

The slide features a red-to-orange gradient background. At the top left, it displays the logos for 'DevDays EUROPE' and 'CyberWise Con-'. The main title 'Compliance by design | Continuous Compliance' is centered in large white font. Below it, the subtitle 'A better approach to compliance' is also centered. The speaker's name and title, 'Marcel Britsch | Product and Change Consultant', are centered below the subtitle. At the bottom, there is a logo for 'BEAUTIFUL ABSTRACTION' with the website 'www.beautifulabstraction.com' and a QR code.

Hello and thanks for your interest in this talk.  
I hope I can make this valuable and exciting...

-

My name is Marcel Britsch. For the last 20 years I have been working as independent consultant with consultancies and directly for private and public sector clients, helping them build the best products and services they can...

I have worked with clients retail, finance, energy but also conservation, automotive, healthcare, Web3.0 / Blockchain (when that was a thing), the UK tax office, and have been for a while product managing an AI innovation team for an EdTech client.

-

I am available as consultant, advisor, coach&mentor, to work with or run your teams.

I also speak at other conferences, blog and podcast.

So please do get in touch...

You can find me here:

Web: <https://www.beautifulabstraction.com>

Blog: [www.thedigitalbusinessanalyst.com](http://www.thedigitalbusinessanalyst.com)

Profile: <https://www.linkedin.com/in/marcelbritsch>

/////

### **Bio**

Marcel Britsch is an independent Digital Consultant, Product Manager and Agile Transformation specialist.

He has been living and working in London for over 20 years. He has worked with creatively and technically focused agencies, consultancies and clients across EdTech, MedTech, Fintech, Web3.0, energy but also conservation and automotive.

He helps organisations build solid products and services in a sustainable way by facilitation, pairing, coaching or hands-on product management.

He believes that project success is strongly linked to happy teams, value-focused decision-making and fast feedback cycles. He is passionate about finding the best tools and techniques to optimise team culture, ways of working and solution design. He considers projects that follow classic waterfall / big-design-up-front practices to be too likely doomed to go anywhere near them, but loves to help organisations build products and transform in incremental evolutionary fashion or move towards this approach.

Outside of work he is interested in SciFi and comic books, Theravada Buddhist meditation and number theory.

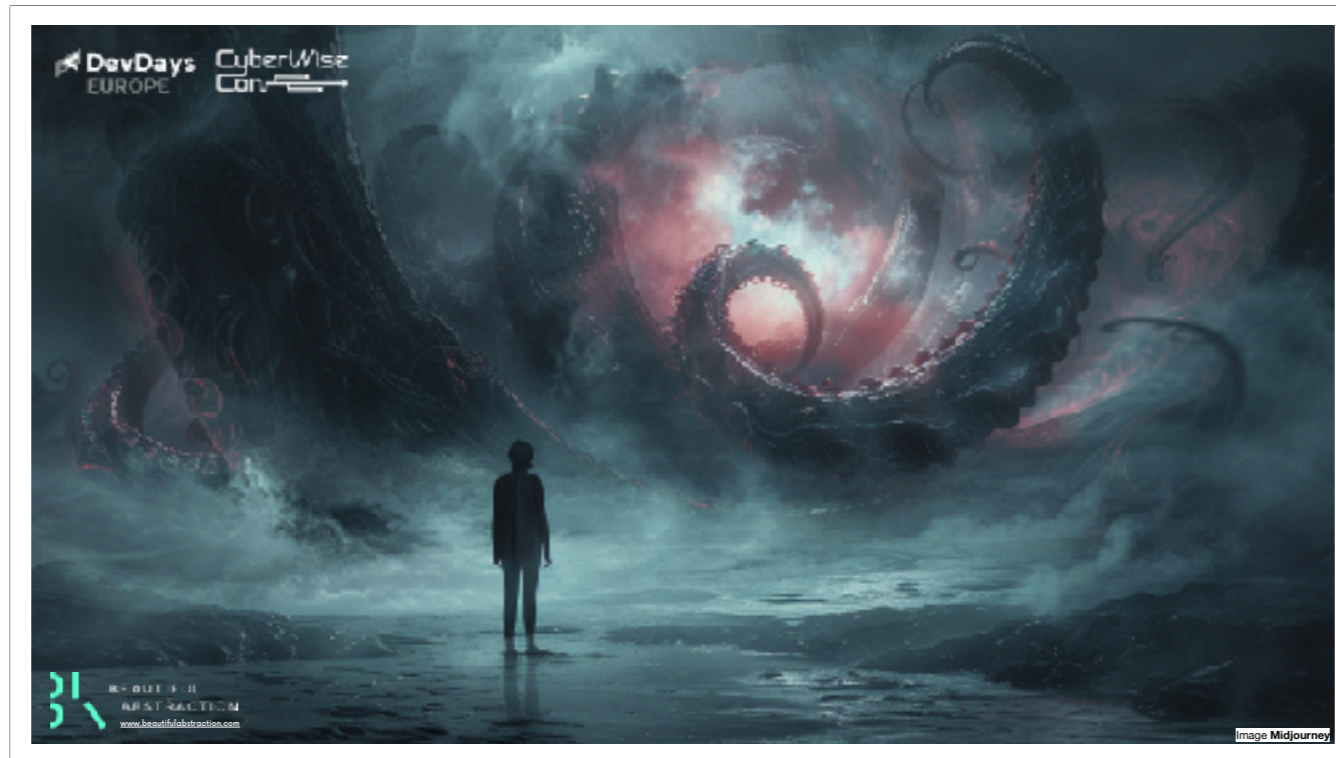
He is a regular speaker at conferences, teaches at Cambridge University, blogs at [www.thedigitalbusinessanalyst.com](http://www.thedigitalbusinessanalyst.com), has hosted The BurnUp podcast about 'all things agile', and can be found at <https://www.beautifulabstraction.com>.

—

Web: <https://www.beautifulabstraction.com>

Blog: [www.thedigitalbusinessanalyst.com](http://www.thedigitalbusinessanalyst.com)

Profile: <https://www.linkedin.com/in/marcelbritsch>

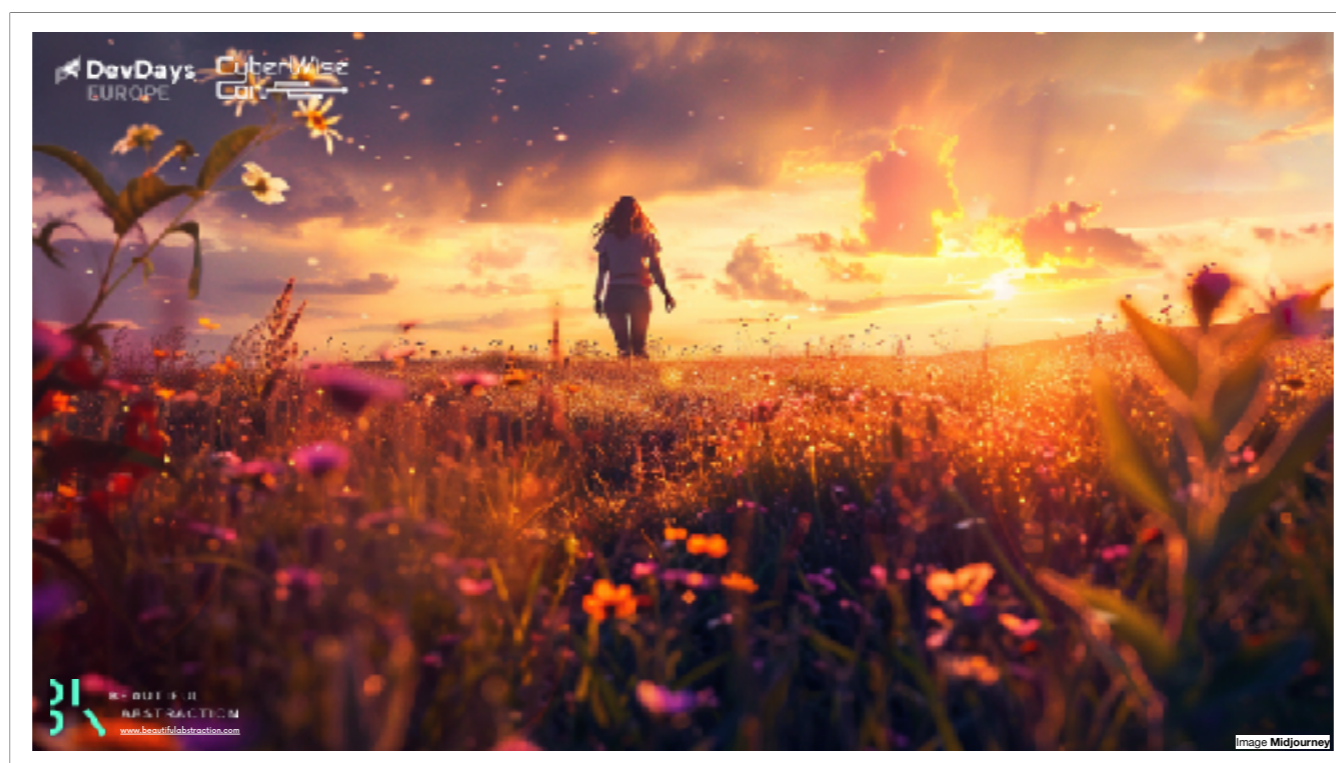


Who's ever had to deal with compliance?

Who's ever thought that what they were asked to do for compliance was painful and / or a waste of time?

I certainly have.

I hope that over the next 40 minutes I can shift your perception from this, to a little bit more like this:



So that compliance becomes not only valuable but also comes with ease.

////

*I'm a product consultant, and I help organisations design, deliver and operate the best products and services they can. I have worked with agencies, consultancies and clients, across public and private sector, across Fintech, Medtech, automotive, Web3.0/Crypto, Energy and Sustainability, and then some. Right now I'm working with an Edtech AI innovation team.*

*As an independent consultant I'm very interested in hearing from you to exchange ideas, explore collaboration or if you want to discuss where I might be able to help out with whatever you are doing (whether this is by doing a hands on product role, coaching, mentoring, facilitating or just speaking like now). So please do get in touch... More details at the end.*

## **Compliance** /kəm'plaiəns/

is to satisfy regulatory, corporate and / or other external or internal expectations

that we are subjected to or which we voluntarily adopt

and which we deem relevant to ensure the sustainability of our business.

So what is 'compliance'?

I'll let that stand for a second, we'll come back to the various aspects...

### **///notes**

The term 'expectations' is working very hard here... It's the 'things' an organisation chooses to comply with (whether they are laws, regulations, values, principles, best practices or customer expectations).

The point being, that an organisation may choose to not comply with certain aspects that they feel are not worth doing so.

Another point is, that we comply, not because we have to do so, but because it ensures that our organisation will exist in the future, and successfully so...



So why's a product guy talking about compliance?

The reason I started to think about compliance deliberately is that when I started working with my current team on an Edtech innovation product, I was worried about the compliance impact if compliance were badly done:

The product has far reaching implications for people's lives and futures from getting a job, a place at university, to getting a VISA - or not - to possibly operating as a surgeon or operating heavy machinery, to making jobs obsolete, to dealing with minors; it is also using loads of PII and technologies like AI/ML. So compliance dragons everywhere...

I was worried that we'd not only be stifled (this being LargeLanguageModel related innovation I needed the team being able to act fast) but that the product might be diluted (this is for an organisation that is traditionally quite risk averse and conservative, and also tries to 'do the right thing' sometimes losing business realities out of sight).

So from day 1 my team and I were thinking of 'how compliance could be done differently', how we could work better with EDI, Risk, Infosec and Opsec, Compliance etc and took a look at compliance in general and our previous experiences and what could be learned from them...

**If you want a single thing to focus on, then it's this: involve compliance early and from day one.** But how do you engage with them, how do you work with them? Let's look at that in more detail...

//

But why am I talking to 'you'? I.e. to product people, software engineers, UX designers - I hope - rather than whip compliance people into shape?

In fact, when I recently gave a shorter version of this talk at DevOps Days Zurich (this version has more juicy - literally eye watering - examples) I was asked by an engineer why they had to care about compliance. Why, they argued wasn't this fed in like any other requirement by the PO.

They kinda had a point and kinda didn't.

The simple answer is that in an ideal world, you'd get valuable requirements, well formed, well articulated, at the at the right time, with no need for involvement of any other disciplines as it always happens with any requirements other than compliance... As if!

But while good teams seem to have quite some control over their product requirements, I feel most teams still don't control compliance requirements as well, leading to the usual issues from bad products or having to retrofit stuff at late state.

But ok, maybe as an engineer you don't care what you implement (I really hope you do) so that argument won't work.

Here is a better one:

Much more importantly, as you'll see shortly, a key characteristic of compliance requirements is that they are less like product features and more like operability or certain infrastructure requirements in the sense that the way they get approached and implemented impacts how you work and what you can do and design, no matter what discipline you work in.

For this reason, you want to be part of the discussion to provide the best solution for your organisation but also to make your life easier...

This'll become clearer as we go through examples...

DevDays EUROPE CyberWise Con-

# Today

- How to think about compliance
- An approach to 'better' compliance

31  
RUST RATION  
www.bendthelabstation.com

For this short talk I can really only hope to

- shift how you think about compliance
- explain why you should care (whatever role you may have)
- briefly outline a 'better' approach to compliance

If you are interested in this topic, there is a freely available version of a playbook I wrote about how my teams implement continuous compliance available via my website. Link at the end.

///

To ease ourselves into this topic I want to share some of those lessons I learned while thinking about compliance...

Lesson 1

# Compliance will get more complex

You need to proactively manage the constantly changing compliance landscape.

This is where the first lesson comes in:

Compliance is not only painful if badly done, but worse, there is no way out:

**The compliance landscape is getting more and more complex.**

"The [Thomson Reuters Regulatory Intelligence](#) service calculates that an average of 200 international regulatory changes and announcements were captured daily in 2015 and again (thus far) in 2016."

**So you need to proactively manage the constantly changing compliance landscape.**

And you need to have the process and more importantly the mindset to handle this!

### **///notes**

The point I'd like to emphasise is that many organisations and teams are looking at compliance the wrong way: they see the challenge in getting whatever they have done to be compliant.

This is not the challenge, in fact, it gives rise to an anti-pattern as we'll see later.

The challenge lies elsewhere: change and keeping up with change.

You can easily see why we see this proliferation and increase in complexity:

- Customer expectations and what this means for how organisations act and behave

- Complex products / technologies many with increased risks
- Increasingly complex technologies and supply chains and resulting blurred boundaries between stakeholders
- Changing global landscape

Lesson 2

# Compliance is valuable

And the second lesson:

**As painful as it may be, let's be honest, compliance is a good thing...**

**The simplistic way to look at it is to say 'it avoids you being sued', 'it keeps you in business with your banking or medical license'. But that's too narrow a view, we need to think about the wider impact of corporate failures.**



This floated into my inbox when I initially wrote this talk...

Uh oh, this doesn't sound good, let's remind ourselves briefly what FTX was all about:

/////

Source: [theinformation.com](https://theinformation.com) newsletter.

FTX scandal

- <https://www.techtarget.com/whatis/feature/FTX-scandal-explained-Everything-you-need-to-know>
- [https://en.wikipedia.org/wiki/Bankruptcy\\_of\\_FTX](https://en.wikipedia.org/wiki/Bankruptcy_of_FTX)
- <https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/>



Another classic, is the rise and fall of FTX.

Prior to its fall the **3rd largest crypto exchange** by volume (**valued at 32B USD**, trading around **21B USD every 24 hours**) with **1M+ users**. The company went bankrupt when Coinbase (a competitor) published an article about questionable banking practices between FTX (the exchange) and Alameda Research (an investment firm) both owned by Sam Bankman-Fried. At this point (08/2023) the court cases are still to start and some poor finance forensic guys are still disentangling the mess, but at some point it was unclear where **8B USD of client money** had gone (potentially into a mix of trading losses of said client money via Alameda Research and private asset purchases).

Whether 30ish CEO of FTX SBF and the CEO of Alameda Research Caroline Ellison (his ex girlfriend) were out for fraud or just reckless or in over their heads is still in question, for now SBF is awaiting trial, CE pleaded guilty offering full disclosure to avoid up to 110 years in prison.

2025 Update: SBF - 25 years prison, 2 years for Ellison (and other sentences for his co-defendants)

Oh, and there is the minor matter of those nootropics the guys allegedly used to fuel their brains...

**So the question really is, are you aware what the fuck you are doing? And yes, you are responsible!**

#### **//// Notes**

FTX scandal

- <https://www.techtarget.com/whatis/feature/FTX-scam-explained-Everything-you-need-to-know>
- [https://en.wikipedia.org/wiki/Bankruptcy\\_of\\_FTX](https://en.wikipedia.org/wiki/Bankruptcy_of_FTX)
- <https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/>

## FTX drug use

- <https://nypost.com/2022/11/15/crypto-ceo-caroline-ellison-tweeted-about-regular-amphetamine-use/>
- <https://astralcodexten.substack.com/p/the-psychopharmacology-of-the-ftx>
- <https://twitter.com/carolinecapital/status/1379036346300305408>

## Silicon Valley Bank collapse

- <https://www.techtarget.com/whatis/feature/Silicon-Valley-Bank-collapse-explained-What-you-need-to-know>
- <https://www.theguardian.com/business/2023/mar/17/why-silicon-valley-bank-collapsed-svb-fail>

## Credit Suisse collapse

- <https://www.investopedia.com/what-happened-at-credit-suisse-and-why-did-it-collapse-7369825>

## ///Notes

And while this 'lack of control is worse than ENRON'S' (<https://www.ft.com/content/7e81ed85-8849-4070-a4e4-450195df08d7>), there are many other recent examples like this, including, to a lesser degree Silicon Valley Bank, and to a different degree Credit Suisse's collapse that show similar patterns of greed, ignorance and hubris. In fact, some CS analysts were quoted in an article I unfortunately can't find anymore, signing off after CS's collapse basically saying, "Oh well, no harm done. Volatility is good for business."

## // image

Photo by [Isabella Smith](https://unsplash.com/@__isabella__?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash) on [Unsplash](https://unsplash.com/photos/green-trees-near-body-of-water-during-daytime-sNGImLIEZB8?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash)



**Caroline**  
@carolinecapital

nothing like regular amphetamine use to make you appreciate how dumb a lot of normal, non-medicated human experience is

1:41 pm - 5 Apr 2021

602 Retweets 926 Quotes 2,270 Likes 534 Bookmarks

Reply Retweet Like Bookmark Share

photo by Isabella Smith via Unsplash

Lesson 2

# Compliance is valuable (beyond getting not sued)

So coming back to why compliance is valuable: The simplistic way to look at it is to say 'it avoids you being sued', 'it keeps you in business with your banking or medical license'. **But that's too narrow a view, we need to think about the wider impact of corporate failures.**

///

I don't want to out anyone who's still trading crypto so we'll move on swiftly. But who has a bank account, or a pension?

The list of compliance related corporate failures just in banking failures is long from Citigroup and JPMorgan Chase being involved in the fall of Enron (destroying **20,000 employees pensions worth 2B USD**) via Barrings to Lehman Brothers (kicking off a proper **financial crisis**) the aforementioned FTX 'loosing' **8B USD** and Binance, and more recently Silicon Bank Valley (a number of **20B USD** to cover customer deposits by the Federal Deposit Insurance Corporation is floating around - while directly that fund's paid for by the banks, ultimately it's paid by the public as fees) and Credit Suisse. And that's just financial...)

We'll come back to the value bit, but let's look at some further examples of what happens when compliance fails... The point really being the wider impact.



I briefly worked with Greensill right before their fall, and always wondered why a Supply Chain Finance FinTech organisation would need four private jets! My dad, a retired banker, said to me when I was a kid: always look at what cars they drive (or planes they fly, I guess). That says a lot about their attitude...

The story is an absolutely fascinating mess of greed, hubris and delusion, involving the likes of Softbank and Credit Suisse in a dangerously entangled mess where the same organisation appeared as owners/creditors and debtors.

Greensill serviced around 500B USD p.a. in what's called supply chain finance, usually a low risk mundane business. The idea is that for a fee an intermediary takes over buyers' debts thus settling payments earlier and creating liquidity. Greensill, together with banks like - of course - the late Credit Suisse, created products for investors to finance this debt. It all fell apart when one of Greensills re-insurers became concerned about inadequate business practices and didn't renew their insurance policy, which led to other partners getting concerned about risk (e.g Credit Swiss freezing a 10B fund), and Greensill filed for bankruptcy in 2021.

To be fair, even with the few bits I saw of Greensill, I felt that there were a load of spreadsheets and manual processes for a FinTECH company.

As to the impact of the collapse: At some point it was suggested **50,000 jobs** might be at risk. As well as the damage in funds like those run by Credit Suisse, the UK taxpayer may be on the hook for **millions in debt guarantees** offered in the coronavirus crisis. German municipalities who deposited with Greensill Bank in Germany, a key element of the Greensill financing arrangement, could lose up to **EUR500m in uninsured deposits**.

### **///notes**

"Greensill Capital needed the insurance to back \$4.6 billion it was owed by businesses around the world, and without it 50,000 jobs would be in jeopardy, they said."  
(<https://www.nytimes.com/2021/03/28/business/greensill-capital-collapse.html>)

///

<https://www.instituteforgovernment.org.uk/comment/greensill-saga-tougher-financial-regulation>

[https://en.wikipedia.org/wiki/Greensill\\_Capital](https://en.wikipedia.org/wiki/Greensill_Capital)

<https://www.nytimes.com/2021/03/28/business/greensill-capital-collapse.html>

<https://www.bloomberg.com/news/articles/2021-03-11/how-lex-greensill-s-7-billion-empire-unraveled-in-days>

<https://www.theguardian.com/business/2023/feb/28/credit-suisse-greensill-swiss-bank-finma>

<https://www.afr.com/companies/financial-services/greensill-capital-insurer-had-weak-underwriting-20220819-p5bb9h#:~:text=lack%20of%20a%20robust%20buyer,underwriting%20limits%20and%20organisation%20structure>

///image

Photo by [Chris Leipelt](https://unsplash.com/@cleipelt?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/s/photos/private-plane?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)

Consumer fraud

1985, Austria, illegal food additives

**Fortunately no deaths, kidney,  
liver or brain injury, but major  
economic damage**

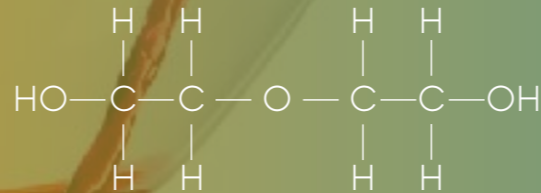


photo by Apolo Photographer on Unsplash

A totally different scandal, but one I remember from being a kid in Germany is the 1985

Glykolwein-Skandal where several Austrian wineries illegally adulterated their wines using diethylene glycol (a minor ingredient in some brands of antifreeze) to make the wines appear sweeter and more full-bodied in the style of late harvest wines.

In the volumes detected in some of the wines glycol can lead to kidney, liver or brain damage, or death even.

All this came to light when a winemaker wanted to tax deduct huge amounts of antifreeze for 'machinery' (although he only had a small tractor).

Fortunately no one died, but there was **multi million Schilling** impact to Austria's economy due to collapse of wine sales.

As to eye watering (literally)...

**///notes**

[https://en.wikipedia.org/wiki/1985\\_Austrian\\_diethylene\\_glycol\\_wine\\_scandal](https://en.wikipedia.org/wiki/1985_Austrian_diethylene_glycol_wine_scandal)

[https://en.wikipedia.org/wiki/List\\_of\\_food\\_contamination\\_incidents](https://en.wikipedia.org/wiki/List_of_food_contamination_incidents)

<https://de.wikipedia.org/wiki/Glykolwein-Skandal>

**///image**

Photo by [Apolo Photographer](https://unsplash.com/@apolophotographer?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/s/photos/wine?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)



Talking about kidneys and other damaged organs: a still (2023) ongoing scandal in regards to ‘artificial tears’ eye drops, lead to “A total of **68 people** in 16 states have been infected with a rare, extensively drug-resistant *Pseudomonas aeruginosa* strain linked to the eye drops. In addition to the **[4] deaths, eight people have reported vision loss and four have had their eyeballs surgically removed (enucleation).**”  
<https://arstechnica.com/science/2023/03/two-more-dead-as-patients-report-horrifying-details-of-eye-drop-outbreak/>

The maker of eye drops (**FDA** approved but in India) had “**a slew of manufacturing violations—from brown slime on filling equipment to a lack of basic measures and systems to ensure sterility**—according to an inspection report released by the Food and Drug Administration. The inspection report outlines eleven "observations" of failures, with specifics. The first is that Global Pharma didn't seem to bother verifying whether its eye drops, which the company claimed were sterile, were actually sterile.”

### **///notes**

<https://arstechnica.com/science/2023/04/fda-details-slew-of-failures-at-plant-that-made-eye-drops-linked-to-deaths/>  
<https://arstechnica.com/science/2023/03/two-more-dead-as-patients-report-horrifying-details-of-eye-drop-outbreak/>

### **///image**

Photo by [salvatore ventura](https://unsplash.com/@salvoventura?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/images/things/eye?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)



Another case, this time in Germany from 2006, and - of course - involving sausage saw 110 tons of rotten meat, some of which was more than four years out of date, turned into meat products to be then soled to consumers in Germany and the EU (UK obviously then still being in the EU). The main suspect (a Munich wholesaler) committed suicide.

///

Obviously the list is much longer, and that without going anywhere near thinks like **data privacy** (like, say Tesla's recent privacy hiccup with data labellers reviewing footage of the cameras on and around the cars (including when parked) and promptly turning them into memes and sharing them with colleagues when something interesting happened, for instance a naked guy walking (in his garage I imagine) towards his car...)

And that's just one of the more funny (nevertheless concerning) data breaches...

#### **////notes**

Note that in this specific case the meat was sold to fastfood chains (e.g kebab), but that this was just one case in a series of similar scandals affecting meat products in general.

///Meat

<https://www.dw.com/en/rotten-meat-scandal-raises-stink-in-germany/a-2760787>

<https://www.spiegel.de/international/rotten-meat-scandal-german-meat-distributor-hangs-himself-a-435457.html>

[https://en.wikipedia.org/wiki/List\\_of\\_food\\_contamination\\_incidents](https://en.wikipedia.org/wiki/List_of_food_contamination_incidents)

[https://en.wikipedia.org/wiki/Category:Food\\_safety\\_scandals](https://en.wikipedia.org/wiki/Category:Food_safety_scandals)

<https://xtalks.com/10-of-the-worst-food-safety-scandals-in-recent-history-3435/>

///Tesla

<https://gizmodo.com/tesla-elon-musk-car-camera-videos-employees-watching-1850307575>

<https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/>

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/>

///image

Photo by [Rich Smith](https://unsplash.com/@richwilliamsmith?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText) on [Unsplash](https://unsplash.com/s/photos/wurst?utm_source=unsplash&utm_medium=referral&utm_content=creditCopyText)

Lesson 2

## Compliance is valuable (beyond getting not sued)

You need to think broader and identify where the real value lies.

Whether you are worried about your pension, your eyes or whether you drink toxic wine or eat rotten meet, **the point of all this is this:**

Yes, being compliant keeps you out of prison and allows you to keep that banking or medical license.

But more so, looking at those pensions, food safety, employee's rights, or medical data: compliance is a good thing. It keeps people honest and in turn 'everyone else' protected.

Of course, as everything compliance can be detrimental if badly done or if used in nefarious ways (we'll get to both in a sec).

But not only does compliance prevent the worst case of fraud, value destruction or malpractice (you may not care), but your customers do: for instance customers may pay a premium for us being 'compliant' not only with statutory requirements, but also things they deem valuable, such as voluntarily adopted requirements that may lead to a B-corps, or (more controversial) Stonewall 'seal of approval', or not using slave labour somewhere abroad.

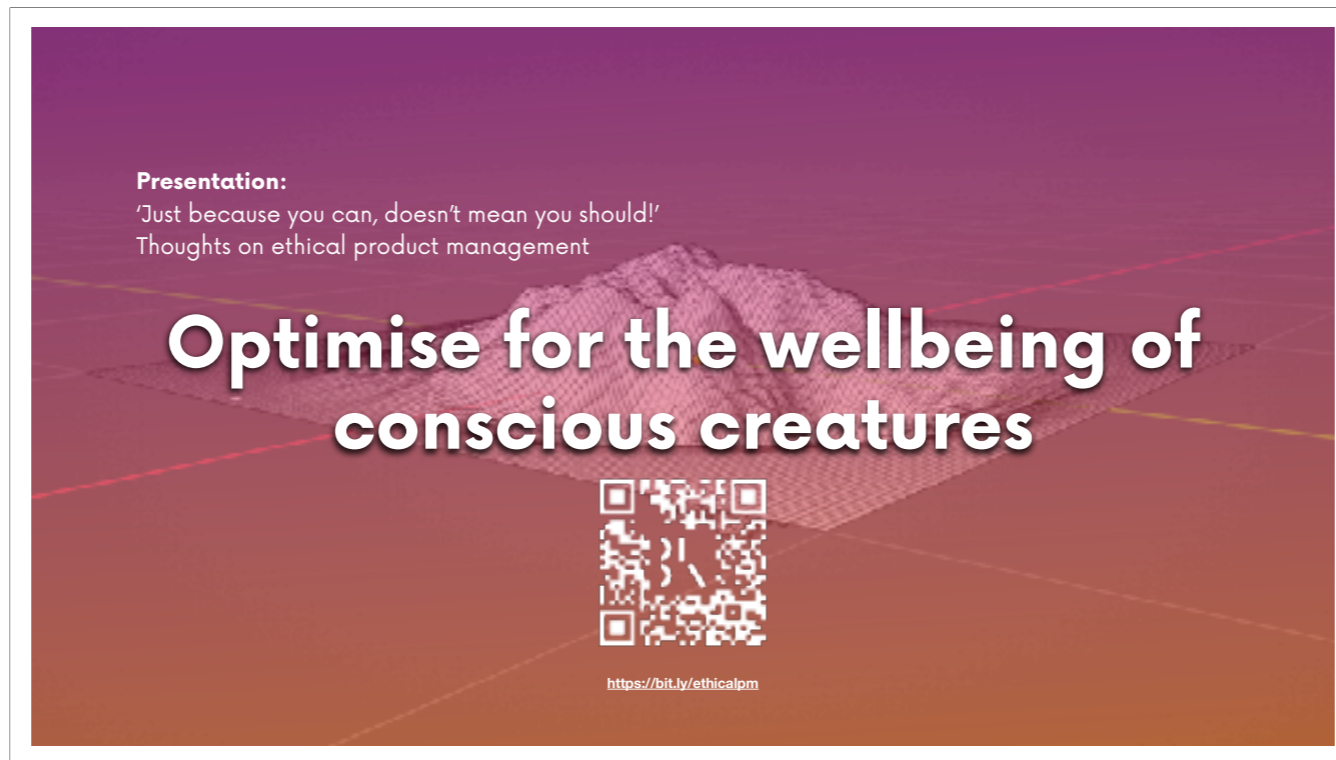
It's important to recognise that compliance is not only about statutory (mandated) requirements but also those we deem valuable and freely choose to comply with.

**You need to think broader and identify where the real value lies.**

### ***///Notes***

<https://ca.indeed.com/career-advice/career-development/why-compliance-is-important>

<https://www.mckinsey.com/industries/financial-services/our-insights/the-case-for-compliance-as-a-competitive-advantage-for-banks>



Which raises an interesting point: What is a good corporate citizen?

What should you comply with - say beyond those statutory requirements?

//

If you are interested in this, you may want to check out a talk about Ethical Product Management I gave at Product World earlier this year (link later).



Here is such an example.

Just because there are statutory compliance requirements, doesn't mean they are 'good' / or ethical.

So the you may also want to ask the question: What do you NOT comply with? And if you don't, can you play?

As example, China is an environment where compliance is NOT optional and where compliance, I'd argue is questionable in certain areas. Sure, social credits might drive positive behaviour shift, but they also might (and do) drive discrimination, also, 'cleansing' language might be seen as good if it is about pornography some might argue, but what about the 3 forbidden Ts (Tiananmen, Taiwan, Tibet) and the resulting rewriting of history?

//

If you are interested in what the Chinese Cyber Security Regime means for companies operating in China or with China, check out my podcast where I discuss this with a specialist in this domain.

<https://www.theburnup.com>

//

Which then brings me to the third lesson...

Lesson 3

# Compliance is optional

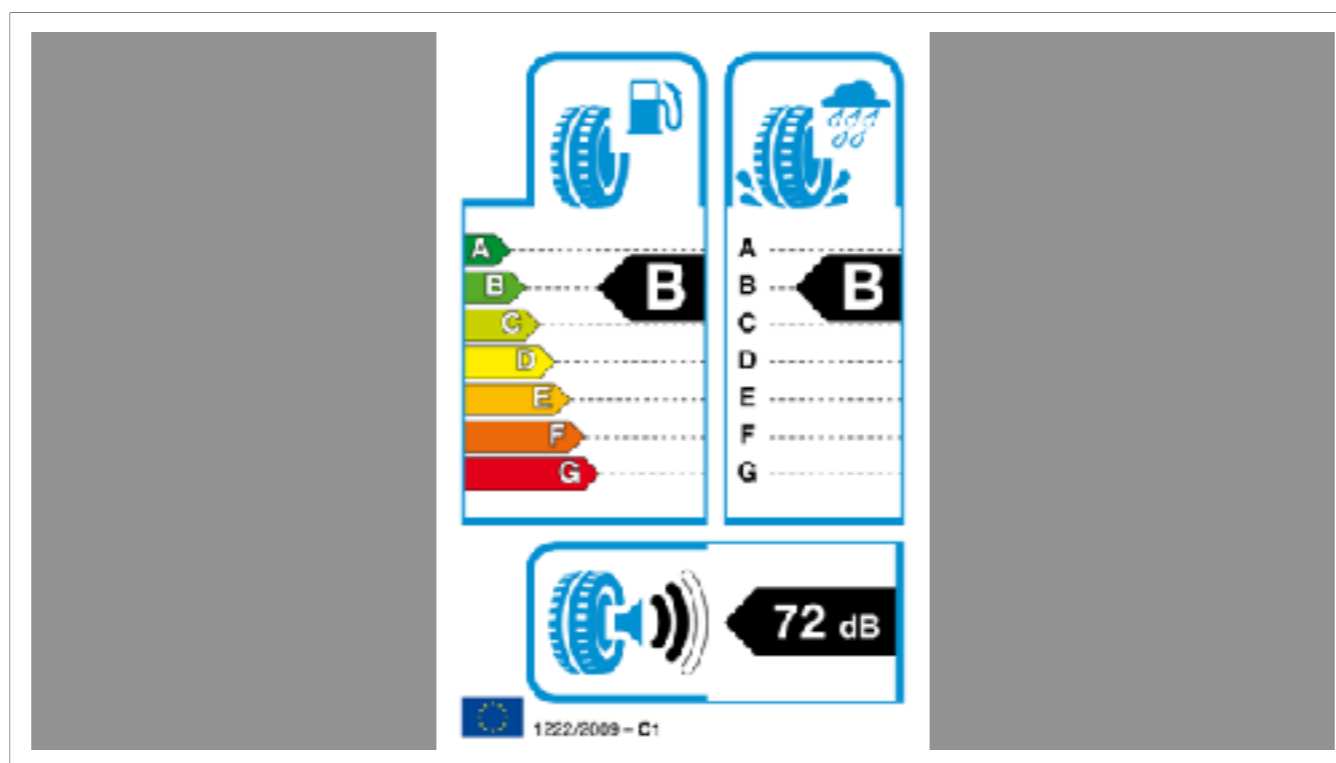
Have a clear stance on value and risks.

## **It is your choice to comply.**

As an organisation (and individual) we need to have a stance on which expectations to comply with and which not. This will be driven by values and principles, or organisational goals, our appetite for risk and 'punishment', and the arena we want to play in (see the previous slide).

We may choose to comply with implicit customer expectations to avoid social media backlash, but we may choose to not comply with explicit SEC regulations if the cost of paying the penalty is less, then say, the up in share price we have affected by writing that illicit tweet. Not that any CEO would ever do that :)

**As with risks we need a clear stance where to play and where we won't.**



On one of my previous projects some time ago, we had to plaster these, and other emissions related disclaimers all over the clients website: not only did the designers rebel, but we found - through user testing - that the amount of smallprint (not necessarily their content) impacted sales negatively, but more so, confused customers so they were none the wiser (negating the intent of 'informed consumption' of this regulation).

Add to this that the regulation was new, purely defined and even less understood, our project sponsor went against demands from legal who wanted these all over the place, and instead asked us to design this in an informative and less intrusive, sensible way. His point was: "No one knows what the right thing to do is, let's do what feels right (in spirit), let's see what the competition does, let's see if someone gets sued. And if we get sued, it's in the 10s of thousands, which is easily balanced with not losing sales..."

This may sound cynical, and I'm certainly not advocating skimping on compliance, BUT if you think about it, it makes business (and compliance) and user sense, as it allowed us, over time to learn, and optimise the display of this type of information.

Ultimately no one got sued, customers were better informed, and we sold product...

Lesson 4

# There is not 'one right way' to be compliant

Define desirable outcomes, then find the best way to be compliant.

Which is related to the final lesson:

**There is not 'one right way' to comply**

While some regulations might be highly prescriptive, many are not, and the **trend (certainly in Europe) is towards regulations that are 'in spirit' rather than 'in word'**.

I have spoken to a friend who's helping a bank become 'digital'. A myth he had to battle was that banking regulations would not allow CI/CD: Separation of responsibilities and all that. So their idea was: developers code (and have no access to prod), ops deploy to prod (and make any last minute changes - on prod). I have issues with this... Anyone else seems something wrong here?

Let's look at what the regulation is about: Avoidance of fraud, minimising the opportunity for collusion of bad actors in dev and ops, in this case. The above approach does do fuck all to prevent this type of fraud. So rather than follow some misguided prescriptive implementation, what you want to do is look at the goal of the requirement.

If you do this, you'll see that you can perfectly, in fact better, mitigate this through CI/CD: no manual access to prod at all, for anyone, full automation, infrastructure as code, dual actors (code - review/deploy) and highest degrees of automated tracing and auditing.

**So, define desired outcomes, then find the best way to be compliant in that context.**



So here is your take-away:

I'm not concerned about that certification you need as license to operate. Everyone gets that. But, if you only focus on not getting sued or not losing that license, you are missing the point entirely:

DevDays EUROPE CyberWise Con-

Getting compliance right matters, it means

- **value & quality** (product)
- **at pace** (delivery)
- **solid compliance** (operations)

31 R+ BUI F H RUST RACTIC M www.beandflobstraction.com

Good compliance means

- Stakeholders (customers, clients, etc) get the product (and compliance) value they deserve (rather than just compliance box-ticking or a product compromised by compliance requirements) and as we have said there are various 'types' of value connected to this that an organisation can realise
- You can deliver quality at pace (rather than being stifled)
- You'll have solid compliance operations that can keep step with the fast changing compliance landscape and react to any issues and changes

///

Coming back to my much earlier point about why you should care and why you want to be part of the discussion, this is it. You might not care about the specifics of the wording on a T&C page (and that's ok) but no matter what job you hold, you do care about the process and tools that compliance force on you as you deliver :) So you want to be part of it, discuss, challenge and advise. **And as we'll see in a minute, cross-disciplinary collaboration can do magic for compliance.**

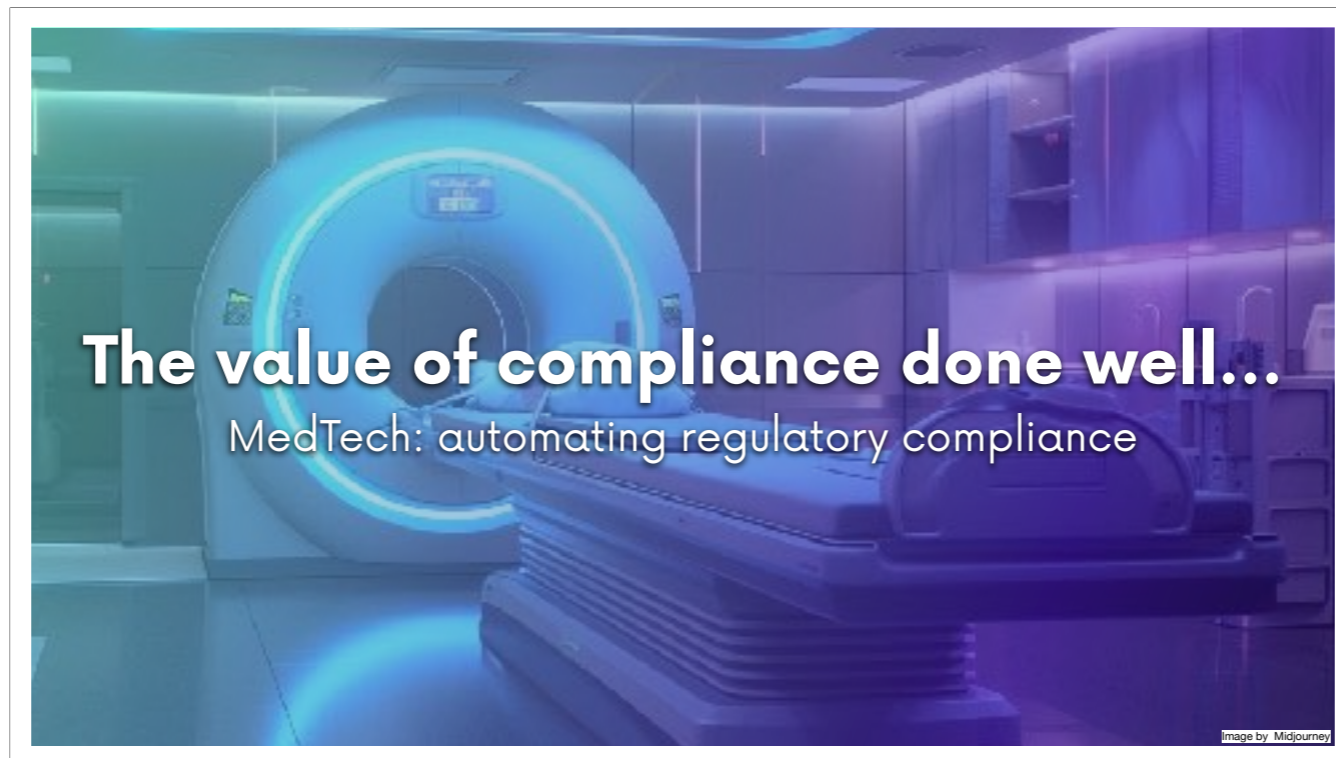
///notes

<https://www.mckinsey.com/industries/financial-services/our-insights/the-case-for-compliance-as-a-competitive-advantage-for-banks>



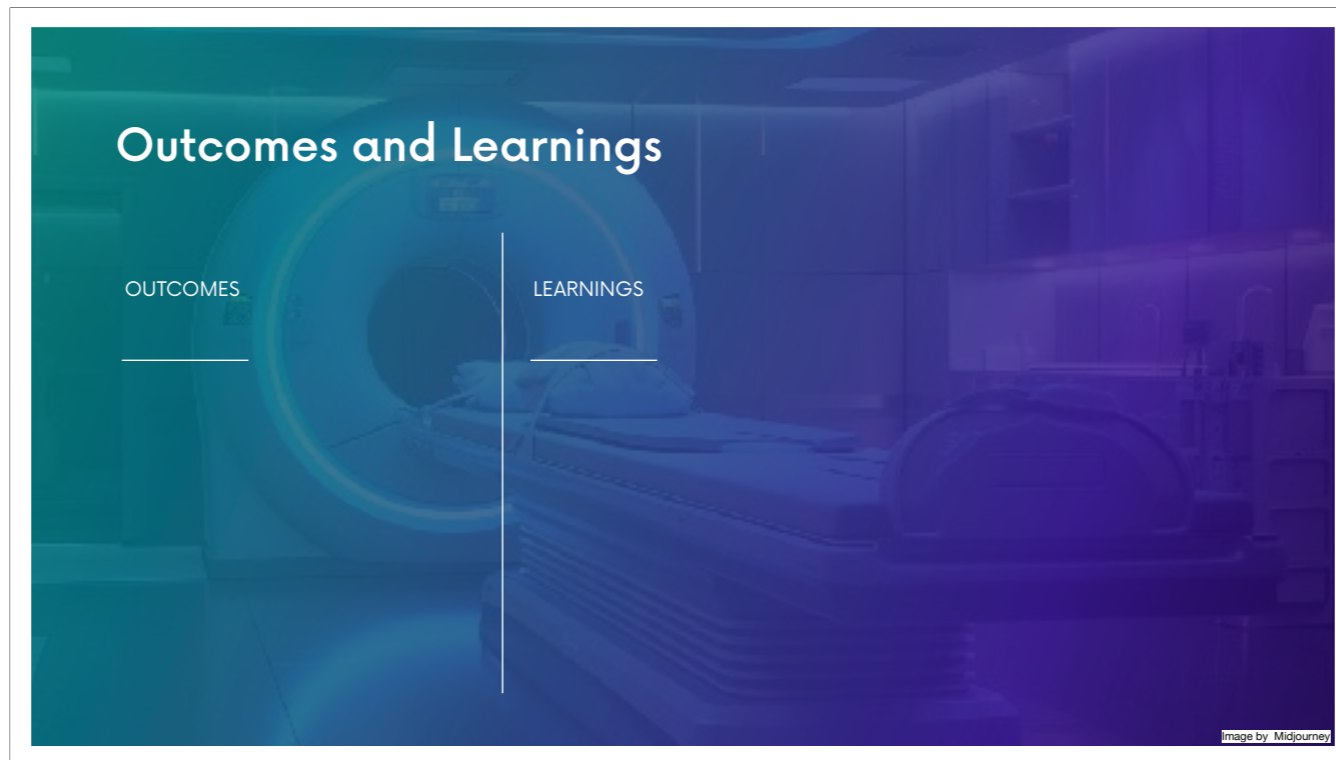
So arguably your entire business' sustainability ultimately depends on how well you handle compliance.

Turning it on it's head, there is competitive advantage in doing compliance well.



Imagine a producer of medical devices company wanting to move the app running on their CTs and MRIs into the cloud and towards CI/CD. One reason being speedier feature delivery. When analysing their value chain they realise that the biggest impediment is their compliance certification process, where for every 3-6 month release hours and hours are spent manually creating documentation and release notes so that in case anything goes wrong the company can demonstrate how they have mitigated risks.

Through close collaboration with the medical regulator as well as the compliance department, but also DevOps engineers, risk and product people the organisation is able to move all compliance concerns into the delivery pipeline, allowing risks to be identified and logged as stories are created, and these automatically linked to features, ACs, test cases and test results, ultimately all nicely packaged up in a single document which can be submitted for certification.



### **So what are the outcomes of this?**

1. Reduced compliance effort and duration down to mere hours and consequently allowed for bi-weekly (or more frequent on-demand) releases, but more importantly massively increased the reliability of the compliance documentation and overall process.
2. Consequently: Major increase in throughput, reduced cycles times, increased quality and reliability, faster learning. Happier teams.
3. Owning this capability the organisation would be able to position this as competitive advantage and make this part of their comms to ultimately have one of the most successful MedTec IPOs ever.

### **So what are the learnings form the case study?**

1. Yes, we an apply agility in MedTech
2. Carefully assess your 'goal' (are you solving the right problem? Or rather: What is the problem to solve?)
3. If you start with the users(and look at them holistically, i.e. internal / external, primary / secondary) you may even solve the right problem :)

And in this specific case

4. Identify your bottlenecks (following lean / flow theory: resolve downstream bottlenecks first)
5. Consider innovation across your entire value chain
6. Cross-functional collaboration is important at all stages
7. Iterative design and delivery provides value early and closes that fast learning / feedback loop
8. You really need to innovate culture, process, and tools.

///

Note: this took time (3 years) BUT value was released as per our roadmap 3 months in.

The big point being: you can work incrementally, at pace, 'agile' even in highly regulated environments.

# Outcomes and Learnings

## OUTCOMES

---

- Efficiencies
- Increased pace & learning
- Successful IPO

## LEARNINGS

---

- Agility works in regulated industries
- Solve the right problem
- Understand your users
- Optimise for flow
- Collaborate cross-functionally
- Iterate
- Innovate across culture, process & tools

Image by Midjourney



Further detail on this example and the specific value of your delivery pipeline in regards to compliance.

DevDays EUROPE CyberWise Con-

# How do we get there?

Playbook



<https://bit.ly/compliancebydesign>

BEANSTRACTION  
www.beanstraction.com

So how do we work towards this 'good' approach?

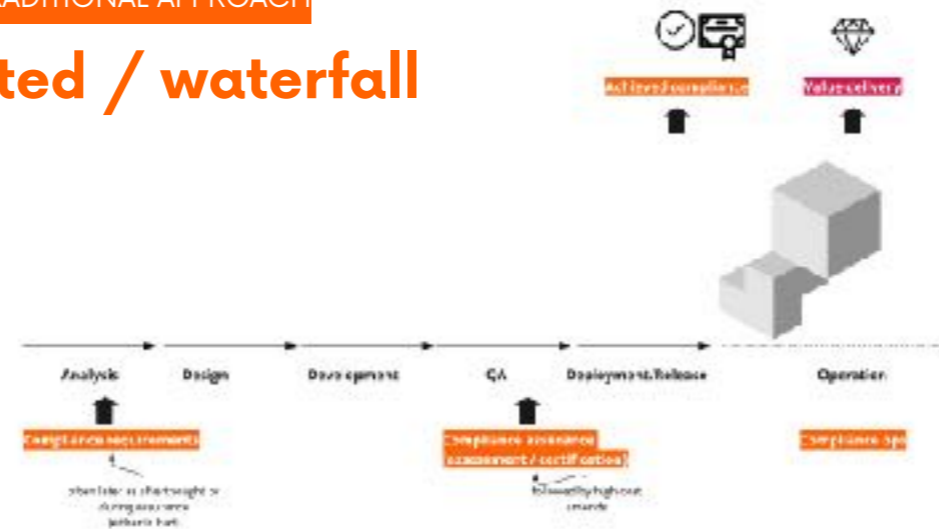
There is an early version of a playbook I wrote with more detail, but I'll give you the gist.



To the observant amongst you it should be obvious by now that (and why) the traditional compliance approaches cannot work:

## THE TRADITIONAL APPROACH

# Gated / waterfall



I assume I'm preaching to the converted. So I'll keep this brief.

In the classical compliance approach (even if the rest of the process is agile) we get a batch of compliance requirements sooner (or rather later), build the thing, then go through compliance assessment and certification as required, then, after having made the needed (often high cost) last minute changes, and often compromised effectiveness and quality of our product, go live, and operate the product and compliance with whatever features resulted from those requirements...

//

The problem you get is the same as with any non agile process:

- over-design, missed requirements, no opportunity to learn
- Reduced pace and quality

But coming back to my earlier points, due to the nature of compliance, we see a three-fold impact:

- Compromised compliance and design of the product
- Negatively impacted delivery (pace)
- Mediocre compliance operations (tools, processes, reliability and ability to react to change an issues)

DevDays EUROPE CyberWise Con-

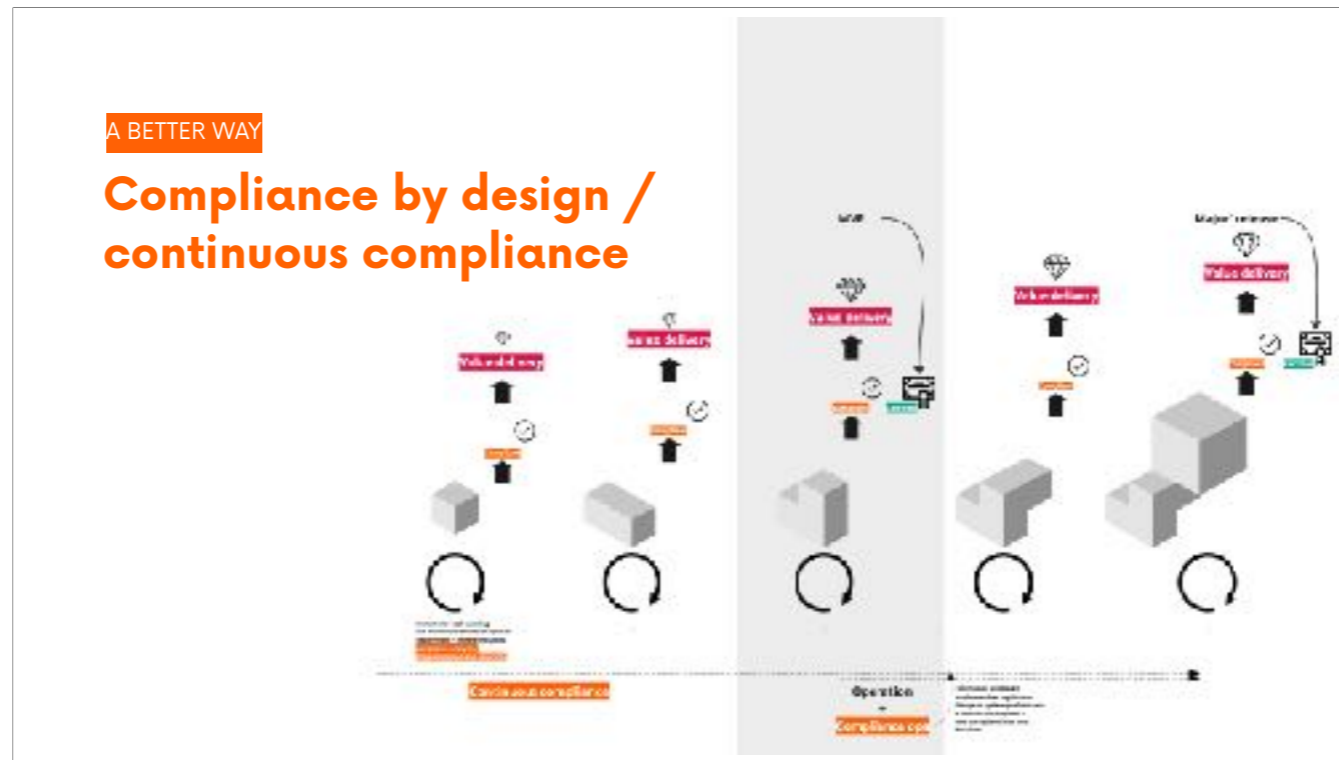
Shifting to a better model:  
**Compliance by design /  
continuous compliance**

BEHOLD INFRASTRUCTURE  
www.beholdinfrastructure.com

So how do we do this differently?

You could see this coming, right?

We do, what we have done with agility, DevOps, CI/CD for other areas of our development lifecycle.



### So moving towards a model where we:

- Deliver in increments, including increment relevant compliance requirements
- So that we are in a constant state of compliance and can compliantly release at any point in time (think continuous integration, deployment and release or release on demand)

I should say that we may include major compliance assessments and certification processes or, for practical reasons allow them their own cadence on top of this 'continuous' process (for instance as part of an MVP or other major release).

Post release we will have compliance operations to monitor for changes in compliance and also monitor system performance so we can take necessary action as part of upcoming iterations.



**To make this Vision reality, we need to do two things**

- **a shift in culture and mindset to how compliance operate and interact with other teams towards continuous close consultative collaboration**
- **a shift in process as to extend the involvement of compliance across the entire value chain, especially making it a continuous aspect of agile design and delivery**

Let's look at these briefly...

# Culture

## Work towards a culture of

What you need to work towards is a culture of:

- Appreciating change (not preventing it)
- Continuous, cross-functional, JIT, consultative collaboration

This means a shift from rare involvement, handovers and 'keep at arms length' to integrating compliance into the delivery team, and appreciating compliance concerns from day one.

On the other (compliance) side it means taking a pragmatic, consultative and supportive stance as 'just yet another' stakeholder who is part of solution design (rather than a gate keeper, final approver or 'the department of 'no'').

- Managing compliance proactively (rather than focusing on mere prevention)

Compliance must be intrinsic to product design, not an afterthought or add-on.

- A shift from compliance in principle to compliance in practice - from 'prescriptive' to 'in spirit'.

By this I mean that the traditional (US favoured) approach of box ticking and compliance with (overly) prescriptive regulations focused on narrow solutions is no longer sufficient. We need think of compliance 'in practice' which means to find the most fitting solution in light of desirable outcomes, principles and a meaningful interpretation of ethics, values and principles.

**Collaboration and collaboration** clearly being the most important ones.

## Work towards a culture of

---

- Appreciating change
- **Continuous, x-functional, collaboration**
- Proactivity
- Compliance 'in spirit'

**Remove 'gates' as much as possible.**

## Build on solid foundations

---

### To enable the require cultural shift, ultimately we need

- Clear values, i.e. we need to define what is important in regards to compliance.
- Aligned objectives and incentives across teams and departments.  
Have shared product objectives and goals to avoid conflicting goals.
- Culture of autonomy and empowerment

## Build on solid foundations

---

- Clear **values**
- Aligned **objectives** and **incentives** across teams
- Autonomy and **empowerment**

**Focus on reducing conflicting goals, permission and empowerment.**

## As management

---

What management / leadership need to do

In a leadership or management role you will NOT want radical, mandated change through which you would be at risk of ending up in bureaucratic hell or a situation of window dressing without actual valuable change.

Instead, approach a mix of top-down enabled bottom up:

### **Identify 'wiling' collaborators in and for compliance**

As with the entire process, start with a smaller group of to affect the change, and work 'outwards' from there. While you will need buy in from compliance 'leadership' the champion could be anyone in the compliance team.

### **Empower, give permission (to work in different ways)**

Provide shared, non conflicting goals, align outcomes with desirable goals and ensure they drive change towards this new compliance culture and process. Reward the right behaviours, e.g. learning, the ability to react quickly and long-term improvement rather than punish one-off failures. Avoid rewarding of behaviours that lead to defensiveness, box-ticking or window dressing.

**Align goals and incentives.** Make sure that they drive desirable outcomes, do not conflict. Make all stakeholders responsible to drive towards the same goals, **manage tensions but avoid conflicts.**

**Identify an exemplar 'team'**

Task this team with delivery of a product or service, and, as part of this, and let them explore and implement this new compliance approach. Allow the team to iterate. Most importantly, provide servant leadership to remove blockers, provide guidance and facilitate where the team struggle internally or at their interface with external stakeholders.

**Foster radiation outwards and diffusion of 'what works well'**

Take things that work well, and use them to affect change across the wider organisation, be this by transfer to other teams or outwards to other departments or upwards to management and leadership.

## As management

---

- Identify 'willing' **champions** in compliance
- Give **permission** to compliance to 'do things differently'
- Align conflicting goals and incentives: **reward behaviours that drive desirable outcomes**
- Identify an **exemplar team** and 'let them get on with it'
- **Foster adoption** of 'stuff that works' across the organisation

## As team

As team you will want to

### **Include compliance from day 1**

Only by making compliance part of the team (and this most often does not mean full-time) can we achieve proper continuous compliance (and / or work towards this goal). This can be the 'champion' mentioned earlier or another 'willing collaborator' identified and supported by them.

### **Define the scope of compliance and the stance on risk you want to take.**

This, of course must be in line with the formal stance the organisation takes, and dependent on where the organisation is, may mean following what is there, challenging it or defining it from. This must cover the regulations, principles, expectations (formal and informal, internal and external) the team needs to comply with.

Note that there might be items set and defined at organisational level, but also very specific ones, applicable to the team / initiative only.

*As a bank all teams will have to follow certain regulations, e.g. what is defined in the FAS handbook. When building a payment gateway for this bank, you'll have to consider additional specific regulations, such as KYC, PCIDSS, IAS for finance, credit card handling and accounting, it will also mean compliance with privacy regulations like GDPR or other, WCAG for accessibility, consumer protection, and advertising and marketing best practices. At organisational, there might be additional regulations related to inclusion, sustainability or anti-slavery which the organisation and or their customers may find valuable to 'care about'.*

### **Define ways of working**

This will include a number of tasks such as identify / defining

- Who relevant compliance 'stakeholders' are
- How they will be engaged with - or rather fit into the team - and how collaboration will unfold.

- What top level compliance activities are required
- When in the overall process each compliance aspect will be relevant (remember, early and continuously is generally best)
- What tooling maybe required or valuable

We don't have to go over-board with this, too early, but can approach this in agile / lean manner. Frequently a compliance charter, or making compliance aspects part of the team charter is more than sufficient.

**Get on with it, incrementally.**

Don't take on the world. Get management so facilitate and unblock where you get stuck. Communicate and transfer outwards where things work well. Do all this in steps, approach it incrementally.

Small improvements that are actually enacted and delivery value are better than overly formalised processes that are only box ticking exercises.

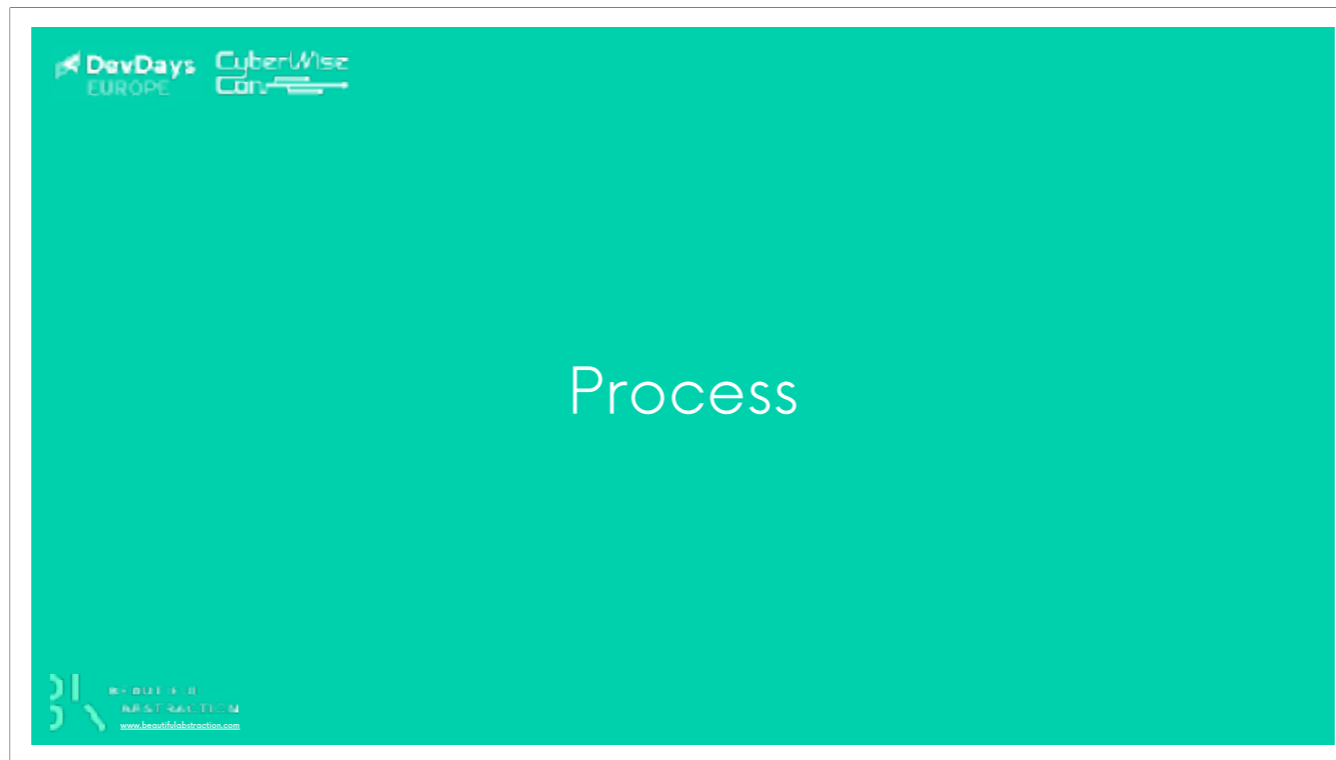
//

*I have worked on projects where stakeholders from the legal team - yes, that is lawyers - were part of the deliver team, helping define complex legal aspects of tokenomics (how can we avoid this being a security) or land- and ownership rights for carbon trading solutions (if you own the land, do you own the trees? And if you do, do you own the carbon sequestered in them?). You can imagine how important it is to have these onboard from day one, actively taking part in solution design, especially where you head towards new grounds and get into the territory of legally undefined areas of innovation.*

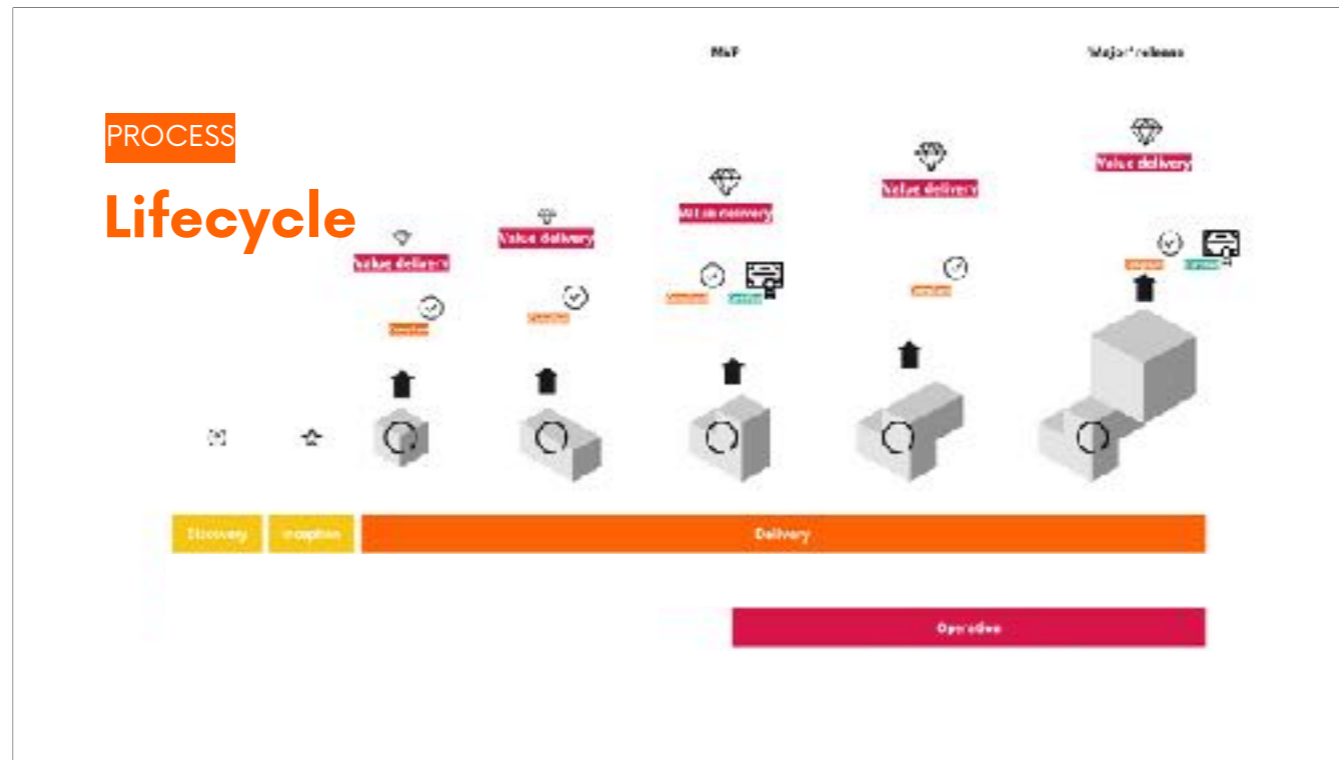
## As team

---

- **Include compliance** from day 1
- Define **scope of compliance** (which regulations, principles, expectations?) and **stance on risk** (what's too risky?)
- Define **ways of working**
- **Get on with it, incrementally and evolutionary** (compliance features and process)



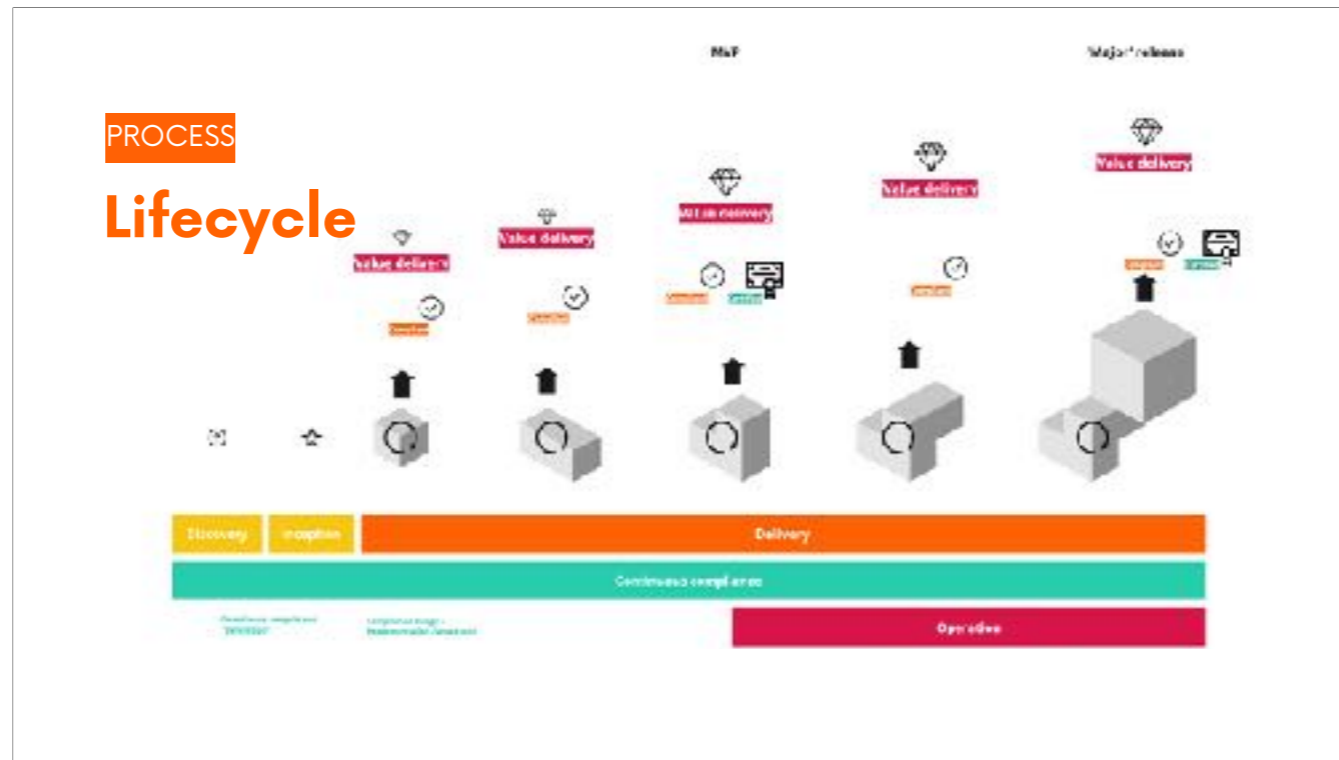
What does this mean for our process of actually delivering a process or service?



The way I think about it, we have 4 (usually overlapping) phases:

- Discovery where we define what to do
- Inception where we define how we do it
- Iterative delivery
- Operation

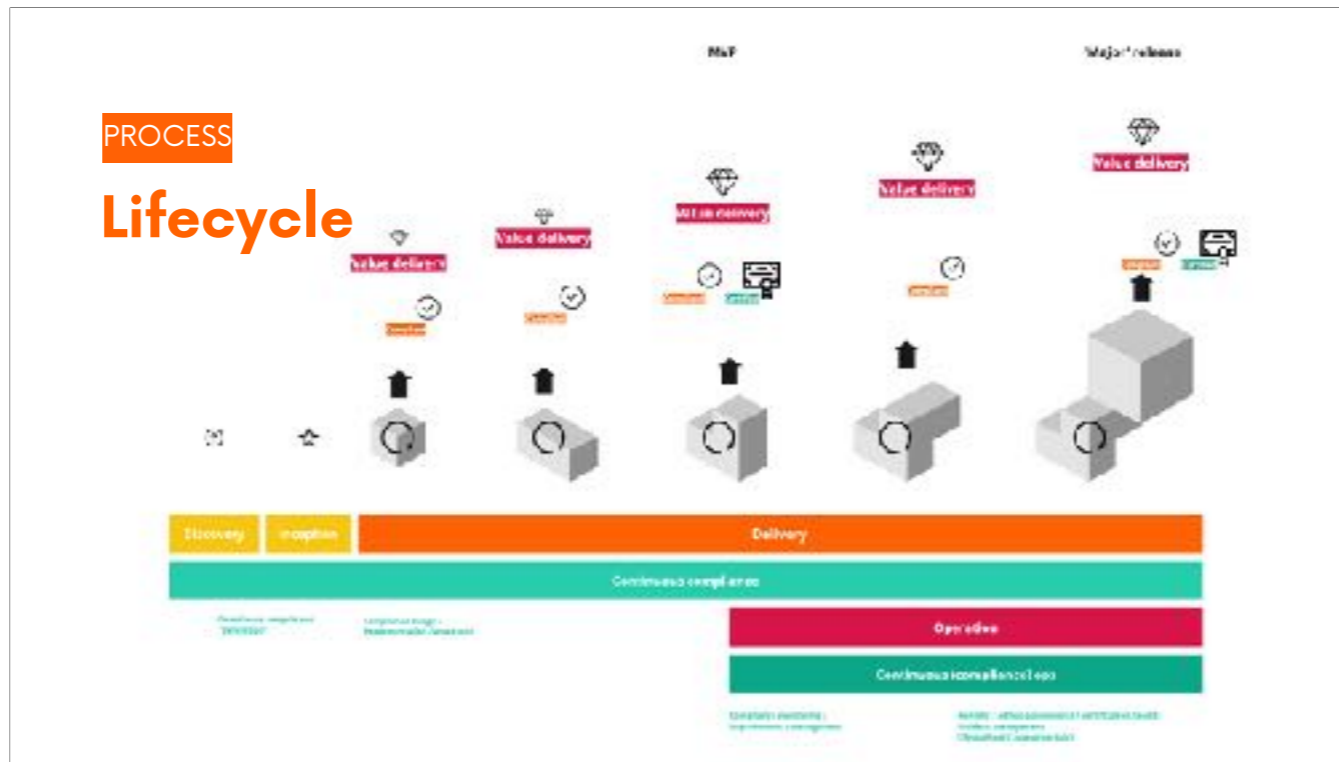
(If this sounds anti-agile, check out my other writing or give me a shout: it isn't)



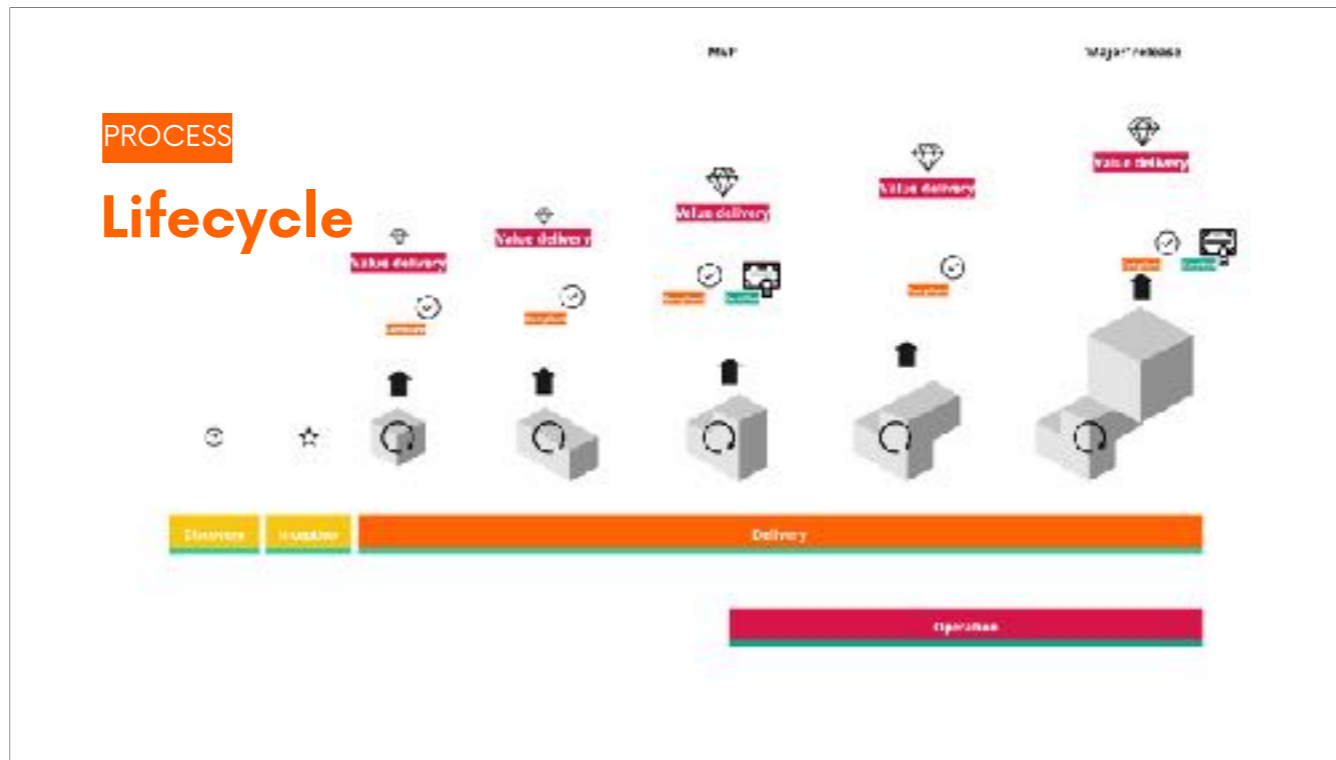
**Onto this, we overlay - or rather include - compliance.**

Specifically this means:

- In the early stages (discovery) we define compliance objectives and key concerns.
- During inception we define our compliance stakeholders, ways of working and top priorities.
- During delivery we analyse, design and implement (demo / validate) iteration relevant requirements, gain increment relevant certification. We also define compliance metrics.



- During operation we monitor compliance, react to any changes (which we feed back into the cycle) and react to incident and requests (feeding learnings back in).



Ultimately we want to achieve embedded, continuous compliance.

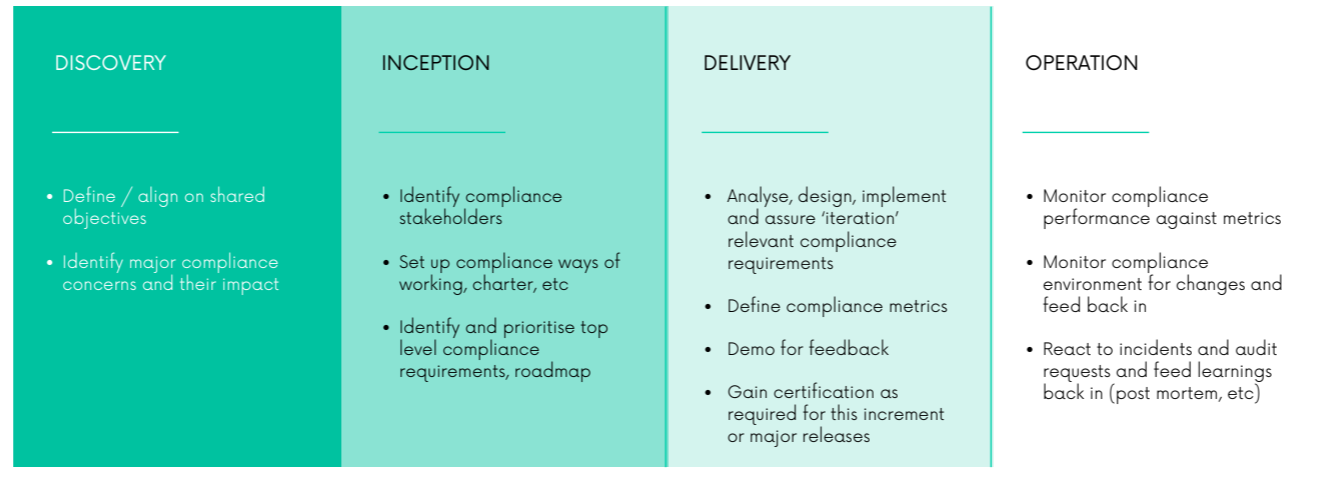
Remember what I said about allowing major certification to run at their own cadence (here as an example for MVP or 'major' releases, or simply periodically - remember, if you get this right, you'll always be compliant, i.e. ready for such assessments whether planned or ad hoc audits).

///

More about all of this in the longer talk and the playbook.

## COMPLIANCE ACROSS THE SDL

# Lifecycle



Again, there is much more in the playbook, but you get the gist.



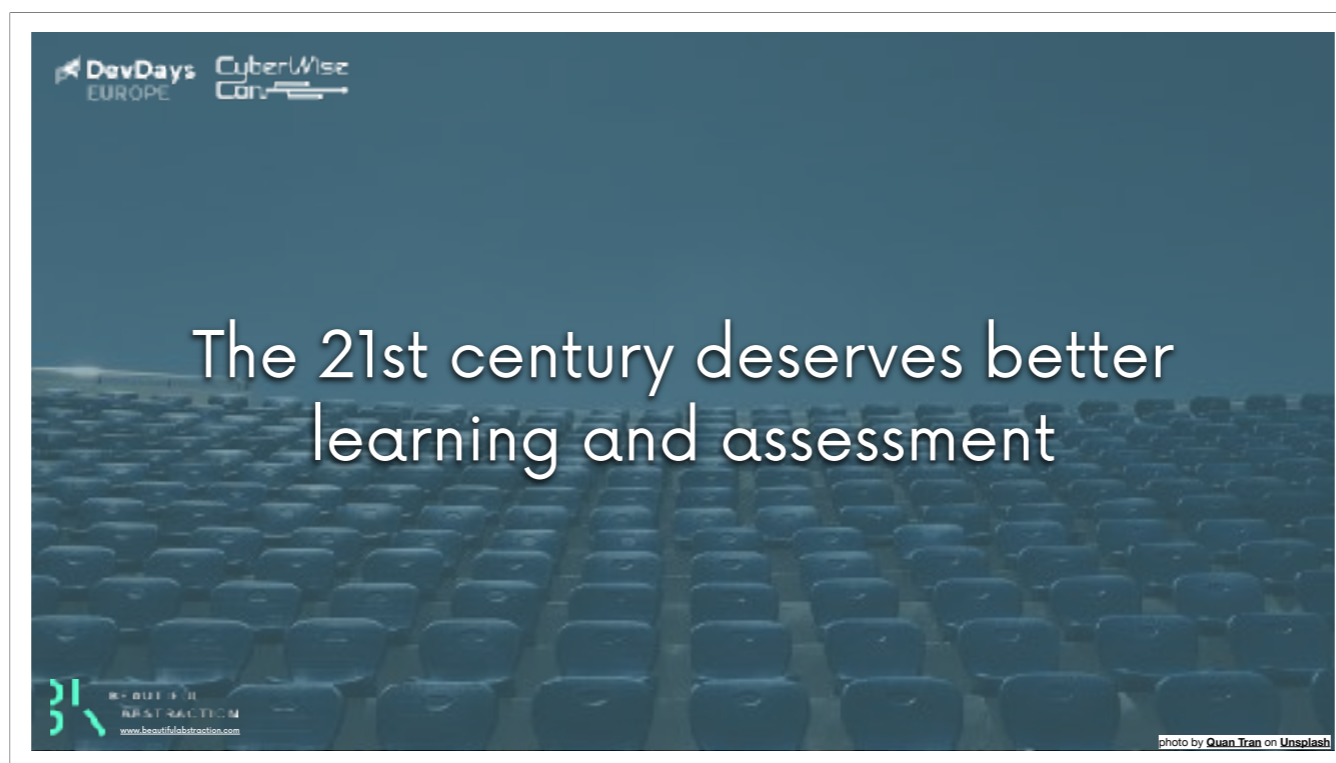
Before we conclude I want to share a very recent example of **continuous compliance** in practice:

My recent client, British Council ([www.BritishCouncil.org](http://www.BritishCouncil.org)), are one of UK's most prominent organisations for global cultural exchange, a big part of this being English language learning and assessment. For instance, they co-own IELTS which is the foremost English assessment / certification that the UK government, universities and other organisations will require from second language English speakers when they apply in the UK (and other English speaking countries) for study, work or citizenship.

As leaders in their field, they are strongly focused on understanding and shaping the future of English teaching, learning and assessment.

////image

Photo by [Ivan Aleksic](https://unsplash.com/@ivalex?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash) on [Unsplash](https://unsplash.com/photos/brown-wooden-table-and-chairs-PDRFeeDniCk?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash)



Traditionally, as many of us have experienced, language is often taught out of context, i.e. we learn on grammar and vocabulary, but not really on how to use language to achieve communication goals.

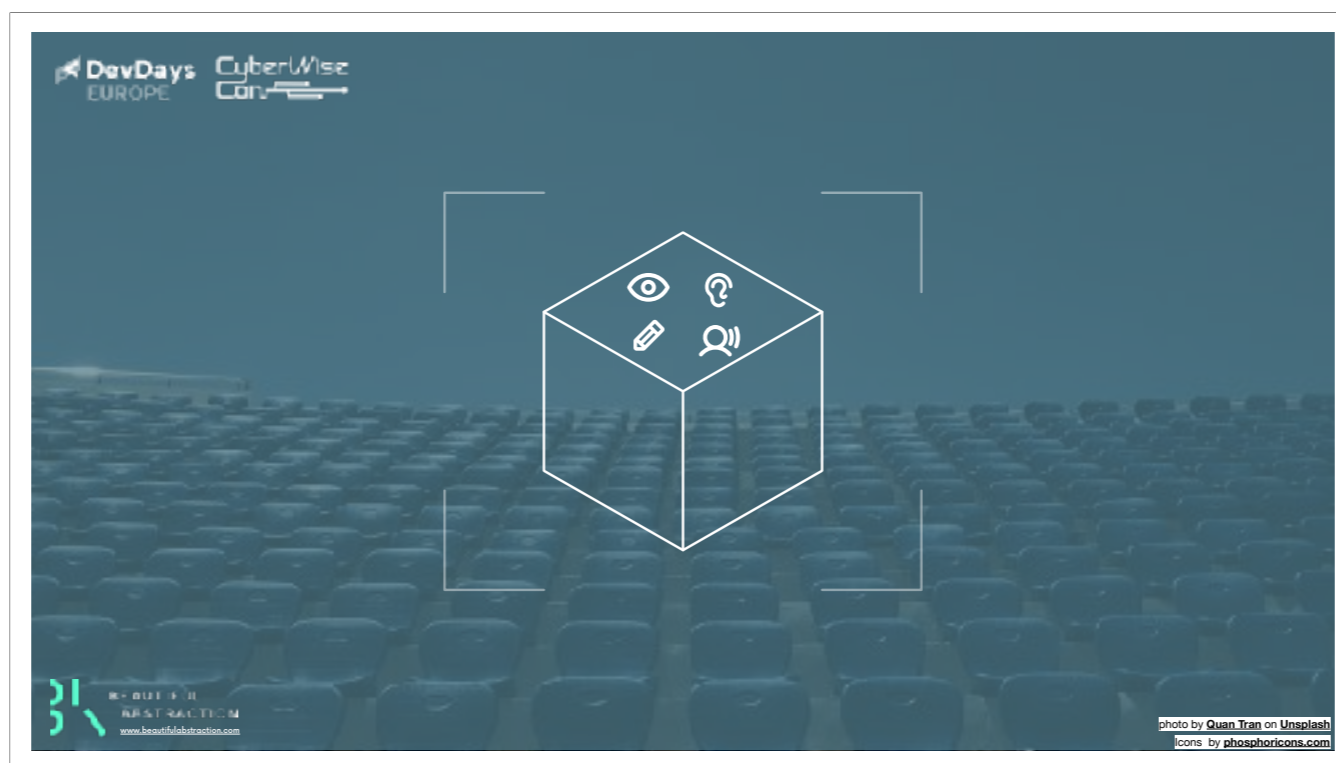
More so, the traditional model of learning, exam, learning exam, rinse and repeat is not particularly useful to foster learner progress nor is it representative of proficiency.

What makes this even more difficult is that teaching institutions find it hard to provide students with the attention and feedback they need, especially where speaking practice is concerned, as this requires dedicated teacher time, and therefore is expensive.

All this means that there is ample opportunity to innovate in this space...

////image

Photo by [Quan Tran](https://unsplash.com/@tranvanvosongtoanquan?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash) on [Unsplash](https://unsplash.com/photos/a-stadium-filled-with-blue-seats-under-a-blue-sky-6Kc77imm5YI?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash)



In a nutshell

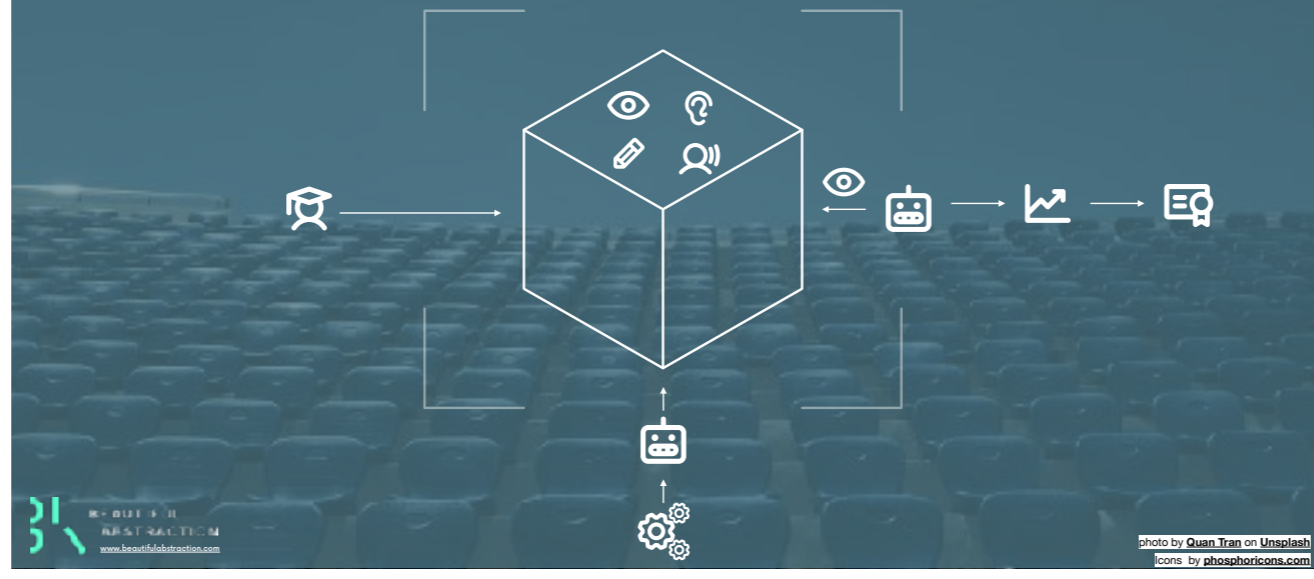
- my team is building an immersive environment
- where students interact with virtual personas (chatbots, if you like).
- while they solve communication tasks
- the system will provide feedback to inform their learning progression,
- and ultimately issue credentials or certification.

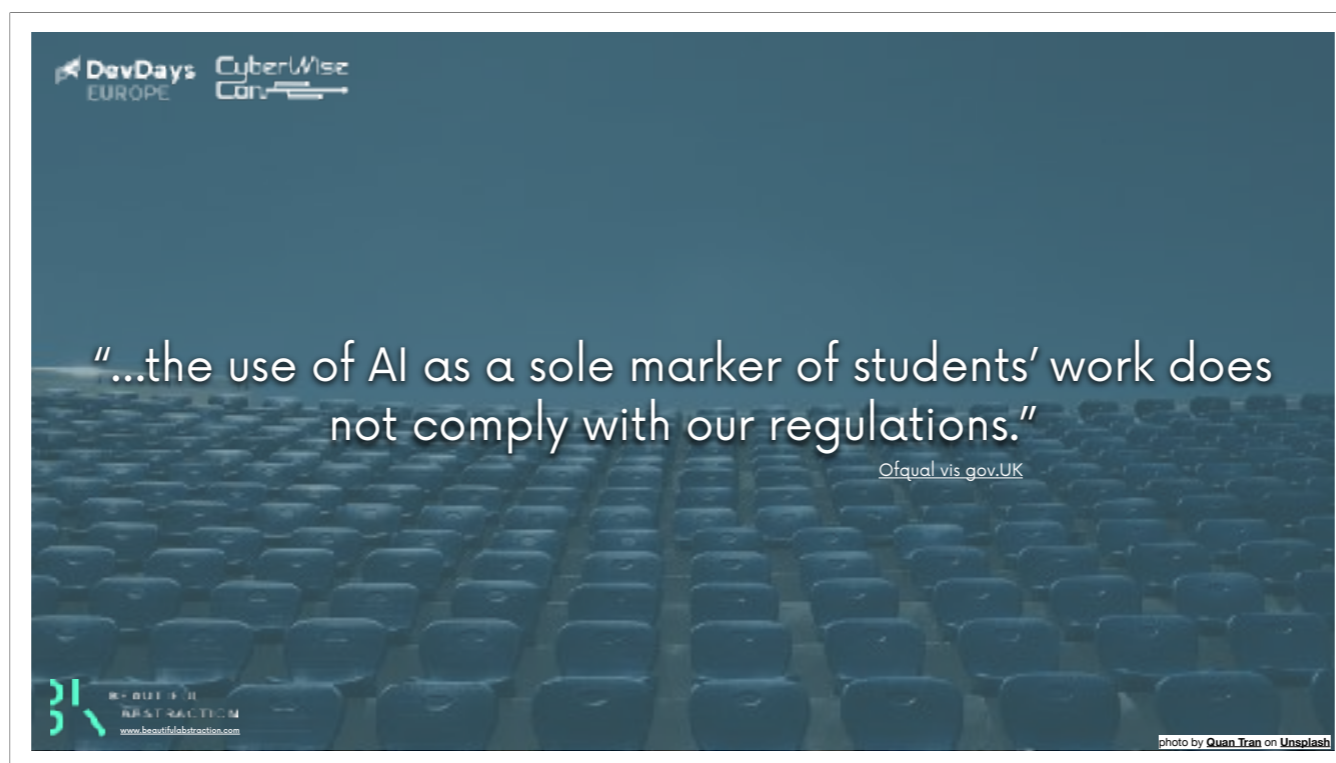
Enabling all this with technology, such as as 'AI' based chatbots and algorithmic assessment allows this to be provided at scale and quality and therefore be made generally accessible and affordable.

////image / icon

Icons by [phosphoricons.com](https://phosphoricons.com)

Photo by [Ivan Aleksic](https://unsplash.com/@ivalex?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash) on [Unsplash](https://unsplash.com/photos/brown-wooden-table-and-chairs-PDRFeeDniCk?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash)





There are many challenges with a system like this, some ethical and related to internal 'policies around things such as EDI, others hard regulatory around privacy, assessment and certifications.

This is one.  
OfQual (Office of Qualifications and Examinations Regulation), the UK regulatory body for qualifications have basically disallowed autoscoring as sole technology in marking decisions (at least for now). They also highlight issues such as bias, inaccuracies and transparency.  
And they are right. The risk of bias is too high for now.  
Even with humans we mark multiple times, move invigilators around etc etc.  
If you think the is not an issue, I'd like to refer you to the ETS 2011 scandal - which didn't even involve 'AI' (details see below).

///source  
EU AI compliance checker  
<https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/>

<https://www.gov.uk/government/publications/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector>

Regulator  
The Office of Qualifications and Examinations Regulation (**Ofqual**) regulates qualifications, examinations and assessments in England.  
<https://www.gov.uk/government/organisations/ofqual/about>

<https://www.gov.uk/government/publications/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector>

"Using AI to mark students' work  
Ofqual wrote to all awarding organisations in September 2023 to confirm that the use of AI as a sole marker of students' work does not comply with our regulations. Ofqual reached this view partly because such use does not meet requirements for a human based judgement to be used in marking decisions. But it is also our view – by virtue of taking a precautionary principle – that the potential for bias, inaccuracies and a lack of transparency in how marks are awarded could introduce unfairness into the system. This would be

unacceptable in the marking process. There are opportunities for AI to complement and quality assure human marking, though further information and evidence will be needed to be assured the use of AI as a sole marker is appropriate in such a high stakes process.

Using AI in remote invigilation

For similar reasons, Ofqual clarified with regulated awarding organisations in December 2023 that the use of AI as a sole form of remote invigilator for student work is unlikely to be compliant with our regulations. The importance of effective invigilation to ensure the authenticity of students' assessment evidence, and prevent and detect malpractice or maladministration is currently best secured by human involvement. Ofqual will keep this position under review in light of further research and evidence."

<https://www.gov.uk/government/publications/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector>

////

/// references

Home office approved EOEIC test delivered by US company ETS (toefl).

Accusation of cheating (2011-2014) against more than 97% / 35,000 students, which led to thousands being thrown off their courses and forced out of the country. It's a story of detention, suicide and debt...

ETS lost their license to conduct secure English tests.

Very complicated case of a greedy supplier not reporting or addressing fraud, while then, once the Home Office started to look at it based on some really fraud cases, being of zealous...

" Digital forensics expert Professor Peter Sommer said: "What seems to have happened is that the voice files became somehow separated from the individuals."

However, it was impossible to verify the files were what ETS said they were because they contained no electronic metadata showing when and where they were created.

"Immigration barrister Nick Armstrong said it would have been simpler for fraudsters to discard all the test entries from the exam hall - including those by genuine candidates - and just upload those from a secret room. The same faked test could be sent for multiple candidates, he believes.

This meant that when the recordings were scrutinised with voice recognition software, people who thought they had passed on their own merits would be wrongly branded cheats.

"

"It is an explanation for why the numbers of so-called fraudulent tests were as high as they were found to be," Mr Armstrong said."

<https://www.bbc.com/news/uk-60264106>

The case continues.As far as I know at lest 3500 students have been cleared so far.

Think of the case of ETS (owning TOEIC and TOEFL) as an example of how high risk in my industry can be: They assessed between 2011 and 2014 around 60,000 foreign students with their TOEIC test which would have granted the students access to universities in the UK.

We do know that there is a lot of fraud and cheating happening, but...

ETS claimed that around 97% were cheating. 60% got their VISAs revoked, had to leave the country, could no longer study.

The fallout were life-changing for many, life-ending for some, and while the test is still around, ETS lost their license to work for the UK Home Office (due to the mess they created)..

But, it was found that when ETS finally provided 'evidence' (audio files of students' performances) these rarely matched the real students: Home office and ETS claim that this therefore was fraud. While students and their lawyers suggest technical issues or maybe fraud (but not by all student, but by someone subverting entire centres and hiding their tracks). Clearly they argue it is unlikely that 97% of students cheat.

It is, however, almost impossible to challenge the home office from outside.

**Note that there was no automated decision making involved. But my point remains, as we possibly would trust an algorithm even more (think post office scandal) than a human process, and that algorithm could assess even more students..**

**This is why we need transparency, and humans in the loop, and explainability, the more we automate systems.**

# Ethics / regulatory areas

- **Privacy** (GDPR)
- **Children's safeguarding** (GDPR / UK GDPR / ICO Children's code)
- **Anti-Discrimination / EDI / Accessibility** (EU AI Act, UK Equality Act, EAA, internal EDI policies)
- **Dark patterns / manipulative UI** (Digital Services Act, Consumer Protection Laws)
- **Transparency and explainability** (EU AI Act, GDPR)
- **Assessment and certifications** (Ofqual, CEFR standards)
- **Cybersecurity / OPsec / Infosec** (various external / internal policy / ISO)
- **Auto content generation** (Copyright Act 1988, EU Copyright Directive)
- **AI application** (EU AI act, internal policy)
- **Monetisation & productisation** (Consumer Rights Act, GDPR, PCI DSS)

photo by [Quan Tran](#) on [Unsplash](#)



There are many challenges with a system like this. Here are the key ethical ones and what we did about it:

- The one that usually first comes up with assessment in general and AI based system specifically is bias and fairness. While important this is something we can mitigate by careful data selection, model training and monitoring.
- What I'm more worried about, with AI systems in general, is whether we optimise them for the right goals: This is much more impactful and harder to get right. In our case: does the interaction teach and reinforce the right things, does the assessment measure the right things. Solid academic foundations, monitoring, longitudinal studies, building for explainability can address this.
- With a system like this, there is also the impact of technology on interaction and what this means for a learners and test-takers performance. The available research is looking very promising: there is evidence that the impact of automation be positively correlated (i.e. students prefer to speak to a machine than to a human (less embarrassment)).
- A very different concern is the impact of the ethics of model training in terms of copyright concerns, impact on workers conducting low level data labelling and cleansing tasks, and energy consumption. Here a considered choice of supplier can mitigate. Evolutionary architecture allows us to benefit from top-of the range services at genesis-level market maturity in the early stages, while being able to switch to more ethical providers in the future. (Imo, for instance we should avoid any models or services by xAI corp.)
- While technology can democratise, and create efficiencies, especially high tech can also be exclusive to those markets where technology is available and affordable. It can lead to job losses or exclusion of humans. Automation - while maybe tempting for reasons of efficiency - can be detrimental to the overall CX, for instance where users want to inquire about or challenge assessment decisions. We mitigate this by keeping humans in the loop and have positioned this as augmentation / support, not replacement for human teaching (double marking, customer support etc). This also addresses regulatory requirements.

- Finally, the potential negative impact of outcome (especially where we get to the point where we provide certifications for access to education, jobs or even VISA applications) is immense.

(For an example of how far reaching impact in this field can be, see <https://www.theguardian.com/uk-news/2024/feb/11/english-test-scandal-students-renew-fight-to-clear-names-after-10-years>)

More so, Ofqual (the UK regulator for qualifications and certifications) does at this point not allow fully automated marking.

Our believe is that the most appropriate way to mitigate this is by incremental rollout of products, initially in low stakes (low risk) scenarios while monitoring system quality via fast feedback loops (automated and with human involvement). As confidence increases, stakes can also increase.

////References

- <https://www.gov.uk/government/publications/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector>

Charter, inclusion from day 1, solid foundations, continuous monitoring, human in the loop, MVP and deployment in low stakes environments (as opposed to some of our competitors). Not blitz scaling.

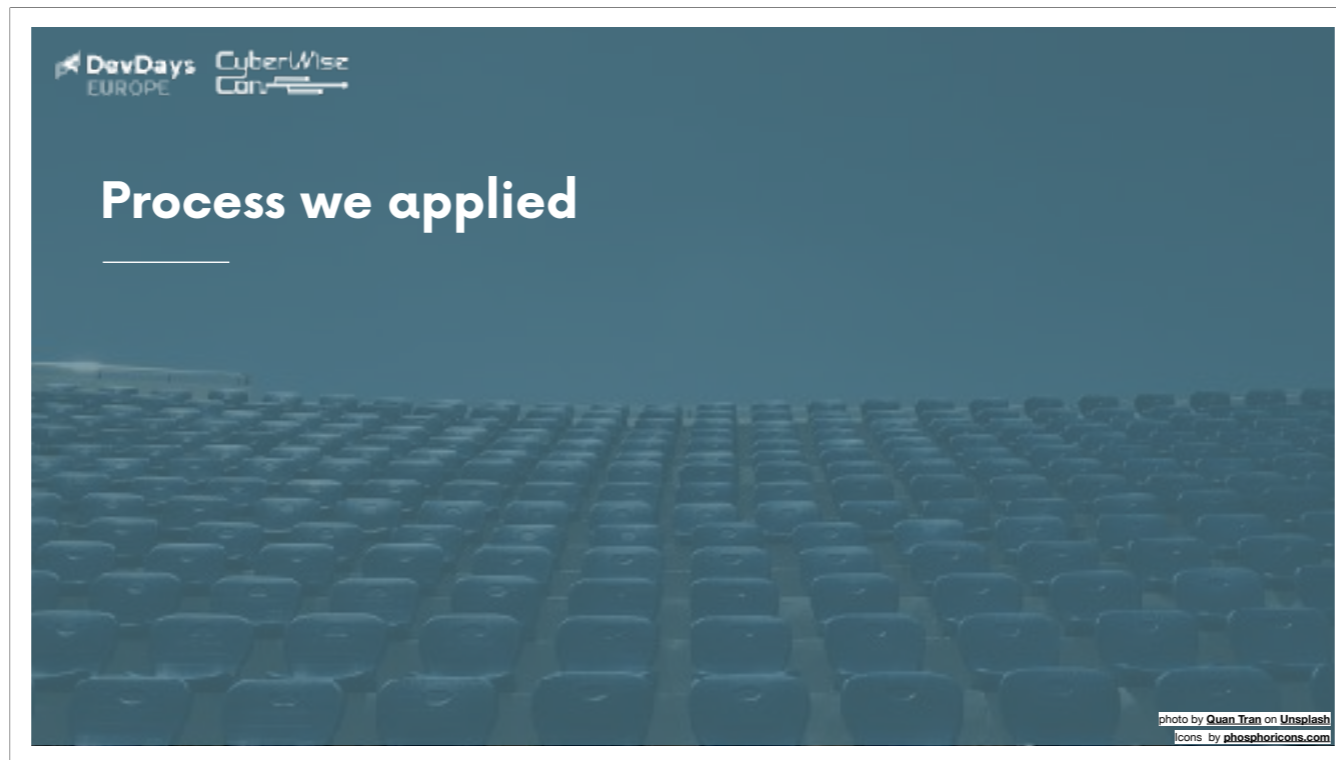
////image / icon

Icons by [phosphoricons.com](https://phosphoricons.com)

Photo by [Ivan Aleksic](https://unsplash.com/@ivalex?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash) on [Unsplash](https://unsplash.com/photos/brown-wooden-table-and-chairs-PDRFeeDniCk?utm_content=creditCopyText&utm_medium=referral&utm_source=unsplash)

# Ethical challenges

- Algorithmic bias / fairness  
**Careful training, monitoring**
- Validity  
**Academic foundations, monitoring, explainability**
- Impact of human-machine interaction  
**Research is looking good**
- Model training 'economies'  
**Mindful selection or longer-term strategy**
- Accessibility & impact of automation  
**Augmentation & support vs replacement, 'human in the loop'**
- Impact of outcome / regulatory concerns  
**Incremental rollout in low stakes scenarios with fast feedback loops**



We underpinned this by a continuous compliance process (for which we were an exemplar team)...

## Process we applied

---

- Sought (and got) permission to work differently
- Defined our ethics / compliance stance
- Seek motivated compliance champions with the right mindset
- Educate the organisation on continuous compliance
- Engage with core compliance from day 1, then 'continuously'
- Collaborated with experts and academia
- Regular reviews of system state in light of impact

# In conclusion...

DevDays EUROPE CyberWise Con

- Change the narrative
- Shift culture and process
- Chose strong champions and allies
- Involve them continuously
- Go incrementally

BEHIND THE ABSTRACTION  
www.behindtheabstraction.com

Image Midjourney

Agile compliance is possible - and valuable.

To get there you need to shift mindset (culture) and process).

If had to think of success factors I'd say

- Change the narrative
- Shift culture and process
- Chose strong champions and allies
- Involve them continuously
- Go incrementally



# I'd love to hear from you...

**Marcel Britsch**  
Product consultant



[www.beautifulabstraction.com](http://www.beautifulabstraction.com)



**Web**

[www.beautifulabstraction.com](http://www.beautifulabstraction.com)  
[marcel.britsch@beautifulabstraction.com](mailto:marcel.britsch@beautifulabstraction.com)



**THE DIGITAL BUSINESS ANALYST**  
Agile musings and ramblings

**Blog**

[www.thedigitalbusinessanalyst.com](http://www.thedigitalbusinessanalyst.com)

Thank you

I am available as consultant, advisor, coach&mentor, to work with or run your teams.  
I also speak at other conferences, blog and podcast.  
So please do get in touch...


////

You can find me here:

- LinkedIn: <https://www.linkedin.com/in/marcelbritsch>
- Site: <https://www.beautifulabstraction.com>
- Blog: <https://www.thedigitalbusinessanalyst.co.uk>

DevDays EUROPE CyberWise Con

# Thank you, questions?



<https://bit.ly/compliancebydesign>

BEAUTIFUL ABSTRACTION  
www.beautifulabstraction.com

Download this deck and find links to related content via the QR code above or here <https://bit.ly/compliancebydesign>.

Questions...

---

I am available as consultant, advisor, coach&mentor, to work with or run your teams.

I also speak at other conferences, blog and podcast.

So please do get in touch...

You can find me here:

- LinkedIn: <https://www.linkedin.com/in/marcelbritsch>
- Site: <https://www.beautifulabstraction.com>
- Blog: <https://www.thedigitalbusinessanalyst.co.uk>