



The Deloitte On Cloud Podcast

David Linthicum, Managing Director, Chief Cloud Strategy Officer, Deloitte Consulting LLP

Title: A view from Red Hat on how banks can rein in growing cloud complexity

Description: As both banks and regulators have accelerated their move to cloud, complexity has significantly increased. In this episode, David Linthicum talks with Red Hat's Dr. Richard Harmon about how banks can rein in that complexity and leverage cloud to better meet regulatory requirements and manage risk. According to Richard, identifying critical failure points and adaptability play key roles, but the biggest determinant of success is an enterprise-wide cultural shift to a cloud-centric world.

Duration: 00:25:27

David Linthicum:

Welcome back to the On Cloud podcast. Today on the show I'm joined by Richard Harmon, global head of financial services at Red Hat. How are you doing, Richard?

Richard Harmon:

Very good, David, and thanks for having me on your show.

David Linthicum:

It's my pleasure. I'm looking forward to this because, as the audience knows, I love podcast recordings where I get to learn about things that I may not know as much about that I would like to know more about. So, what does the global head of financial services do at Red Hat?

Richard Harmon:

What we are trying to accomplish is to make sure that, globally, we help as many of our customers as we can to modernize their applications and their infrastructure and platforms. But our goal really is not only just technology, because we're the largest open source company and part of the IBM world as well now, and our goal really is also to ensure that technology not just makes our customers more successful, but also their customers are getting completely new and innovative capabilities that they don't have today. So, it's really the gamut of financial services, which is from banking, to capital markets, to wealth management, hedge funds, insurance, exchanges. We also cover extensively most of the central banks globally as well. The regulatory side, as we all know in financial services, is a key aspect of what you can do as part of the industry, and also the industry overall informs the regulators about new things that are coming and new innovations that are coming.

David Linthicum:

So, in the last five years, what's changed in terms of regulatory issues that financial institutions may be aware of and also need to build another technology?

Richard Harmon:

Obviously, the biggest change is probably the whole movement toward the cloud. Regulators are also moving toward the cloud, just as financial services institutions are. So, I'd say from a big picture perspective, at least from an IT infrastructure perspective, that's probably the biggest change. I think what the regulators are starting to become very sophisticated in and appreciate is when you move into a sort of hybrid multi-cloud environment. What I mean by multi-cloud. You have Amazon, Microsoft Azure, and there are many other cloud providers in different regions and different countries. But in that public cloud layer, you also then have private clouds that individual institutions run their own technology for. Eventually we'll have an intermediate layer, which will be sovereign clouds, which are clouds that are specific to a country or a region, and it protects the data and what information is allowed to leave the country.

So, what I'm trying to highlight here is that complexity. Think of it as a three-dimensional chessboard. That makes it very, very complex, and if you have unique systems in each of those clouds, and each cloud has some nuances that are very different, because every cloud has strengths above others in certain ways, in certain technologies, then you've sort of potentially exponentially increased the amounts of complexity that you have to manage. So, one of the challenges the regulators are concerned about is that enhanced complexity. While it drives innovation, it drives automation, it drives hopefully cost savings, but also what comes with it is potentially a higher complexity.

David Linthicum:

Yeah. It seems like with more complexity we have security issues that also pop up. Because, even if the security is very sound, if you're increasing complexity you have more attack vectors, all these things to deal with, the ability to distribute data, the ability to lock down data. Some data in some countries can't be transmitted out of that country. It has to be exposed and handled in a particular way. So, it just seems like it's not only the complexity of the deployments, the ability to leverage multi-cloud, private cloud. The enterprise systems are still there. It's part of the architecture. But really, the complexity of dealing with the components and the moving parts within the FSI, financial services industry, because they're so heavily regulated. What are your thoughts on that?

Richard Harmon:

I completely agree with you. You're spot-on. The last ten years we've been on a digital transformation mode, and we're still on that mode. It'll probably never end. But digital transformation, particularly coming out of the COVID period, now everything is moving also into real time. When things are in real time, that means you need to have most systems heavily automated, so you don't have human interventions, and you also have to have a very sophisticated setup, capabilities to ensure resiliency, especially when you get to things like payments or clearing systems or trading systems. I think the overall challenge of that is the ability of not just technology, but also people in terms of adapting to a different environment, a different way of doing work, a different way of building applications, a different way of storing data.

Then any institution that is multi-country or global, they will have, as you highlighted, every regulator in each country will have some nuances that are unique, what data can be stored and where, what data can be removed, what data has to be extremely highly protected, confidential data on the customers. So, that complexity is multi-layered and multi-faceted. IT helps in that. It helps in terms of automation, and the more thing that we can automate from an IT perspective, the more resilient those systems are and the easier it is to move things to adapt to do other things. I'm not trying to scare people, but my point is that this complexity really requires institutions to look at a phased approach as they move into these new environments.

David Linthicum:

Yeah. I can see where things are just getting hugely complicated. So, if we're dealing with cloud-based systems or outsourcing some of the stuff to a public cloud-based systems, normally it's several public cloud-based systems and also different intermediaries. We may use co-los and we have some edge computing stuff. Certainly in the banking industry IoT is a big thing. You have to deal with a network of ATMs and all these sorts of things. The ability to manage risk internally with things that you own and control is one thing, but the ability to manage third-party risk is kind of a dimension that's fairly new to FSI. What are your thoughts?

Richard Harmon:

Yeah, I agree. Different countries have different, say, stages of maturity in terms of looking at that. Third-party risk management has been part of the regulatory or supervisory elements for regulators, for at least the last decade or longer. But with the digital transformation, everything moving into this sort of hybrid multi-cloud environment, now the regulators are starting to realize that this complexity creates potentially more risk. The way I see it, and this is the way I think everyone in the financial services industry sees it, is there's two facets of this. One is around concerns about cloud concentration risk from an institution perspective. So, whether that single institution might have applications, all of their applications, as they're modernizing those applications, potentially moving most of them into the public cloud, if they build something native in one cloud that prevents them from moving into another platform, another cloud, then there's an element of lock in there.

Now the advantage of doing that obviously is you take advantage of some unique capabilities that that cloud provider has or that platform. But that lock in effect is problematic, because if the institution has to be—let's say it's required by the regulator and it decides to move to another cloud provider, another platform, it then will have to effectively redevelop some aspects of those applications. That doesn't happen overnight. That can take months, if not many quarters, and in some cases even a year. So, the regulator is concerned about institutional concentration risk in terms of lock in. But for the real regulatory perspective, they have a more global or sort of market view, and they are concerned about systemic risk.

So, this is not about any single institution deciding to be on one or two or whatever number of cloud providers. It's about several institutions having some mission critical application in the exact same sort of cloud environment or platform. What that means is that if there is an event or some aspect, in many cases people fear, particularly with regulators around cyber security types of tests. This is not just hackers and criminals, but it's also nation state actors, as we've seen over the last two or three years, and these institutions are very, very sophisticated. So, if you have one cloud provider where you have let's say a payment system across five major banks in five or six countries, then you potentially have spillover effects. So, in the worst case, you could think of the Lehman Brothers scenario in 2008, where the problem here is you don't know what's happened and who it has impacted, but that concern is a systemic risk concern that regulators have. That's not relevant to any single institution. Their responsibility is to look at the security of the entire financial system.

David Linthicum:

Do you think that this risk that people are perceiving in looking at cloud-based systems, and certainly third-party risk because you're putting your hands on somebody you really don't control directly, you're a consumer of their services, is turning a lot of financial services companies away from cloud?

Richard Harmon:

I think for smaller firms, potentially yes. I think the other aspect is it's forcing them to simplify how many third-party providers they have, which I think overall is very beneficial. One of the biggest dangers of institutions moving to the cloud is doing the lift and shift. You take something that was nicely set for an on-premise old legacy architecture and say, "I want to move it to the cloud." As all of us know, that's a disaster usually, in most cases. So, the ability of taking legacy systems, where you have a lot of depth—most banks probably spend anywhere from 50 to 80 percent of their overall IT budget in ensuring that all their systems run properly, run efficiently, et cetera. That's a huge cost of maintaining, keeping the lights on in an institution. As they modernize and move those into a cloud environment, there is substantial simplification in many cases, automation, more agility, innovation that comes across, more capabilities.

So, the savings that you get from limiting some of the legacy platforms, and then achieving enhanced capabilities in terms of serving customers, delivering new products, that savings really transforms the ability of a bank to become more competitive and more profitable. But I think the complexity around third-party risk management, in Europe we have the DORA regulation, Digital Operational Resilience Act. That complexity is what's driving a lot of consideration of how many vendors the institution ideally can manage, and how many do they actually need. So, I think long-term it's actually a good thing, because they are going to be a lot more focused and prescriptive, and manage this third-party risk in a much more effective manner.

David Linthicum:

One of the things that kind of strikes me is over the last ten years there hasn't been a ton of cloud outages, but they do occur, and certainly when they do occur we hear about them. I get calls from reporters when they happen. So, how do financial services institutions, financial service in general, manage SLAs? What are some of the best practices that are emerging, and how does it relate into risk mitigation?

Richard Harmon:

Even with the regulators, they take a risk-adjusted view. So, if you have applications that are not mission-critical to the bank, it won't bring the bank down or cause significant financial loss, the SLA requirements, outside of maybe not serving customers effectively if the system is down, that is not a concern from a regulatory perspective. Now the bank might view a particular customer segment, say wealth management, might view being down for a day as a catastrophic event from a reputational standpoint. But if it's not a mission-critical thing, there's probably less need to build a lot of resiliency and redundancy.

When they are mission-critical applications, and this has always been the case for the financial services sector, this is not new, what's new now is they might be in very different platforms. So, moving from a particular cloud and moving back on-prem or moving from one cloud to another, that's a different situation that there's not 10, 15, 20 years' experience. So, the SLAs for those, the regulators are starting to look at those requirements. There's nothing yet firmly explicit as far as ICNS.

I think the institutions themselves clearly understand what they need from an SLA perspective. I think overall we'll have probably a fairly consistent level globally from folks like the Bank for International Settlements and the various central banks in terms of: what are the points that are mission-critical, high-risk, where you have to have lots of agility, portability or exit strategies, as they like to use the term, and in others which are really managed by the institution, much lower risk?

That's something that the regulator is not nearly as concerned about. But the exit strategy piece is sort of the piece around the DORA regulation, which is—I like to use the word portability, but it's the ability of keeping your options open. So, from my viewpoint, if you had all of your applications in one cloud that was in a public cloud, I don't think personally that's necessarily always a problem, if you have the ability of migrating or running those in some other

platform without massive issues, because then you've kept your options of running anywhere open versus being locked into one cloud. Now once you lock yourself into one platform, it doesn't even have to be a cloud, then the portability is not there and it can be timely, expensive, and very harmful, potentially even to the financial system overall, of having that kind of lock in effect.

David Linthicum:

So, the objective is flexibility, resilience, compliance, all those sorts of things that FSIs need to get to in leveraging technology to its most optimal state. What are the steps to success? What do I need to do to make sure that I get to something that's going to be hugely flexible, resilient, and also maintain compliance?

Richard Harmon:

I think there's three key areas. This, again, is what all financial services institutions do and regulators expect from them. They really need to carefully look at their entire IT landscape. They need to understand what areas are critical, what areas are potentially failure points, and they do this constantly in terms of evaluations, and to have agility. They need the agility not just to ensure that they can meet regulatory requirements, but they need the agility to continually adapt and innovate. The one promise of cloud computing is the ability to accelerate and simplify your ability to innovate, in terms of bringing new technology. We see a lot in the AI space. The foundational models are hugely impactful, potentially. That ability of being very agile and flexible, that's the goal of a lot of these activities.

But to do that, it's not just about modernizing the technology. You also have to upscale your expertise and your people. It's a cultural change as well. It's a different way of working. That is usually, from what our experience is, probably the biggest challenge in terms of becoming successful in your modernization or cloud transformation journey. Then the understanding of: what are the foundational elements to success? Like anything you do, you have to lay a solid foundation of technology, people, systems, et cetera, in place. Then you start accelerating as you start to modernize legacy applications into a more modern architecture and gain all those benefits, but you need to do that in a phased step approach.

David Linthicum:

One of the things that I always joke about is that I should have got a psychology degree, not a computer science degree. You kind of hit on this in some steps to success. Drill down a bit on people and culture. How do I make the changes there to ensure success or get closer to ensuring success I guess is probably a better approach?

Richard Harmon:

Yeah. I see this across many different types of institutions, also different regions. There's cultural differences across regions, also sophistication of the technology that's available in regions. I think it's really about getting people to understand what is the goal of why you're going from A to Z, and the outcome of that goal is new capabilities, new benefits that the institution wants to be able to provide to its customers, to serve its customers better. The end goal obviously is to be more competitive, more profitable, hopefully a simpler run institution as well. But to do that, there needs to be a significant investment in the people. Obviously you can hire consultants and they have a tremendous amount of expertise and experience in doing this, which is why we have these global system integrators that have massive teams of highly skilled, highly experienced people, but it's also the staff within that need to be upskilled and educated.

I'm biased because I come from Red Hat. We strongly believe an open culture, a very transparent culture is what helps facilitate that cultural change, that sort of business change, business model change, technology change. Because when it's an open environment where people are sharing freely, they're collaborating together as much as they can, we try to eliminate silos as much as we can. That is the secret, ultimately, from our perspective, of really being able to enhance what everyone is doing, in terms of trying to get the institution to change its overall focus and culture. But it's this notion of being as open and transparent and collaborative, those are some of the secret sauces of really driving a completely different culture within an institution.

David Linthicum:

I think it's key. I think you just hit the nail on the head. I think financial institutions, having worked with those companies for a long period of time, they used to be very autocratic, then very structured, very bureaucratic in how people worked. Everybody kind of worked in their silo, they didn't normally step out of it. Now you look at them, very flat organization, very informal communication channels. Certainly they're widely distributed. The pandemic did that. It kind of blew everybody back all over the country and certainly working out of their homes. I think those institutions are the ones that are taking their business to the next level, when those that remained autocratic aren't going to be moving as fast. Where can we learn more about this? Where do you go to learn more about financial institutions, patterns of leveraging technology, and some of the best practices that are emerging right now?

Richard Harmon:

I'm an academic by training, so I encourage people to look at many sources. Most institutions have varying sophisticated partners, whether they're technology partners or they're consulting partners or system integrators. There's a great amount of knowledge and wealth from those kinds of sources. You also have new generations coming out of schools, on the academic side. They're learning the latest technology, the latest architecture, the latest skillsets. I think that is also the younger generation that you're hiring. But I think the most important part, and this is what we really leverage in Red Hat and many companies do, it's about self-learning.

It's about getting the individuals to want to accelerate and learn as much as they can and dive into the latest technology, because that's exciting for the individuals themselves. It automatically translates into new ideas, new innovations, new approaches in an institution, even if it's somewhat of an autocratic one. But I think it's all about the individual being and their ability to have curiosity and learn from a range of sources. Now that's my academic bias and also Red Hat bias, but I really see the more that we can get humans to adapt and leverage tools, but to explore and want to go at the cutting edge, where the roles allow, that really is where we get innovation, flexibility, and success.

David Linthicum:

Where can our listeners follow you out there? Also, where can they find more information about Red Hat?

Richard Harmon:

We obviously have a very sizeable website. If you're in financial services, please, I'm happy to talk to anyone and everyone. We do provide a lot of publications and other capabilities. We have very, very large partner ecosystem that use our technology to deliver innovative products to all kinds of industries and customers, including financial services. So, there are a lot of ways of getting into the open source world. The Linux Foundation, I'll give a plug for the Linux Foundation. It has over a million projects that it runs. It is an incredible source of looking at what can be done in a global community about innovating all kinds of aspects. So, the community aspect, which is what open source is, is a wonderful source. There are lots of people you can tap into, lots of communities. You can learn that way. You can contribute that way, which is really what it's all about.

David Linthicum:

Let me tell you; I think it's smart for companies like Red Hat and other companies as well to keep talent like Richard around, because you have to have not only an understanding of the technology, but a deep understanding of how you're making the technology work in a specific industry. Industry-specific services and patterns are going to be more important as we move forward. You can't look at this stuff in a horizontal way anymore. It's not one-size-fits-all, but the ability to leverage different industries with different solutions and different emerging best practices. So, I think this is absolutely a great conversation. So, if you enjoyed this podcast, make sure to like us, rate us, and subscribe. You can also check out our past episodes, including those hosted by my good friend, Mike Kavis. Find out more at Deloittecloudpodcast.com, all one word. If you'd like to contact me directly, you can e-mail me at dlinthicum@deloitte.com. So, until next time, best of luck with your cloud journey. Everybody stay safe. Cheers.

Operator:

This podcast is produced by Deloitte. The views and opinions expressed by podcast speakers and guests are solely their own and do not reflect the opinions of Deloitte. This podcast provides general information only and is not intended to constitute advice or services of any kind. For additional information about Deloitte, go to Deloitte.com/about.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Visit the On Cloud library
www.deloitte.com/us/cloud-podcast

About Deloitte

As used in this podcast, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Please see www.deloitte.com/about to learn more about our global network of member firms. Copyright © 2023 Deloitte Development LLC. All rights reserved.