Automated checks

Daily/weekly alerts are setup to automatically detect possible deviations:

- Too low security scores
- Lack of visibility in Gitlab merge requests (S.A.S.T. results, approver...)

Potential deviations are analyzed and remediation actions are taken if necessary

2. Maintaining our culture

Regular trainings about security aspects of development aim at keeping each one's awareness at a high level

Daily support and discussions about security and the right use of our tools continue serving our excellence in this area

Sharing and reminding the value it generates for the company is also an important aspect to stimulate individual engagement

Conclusion

Thanks eveyone for your active contribution to this success : from changing small habits to sometimes adopting very different ways of working, everyone has responded fast and efficiently to this short time unexpected challenge.

It wouldn't have been possible without this shared and global effort : **big kudos to all !**

Topics

Security Ci piano analytics