PLUTORA

WHITE PAPER

Managing Regulations Using Value Stream Thinking

- How to shift governance left and achieve continuous compliance with value streams
- How to respond when a regulating body asks for a set of criteria to be met by a set date

There are many highly regulated industries in the world; finance, healthcare, aviation and retail among some of the best known, and there are many regulations such as GDPR, CCPA, PCI and SOX that impact almost all industries.

While these regulations are put in place to protect us, we, the consumers of the products and services provided are not only demanding the resulting safety, equally we want improvement and extension of capability; we want to be delighted too. This places service providers under increasing pressure to deliver convenience and innovation without compromising security and reliability.

> "I have it on pretty good authority that the CIO and VP of IT Operations were just fired over some compliance audit findings that were no longer tolerable. Let that be a warning to you all that compliance is not just a moral obligation or a set of contractual obligations... it's also the law."
>
> **John, CISO in 'The Unicorn Project'**

The consequences for a business of failing to meet a regulation are significant and often frightening; fines, reputational damage, regulatory constraints, legal action and potentially even jail-time. HIPAA, MiFID, Affordability, cybersecurity standards, Basel II; it's a minefield. It is indubitably correct that we all treat them with the utmost seriousness.

But what's a commonly held myth is that regulations and governance can only be dealt with using waterfall approaches. The cost of compliance keeps on rising, so if we can make savings here, it's going to help our bottom line.

In exploring this further, it's helpful to think about meeting governance objectives from two perspectives:

- How to respond when a regulating body asks for **a set of criteria** to be met by a set date
- How to **shift governance left** and achieve continuous compliance

Meeting a Set Date

Waterfall approaches, where we set a deadline and work backwards from it to plan a series of phases of sequential work is the way we've worked for a long time. But it has its problems. These types of projects are rarely on time or budget with or without superhuman effort that often results in high-pressure and burnout. They also aren't flexible and struggle when requirements change, which they always do.

The alternative is to reduce risk and set the stage for more sustainable working practices by working in smaller increments that allow us to adapt as requirements change and as our understanding of them evolves. We are still aiming for the set date but we break the work down into smaller pieces or batches that allow us to receive fast feedback on progress and sense check before we move onto the next batch.

This approach presents great savings in terms of queuing times, prevents us from taking the big risks we take when we make a big bet and, in the technology world, gives us the opportunity to test our systems regularly without having one big merge event that is unpredictable and has a high probability of going wrong and being hard to unpick.

Imagine you have six months to deliver 120 items.

Scenario One / Waterfall:

You work on all the things in a design phase, then a development and build phase, then a test phase and right at the end of your six months, you deliver everything in one big batch.

Scenario Two / Agile:

You work in twelve increments, delivering 10 items every 2 weeks, getting feedback, checking the pieces work and making sure the next 10 items are the right things.

In scenario two, **we have more confidence in the outcome** as we have been able to consistently check progress, and because we have been able to course correct quickly, we will often have delivered more items. This is controlling the flow of work in a way that allows us to accelerate its delivery and can be used for delivering the 'features' that describe compliance to a new regulation in the same way we might use it to deliver a new product. We test regularly and don't have a painful merge event at the end stage.

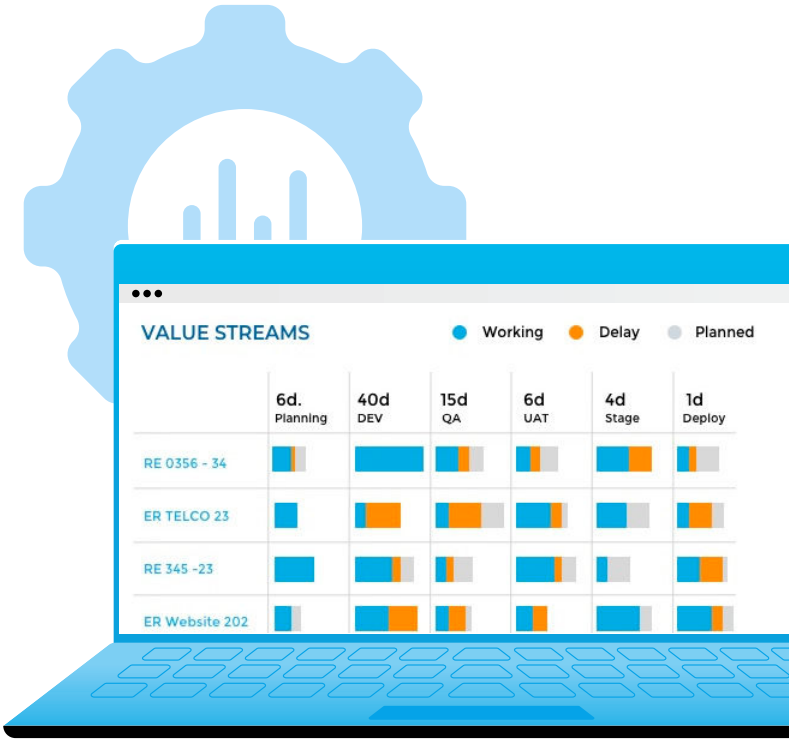
In addition to controlling the flow, we also want to make it transparent or visible so that we can inspect it regularly and adapt accordingly.

By examining the value stream, we can identify where waste is. Feedback loops tell us quickly if we are doing the right thing and improve our responsiveness posture.

By having small value stream centric teams focused on the end-to-end flow, not passing off or handing over to separate teams to perform testing for example, allows us to think like a value stream and be focused and have clarity on the job in hand. Governance, risk management, and compliance (GRC) roles can be assigned to or embedded into the team; using RACI charts is an effective way of making this accountability visible and driving the conversations. Having a GRC voice at every daily or sprint-based event keeps the focus clear while embracing flexibility.

This moves leadership from a management role to a place where it helps the teams to make discoveries about the regulation and how it can be satisfied. This way of working encourages us to bring our auditors into the process; they are friends, not enemies - remember, we all want to be safe and regulators are people too; they protect us from reputational damage and fines. We can ask them to help us check continuously that our direction is true and course correct as needed. We stop having milestones and RAG statuses and start having continuous conversation.

Automation supports and enables these ways of working. Plutora automates governance through release pipelines and standardizes release management across the enterprise. It provides complete visualization, as well as business intelligence, providing transparency and real data to inspect. This creates opportunities for discovery conversations that enables us to adapt.



Governance and auditability are baked in, as are customized approval workflows. If teams have trouble accessing test environments that are shared, Plutora streamlines this process so we aren't working to that one big merging event or test phase but instead are using continuous integration and delivery to get that fast feedback on our potentially shippable increments.

Governance **Audit** **Workflows**

It provides insights into release risk and value stream flow by integrating from your product backlog through to the production platform helping the teams make discoveries about where to mitigate and what to prioritize.

Continuous Compliance

There are frequent instances of new regulations coming through or large-scale changes to those that exist that create additional workload for our businesses, there is also a constant need to ensure that any new changes to our existing systems comply with the existing regulations. In many organizations, the GRC people are in a separate team; like security/InfoSec are, or having a centralized change or release team. Whilst having these overseeing bodies helps us manage dependencies in complex and tightly coupled environments and provides a dedicated squad of subject matter experts, it also creates a situation where we have handoffs between teams and potential delays and friction. It also limits the autonomy of our value stream or feature teams.

When we start thinking of our work in terms of value streams, anything that delivers a product or a service, rather than big batches of project work, it changes our approach and drives us to seek to reduce waste in the process often caused by those handoffs and delays.

In a waterfall approach, the GRC team are often a constraint, brought to the party late and who may be forced to say "no" as having to ingest a large amount of information in one lump is difficult and causes fear and uncertainty. When we plan and deliver our work in much smaller iterations in small, autonomous teams it gives us an opportunity to consider our GRC objectives more frequently and in different ways.

As a compliance director at an Australian bank replied to the question: **"What is the biggest change you predict for compliance in the next 10 years?"**:

> "Compliance being considered at every stage of the business process - not just when things go wrong. It will be an integrated, valued inclusion, from initial planning and strategy development, through all phases of product or service development, to delivery and reporting."

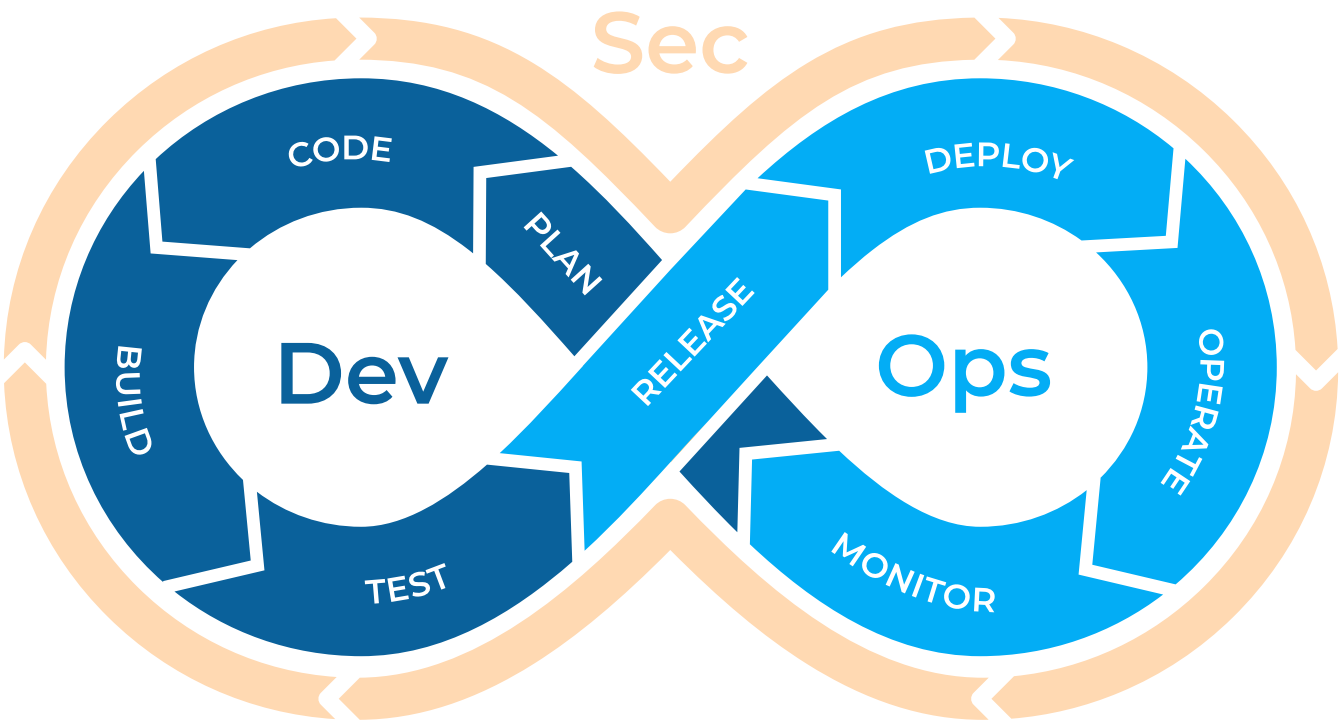
Our small autonomous teams who build and run the product or service can invite their GRC friends into the process, making the product backlog visible, even allowing them to contribute user stories to drive conversation.

They can participate in ceremonies like standups, planning, reviews and retrospectives. They can provide guardrails and guidelines and advise the team on priorities and help make decisions when trade-offs need to be made.

4L Retrospective

LIKED What did you like?	LACKED What did you lack?
LEARNED What did you learn?	LONGED FOR What did you long for?

An example of a Liked, Longed, Lacked, Learned (4L) Retrospective which is useful after a week where the team struggled with a hard problem.



Together, they can work on automating GRC where possible: using the **CICD pipeline** to test requirements and only allow a build to go green when all aspects of a (now automated) checklist are met (**policy as code**) and ensuring that deployment automation tooling supports segregation of duty requirements. DevSecOps practices and tooling reduce the risk of a breach.

Having all these processes automated means that audits can be automated too, massively reducing the time spent on these onerous jobs. A key tenet of this way of thinking and working is that we aim to break dependencies, not manage them, but this isn't something we can do with a click of our fingers or overnight.

Many organizations struggle with environment management, and whilst migrating to self-service cloud platforms helps, this will take time in many cases.

While teams are evolving to autonomy, systems will remain tightly coupled and operating on shared infrastructure. Here Plutora helps to act as a single source of truth for all applications and environments.

It streamlines the environment booking process, supporting both scheduling as well as contention management. Governance and auditability are baked in, as are customized approval workflows.

Again, whilst teams and systems still have dependencies on one another and are not yet able to have a fully autonomous, light-weight peer-reviewed change process, Plutora's Change Request (CR) capabilities and ability to interface into ITSM tools allows seamless movement of CRs across production and non-production. It can orchestrate automation, as well as provide customized approval workflow. Business intelligence reporting and auditability are also included.

Plutora can maintain Configuration Items (CIs) for all aspects of applications and environments and can integrate with a CMDB/CMS to pull this data. Having it updated automatically (utilising deployment automation and CRs), and pushing it back to the CMDB/CMS enriches the single source of truth and improves our governance posture.

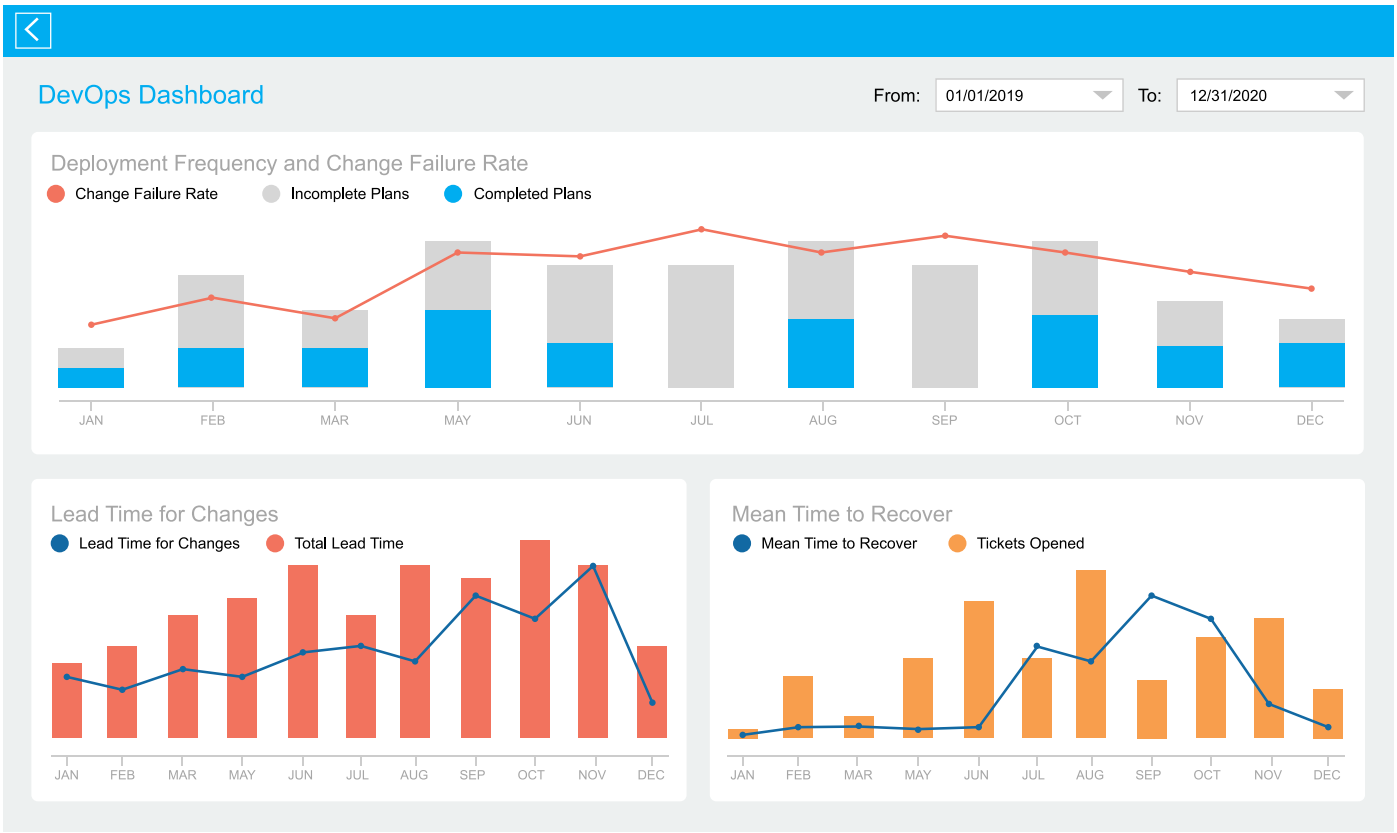
Plutora's business intelligence capability allows prior and upcoming demand to be measured and can be used to predict upcoming demand. Because it has a view of existing capacity it can predict capacity shortcomings, all of which helps ensure teams don't make critical mistakes when making regulatory and governance decisions. It can be used to produce Disaster Recovery (DR) plans using approval workflows that incorporate governance and auditability. It can also utilize test automation to run health checks/pipe cleaning on environments to notify of unavailability, as well as assisting with triage.

Our organizational models can extend from small teams focused on the lifecycle of components to support the regulation to creating governance swarms who collect around teams when their product or service requires. They become advisors and experts in their field instead of blockers.

Having visibility into the end-to-end value stream helps teams, teams that include both engineers and GRC experts, to have sensible conversations about risk and find optimum ways to mitigate problems. Work in organizations passes through many systems. In a traditional waterfall environment, the work is managed through Word and Excel documents and using MS project tools and Gantt charts. In a value stream centric world, our value stream centric teams have CICD pipelines where the work visibly starts its flow as a small item in a backlog, typically Jira. The toolchain has many components; artifact repositories, source/version control and management, continuous integration servers, testing, release and deployment automation, service desk and monitoring.

For us to fully understand the flow of value from idea to realization, and optimize that flow, we need to be able to trace items of work as they travel through the system.

Using Plutora allows us to do just that, integrating the pieces and giving us insights into where we have delays, where we have more risk and how we can increase our cycle time without compromising quality and improving our audit posture.



By providing a single-pane-of-glass view of the software factory, Plutora allows GRC teams to have visibility of the release from the very beginning.

They can understand the scope of the release and decide at what point they want to be involved. GRC approval can be embedded into the process and checks and balances automated where possible. Compliance analytics is possible to understand trends and understand areas of increased risk.

These learnings can be fed back into the software factory. Projects can be scored on compliance maturity, and initiatives run to swarm low scorers. It takes time, years in many cases, to move from a waterfall to a value stream centric way of working and there are many moving parts in terms of people, platform architecture and automation, but Plutora drives collaboration during the transformation and provides valuable insights that inform decisions and direction whilst also providing a backbone for governance.

About Plutora

Plutora, the market leader of value stream management solutions for enterprise IT, improves the speed and quality of software creation by capturing, visualizing and analyzing critical indicators of every aspect of the delivery process. Plutora orchestrates release pipelines across a diverse ecosystem of development methodologies, manages hybrid test environments, correlates data from existing toolchains, and incorporates test metrics gathered at every step. The Plutora Platform ensures organizational alignment of software development with business strategy and provides visibility, analytics and a system of insights into the entire value stream, guiding continuous improvement through the measured outcomes of each effort.

PLUTORA®

Learn more: www.plutora.com

Email: contact@plutora.com