Digital transformation – what happens when projects go wrong?

Kristina Locmele	Hello and welcome to today's episode in our tech podcast series. In this session we will be looking at what happens when your digital transformation projects go wrong. We'll look at the challenges that arise when the Tech fails, how organisations can respond effectively if an issue arises, but also what can be built into an organisation's transformational technology outsourcing contracts, or other complex technology procurements that can help reduce the risk of such failure in the first place. I'm Kristina Locmele, a Senior Counsel in Slaughter and May's Financial Regulation group, and I'm joined here today by my colleagues Ella Williams who is a Senior Counsel in our Disputes and Investigation group with extensive experience in global investigations and crisis management.
Ella Williams	Hi Kristina, it's good to be here.
Kristina Locmele	Hi, and Richard McDonnell, who is a Senior Counsel in our Technology team who advises both on putting the contracts in place for digital transformations andhas also worked with Ella extensively on disputes and investigations if things do go wrong.
Richard McDonnell	Hi Kristina.
Kristina Locmele	Richard, perhaps you could start us off with how we see the businesses use the tech and common risks of tech failure emerging based on our recent experience in the market.
Richard McDonnell	Yeah, of course. I think there's probably a couple of things that are going on here. Firstly updating legacy infrastructure so traditional sort of service physical servers to more cloud-based or virtualised systems. But also I think introducing new tools and particularly AI, a new large language model based tools are definitely becoming increasingly prevalent. Unsurprisingly they offer significant benefits, but they also introduce new risks. There's a few different ways that that tends to materialise so could be software failure. Could be an ability to deliver a particular new spec or it could be

	security vulnerabilities, and they can all cause pretty significant disruption when those digital solutions fail - the results can actually be pretty disastrous. We've recently seen several high profile IT outages that major UK banks, and that's left customers unable to access money or their essential banking services. Unsurprisingly the government's paying quite a lot of interest and these instances have prompted the Treasury committee to write to nine of the banks, and requesting information on those sort of IT failures affecting businesses over the last couple of years. The request looks at details on customers impacted, compensation and causes, and I think the responses that we've seen are actually quite illuminating. The UK major banks combined have experienced more than a month's worth of IT failures over the past two years. Causes very much including changes to tech, operational errors and third party service failures. In most responses banks have also had to compensate customers, and that just goes to show I think that there's both a reputational risk point here but also a financial one as well.
Kristina Locmele	Thank you very much Richard, that's a very helpful introduction to the topic. I think it's also worth saying a few words about regulatory action and enforcement in this space, so we turn to Ella for her insights.
Ella Williams	Of course, regulatory action in response to tech related incidents isn't a new thing, but the frequency of these events, together with the increased publicity that they attract, has increased the focus from regulators on this area in recent years. Enforcement actions resulting from these incidents can lead to significant penalties, as well as compounding the reputational damage that has already been caused by the incident itself. So just taking an example, the FCA and the PRA took action against TSB in 2022 following an IT outage during a programme update, which resulted in a fine of over £48 million for the bank, and then on top of that, TSB's CIO was separately fined personally for the same incident, which demonstrates that regulators are willing to hold senior managers accountable for their role in tech related failures. Another example to mention here is Equifax, it received a fine from the FCA of over £11 million, after and in addition to receiving a maximum fine from the ICO of half a million pounds for failing to manage and monitor the security of UK consumer data where management of that data had been outsourced to its US parent.

Kristina Locmele	Thank you, Ella. And of course, hand in hand with this increased scrutiny, the regulators have created a regime focused on bolstering firms' operational resilience. The transition period for which ended in March this year. A version of this regime has now been extended to ICT service providers to the financial sector, where they are designated as critical service providers. In our previous podcast, we looked at the impact of the operational resilience on digital service providers can be found in this podcast series. The FCA's Consumer Duty, only recently embedded, provides a further regulatory lever that could spur enforcement action in this area. It's also worth noting, perhaps, that in March this year, the FCA published its strategy for the next five years, marking a significant shift in tone and objectives compared to recent strategy papers. The FCA has stated that it intends to adopt a more flexible approach, with less intensive supervision where firms are demonstrably seeking to do the right thing. This will be welcome news for regulated firms.
Ella Williams	I absolutely agree with that and certainly welcome news and we've seen that shift in approach already in practice. But in the types of cases that we are discussing today, where serious failures have occurred which have significantly impacted customers, I think the FCA will likely still seek to hold firms accountable through enforcement action. The FCA see these are very serious regulatory breaches, and this is still a key area of focus for the FCA.
Kristina Locmele	So a bit of good news I suppose, but nothing to relax about just yet. Absolutely agree with you, Ella. Now, moving away from enforcement for the moment, you have extensive experience dealing with what happens when these problems do arise. What advice or lessons do you have for organisations that, despite their best efforts, find themselves facing a tech meltdown and need to investigate the root cause?
Ella Williams	Well, first I would say that it is often necessarily and understandably the case that any work on conducting a look back or investigating the root causes of the issue has to take a back seat whilst the ongoing issue is fixed. So if a technology failure occurs, especially one that is impacting customers, maximum focus needs to be on getting systems back up and running as soon as possible. Firms should activate their existing crisis response plan but bear in mind that they need to be ready to adapt to the specific facts of the incident if needed. Acting quickly is important, but so is remaining flexible and adapting to the facts of the incident.

	In terms of that immediate response effective crisis management hinges on involving the right people, so a good crisis response plan should help you identify who the core internal stakeholders are. Begin by identifying and briefing key senior leaders and functional heads who will need to oversee and manage the response. An in the initial stages, very regular internal briefings, perhaps as event as regularly as hourly in the midst of a crisis, can help maintain momentum, ensure alignment across teams and provide decision makers with timely updates as the situation evolves. Thinking now particularly about the legal aspects of the response, alongside the work to fix the problem, the legal team will need to assess any legal or regulatory notification requirements. If you're a regulated firm, you'll need to consider your obligations under FCA Principle 11 in particular. If it's something big enough that is likely to hit the news, then a firm will want to be proactively contacting the FCA to open lines of communication and provide assurance that the firm is reacting in the right way before the FCA finds out about it from the press or social media. And don't forget the ICO too. If a self-report to the regulator is required, early engagement with them should demonstrate your proactivity and cooperation. You need to be conveying how seriously you're taking the matter, offering a clear, fact-based initial assessment whilst also acknowledging the uncertainties. Maintain open communication and commit to timely updates on the investigation, service restoration and remediation efforts. Finally, you should document all key decisions, actions and findings from the outset. That's going to be an important record of what you did if the regulators later want to look at that response in more detail.
Kristina Locmele	That's a very good tip there, Ella, in particular in relation to documenting all key decisions and actions with reasoning to preserve for posterity. I think a point that very often is missed in the situation of dealing with a crisis. So initial storm over, first steps taken, is there anything else that we could point out to. What's the next step? What's the next thing to do?
Ella Williams	Conducting a root cause analysis, is a very important part of a firm's response to ensure that firms fully learn the lessons of the incident and take steps to address them. Although regulators in the initial stages will usually understand that focus has to be on fixing the issue, they will often expect to hear early on that a root cause analysis is planned, and then they want to see that happen

	without undue delay. Although conducting a root cause analysis promptly is important, it also needs to be approached with care. So, best practice is to establish a cross-functional investigation team, and the team should include a balanced mix of expertise. You need IT and technical specialists, you need legal counsel, representatives from the relevant business units and sometimes you'll also need forensic accountants. I'll also add that it's important to define the investigation scope as best you can upfront. Is there any early indication of what caused the issue and why? But also be clear at the start about the objectives and parameters. And the last point I would make is it's important upfront to design the governance around the investigation: what the team's internal structure is, what their reporting lines are, and that will help support effective and timely decision making as the investigation progresses.
Kristina Locmele	Once again, a lot of very helpful tips here and clearly a lot to think about. It's very easy to see that perhaps organisations should be thinking about the steps that may be required in the crisis whilst they're not in the crisis, and then having that framework, would perhaps help to navigate the crisis more effectively because it's very clear to see there's so much to do and think about.
Ella Williams	Yes, I think the importance of having a crisis response plan already in place cannot really be underestimated. When an emergency occurs, it's incredibly useful to have a plan that is to hand, that has been looked at recently. We've seen clients also often running mock emergencies, so running a test of their procedures to making sure that people know where the response plans are and how they operate, and I think everybody who has done one of those is incredibly grateful that they've done it once they are in an actual emergency.
Kristina Locmele	Yes, that's a very good example of if you fail to prepare, you prepare to fail.
Ella Williams	Yes exactly
Kristina Locmele	… and in the circumstances where there is a storm brewing, I don't think many would like the latter option. Richard, you've worked a lot of tech related investigations and also on putting the large scale technology projects in place. Having seen both sides, what

	advice would you give to organisations looking to procure and implement their transformation projects in a way that minimises the risks of things going wrong?
Richard McDonnell	Yeah, thank you Kristina. I mean it won't be a surprise to anyone that a successful transformation project requires good project management. And I think there's a few aspects to a really good and effective project management, especially where you are talking about an organisation wide project. And not all of these, I think, are giving the attention they deserve. So, I think, when people tend to think of project management they focus on, what I guess, organisational or implementation frameworks. So that will be: top to bottom governance, responsibilities, reporting lines, board level documentation, consideration of risk, timetables, all that sort of good stuff. I think where the problems creep in is how those frameworks are implemented and particularly how they adapt to inevitable changes to the project as it goes along. And there's are a couple of things, I think, that can have a real impact on ensuring that a framework that you put in place is able to adapt properly, and that's culture and expertise.
Kristina Locmele	Very valuable insight here, Richard. Perhaps we could talk a little bit more about the culture element of it that you mentioned.
Richard McDonnell	Yeah, absolutely, and I think culture actually goes a long way. So having a culture where people have the drive and desire to continue a project to the end, not just at the beginning is vitally important. And there are a couple of aspects that we've seen crop up time and again. One is a tendency to under-report, and this is where effectively issues are raised at a very low level but by the time they reach the board, actually the true scale of the risk has been downplayed and that might be moving a flag from red to amber, it might be describing a risk in slightly less problematic language. But I think that can be a real issue, because ultimately the decision makers don't actually have a true picture of events, and the reality only comes to light when something disastrous happens and they haven't had an opportunity to get involved and stop it.
Kristina Locmele	Indeed. I think it's the point where successfully completing the contract is not the end, but it is rather a beginning of a new functionality and new service and a new relationship.

Richard McDonnell	Completely agree, and that's something that is often left to the IT function. And that IT function often can have something of a supplier mentality within the organisation. There are a few reasons for that. It can be organisational history, so you might have an insource team who were previously independent. It's often individual background – many engineers who work for an IT team will have spent some time working for suppliers. Or it's just the way that they're managed. Typically, the IT function is something that is managed in quite a KPI or target-centric way, so they are essentially a cost centre. Again, that can result in an unwillingness to report up the chain and an unwillingness to really lift the cover as to what's going on while the contract's being implemented. It can sometimes result in a focus on the target at the expense of what is best for the business as a whole. A decision might be made to go forward with a particular change or transformation deadline when actually the risk means that the safer approach would be to just take another week to make sure that the risks are all properly bottomed down. We see that time and again.
Kristina Locmele	And I guess when a project is approached in a slightly disjointed way, in this way, you get some key elements lost in translation. The people who are implementing it practically for day-to-day use may not necessarily interpret things in the same way as the project team agreeing the legal documentation.
Richard McDonnell	Yeah, absolutely, and there is definitely a people risk to all this both as you say between people who are agreeing a contract with a particular vendor but also again thinking about the long term nature of these projects. There will be some cycling of individuals and background knowledge that might have been had but gets lost. The other point that I've mentioned is expertise. A lot of these projects now really relate to really new and complicated technology and often the understanding of that technology is limited, and there is a couple of ways you can try and solve that problem. One is obviously reliance on your external vendors and suppliers – they are the people providing the technology to you. But I think, Kristina, as you've been alluding to all along, there's some risk to that. So it comes with pitfalls – it means it becomes increasingly important, I think to manage your external vendors properly, having people who are implementing the project, understanding the scope of the contract. Understanding how service management works, and obviously avoiding concentration risks.

Kristina Locmele	I guess that might require, one would say, sufficient internal expertise to be able to manage that resource and to understand what external vendors are telling you and what they are able to provide and not to wholly outsource something that you don't understand how to utilise.
Richard McDonnell	Completely agree, and I think that has always been something of a problem. But I think given the complexity of technology, particularly being used by regulated institutions that risk has been made more heightened. Often people who are in these functions have been in organisations for a long period of time and they have grown up with a quite different set of systems and legacy infrastructure and now they're being asked to implement something that is very new and often without any training, or upgrading in their skills.
Kristina Locmele	Of course, no one can be expected to be an expert in everything, but I guess what you can do is ask the right questions and not be embarrassed to ask the right questions and take a bit more time to understand what it is that you are getting, how it will work, what are the limitations, and how any changes, upgrades, updates or amendments necessary will be handled.
Richard McDonnell	Yeah, I completely agree, and just to go back to something that Ella was saying, having that kind of cross-functional expertise is something, I think, organisations can bear in mind for day-to-day projects as well, not just in investigations. Sometimes actually having some external support from someone who isn't a vendor but does have sufficient understanding and knowledge of that expertise, but also has experience of regulatory risk and board governance, can be an incredibly valuable asset to senior decision-makers.
Kristina Locmele	As I guess, Ella this is where we can learn a lot from what we've been discussing around organising yourself in terms of dealing with a crisis as to what sort of tips we could take for preparing for and in dealing with a crisis and almost foresee and prepare for those things in terms of risk management and prevention but also dealing with changes as necessary when we are setting up a new project and getting new tech onboard.
Ella Williams	Yeah, I think that's right, and I fully agree with what Richard was saying that there can be a tendency to be optimistic in reporting up the management chain, and so you need to have the right expertise higher up that management chain to be able to ask the right probing questions to stress test what is being told to you from your report.

Kristina Locmele	Well, thank you very much, Richard and Ella, and that's once again a very long list of tips to digest. Thank you for sharing your expertise with our listeners, which I'm sure they will find very helpful. I think it's fair to say that one thing is very clear – effectively managing one of these complex tech transformation projects requires careful planning. It also requires thorough testing and prompt action when issues arise. I think we talked already, about clear reporting lines, involving the right expertise and ensuring regulatory compliance will be crucial in overcoming any challenges. Well, no doubt we could go on for hours diving into each of these points in more detail, but perhaps we leave it here for today. If you're interested in hearing more content like this, or generally about all things tech and digital, you can subscribe to the Lens and the Data Privacy Newsletter and our Digital Horizon Scanning series. Of course, please do also feel free to get in touch with us to discuss any of the specific topics raised in this podcast. Thank you for listening.
All	Thank you.