TRANSCRIPT OF PODCAST
Federal Credit Fridays: Information Security Compliance
***DISCLAIMER: This is a draft transcript that was automatically generated. It is meant as an accessibility aid for the associated podcast, not an official record.*

00:00:04 Intro
Connecting you with thought leaders and experts in federal loan programs. This is Federal Credit Fridays with your host, Anthony Curcio.

00:00:19 Anthony Curcio
Hello, I'm Anthony Curcio, and this is the latest episode of Federal Credit Fridays.
Last time, we kicked off our three-part series on IT compliance and federal credit by exploring a fundamental question, what makes this environment different? We discussed how federal lending programs operate under unique pressures, managing large, long-lived data sets, navigating strict audit requirements, and protecting controlled unclassified information across the full life cycle of a loan. But today we're going to go from problem to solution. If the compliance requirements are more demanding, in many ways even less forgiving, than what we see in other federal or other commercial settings, the natural follow-on question is this. How do agencies and their partners actually meet these more demanding requirements in practice? Over the last decade, the answer to that question has evolved significantly. Advances in cloud computing, the emergence of the shared responsibility model, and the standardization of federal frameworks such as FedRAMP have fundamentally reshaped how compliant environments are designed and operated.
What once required heavy on-prem infrastructure and bespoke security solutions can now be achieved through more scalable, flexible architectures if it's implemented correctly.

00:01:33 Anthony Curcio
At the same time, these tools introduce their own set of trade-offs. Decisions around architecture, cost, performance, and data movement become critical, especially when dealing with the scale and complexity of federal loan portfolios. In other words, while compliance may be more achievable, it's certainly not automatic. To help us unpack how organizations are approaching these challenges in the real world, I'm again joined by Josh Baker. Josh works at the intersection of data, infrastructure, and cybersecurity, helping to design and operate compliant IT environments that specifically support federal lending programs. His experience includes implementing cloud-based solutions, navigating FedRAMP-aligned platforms, and ensuring that large, complex data sets can be processed securely and efficiently. Today, we're going to focus on what works and what doesn't when it comes to building compliant, scalable systems for federal credit. Josh, welcome back to the podcast.

00:02:31 Josh Baker
Hey, Anthony, great to be back.

00:02:33 Anthony Curcio
Well, the last time we spoke, we were highlighting, again, those challenges that are unique to federal credit programs and specifically to the federal credit IT landscape. Let's talk about how you solve them. I'll just maybe throw you an easy softball. What are some of the things that you have found in your career, 10 years or more working in a loan-specific environment that you found to be successful?

00:02:57 Josh Baker
Yeah, Anthony, so the proliferation of cloud services has really been the game changer for me in the last decade. In my experience at Summit, leveraging cloud services is so crucial to me in this space. It's the only way that I have found for Summit to be scalable in this world of large financial data. I mean, 10 years ago, I had so many headaches that I don't have to think about now because we are leveraging cloud services.

00:03:26 Anthony Curcio
Well, let me dig in a little bit. Maybe I'll just cut you off if you're going to say this anyway, but say more. Like how, the cloud is great. I understand a lot of the value proposition is presented to our entire economy, but how does it help with this specific problem?

00:03:42 Josh Baker
Sure, yeah. So really has changed how organizations are able to handle those compliance requirements, especially when it comes to this concept of the shared responsibility model. That shared responsibility model is, it's a framework or a matrix that really describes the division of obligations between the cloud service provider and their customers. And so, you know, one way I can illustrate that to you easily would be you've been here since, you know, for the last 10 years along with me, and you will have noticed that the server room has changed dramatically in terms of size. You know, we used to have a huge closet full of servers and networking equipment, and that required all kinds of maintenance. special HVAC equipment and things like that. these days, we have very little footprint on-premise, and that is due to the fact that we are able to scale in those cloud service providers. And when you're talking about federal credit data, scaling is very important. We used to have lots of conversations about how long we were gonna be able to fit our data in the box that we had bought for our server closet. And thankfully, I don't have to think about that anymore.

00:05:05 Anthony Curcio
And maybe it's TMI, but I can remember Josh, you coming into my office one time asking me for $250,000 for an air conditioner for our- That's exactly right, yeah. And I was like, boy, I wish I had an air conditioner like that in my house. But anyway, those days are over.I mean, it hasn't been that long ago. And I just want to validate and double down on what you're saying. Without being specific, we have one client that has 30 million single family mortgages. And every year we get a whole new data set history for all 30 million mortgages, and we need to keep the previous version. There's a lot of data, right? And I think that kind of makes your point that

you've been making before. And the more data we have, I think the more options we can enjoy for estimating models. You know, we don't want the precision and the creativity of our models to be limited by data limitations. So that makes a lot of sense to me.

00:06:05 Josh Baker
Yeah, and I would say you can tell that this is a unique sector dealing with this financial data, big data, because we had a managed service provider way back who, when we asked them about data storage, they said, Oh, here, we'll give you this fifteen-terabyte box and you'll be fine, you'll be good to go. And I'm sure that was true for a lot of their clients, but I think we shocked them by saying to them, we still need more. And they weren't used to that.

00:06:35 Anthony Curcio
So Josh, let me dig in a little deeper then. So what happens to the physical control?You mentioned a lot in our last episode around NIST and their guidelines. What happens to the physical... elements of those controls that we find in the NIST guidance.

00:06:49 Josh Baker
Yeah, the physical controls don't go away. And this is where, you know, we have the Federal Information Security Modernization Act, or FISMA, which tells government agencies that any commercial off-the-shelf cloud services that they're going to use need to be FedRAMP, which is the Federal Risk and Authorization Management Program. So, when we are choosing a cloud service provider, we have to look for that, and what that means is that the big players that everyone has heard of, the Microsofts, AWS, Google...They've gone through the work of building these data centers in a way that's compliant that the government has given these authorizations to operate to, so we know that our physical controls are taken care of when we store data in their data center, so that's a big convenience for us.

00:07:43 Anthony Curcio
Got it. Well, that's great. So, Josh, as we wrap up today's session, with all this innovation and improvement, especially as it relates to capacity for data, what are some of the new challenges that you face that did not exist before?

00:08:00 Josh Baker
It's a common mistake for organizations to make to think, oh, I'm storing my data in the cloud service provider. I've got my stuff in Azure. I don't need to worry about security anymore.That's just not true. And so when you are using the cloud, you still have to be very creative, maybe even more creative because you have to be familiar with where the responsibility of the cloud service provider ends and where yours begins. So you are also talking about cost considerations. It used to be capital expenditures versus now ongoing subscription costs in the cloud. And you need to, especially when you're talking about, I keep bringing it back to running analysis on large files. If I'm at a workstation in our headquarters, but my loan data is sitting in Microsoft's data center, I'm

constantly pushing and pulling that data over that internet connection, which introduces some serious latency. And then having that latency can really eat into the efficiency of our processes. So one of the things I'm most proud of at Summit is we've done some very cool things with the hybrid architecture to solve those types of problems, make our data available in multiple locations simultaneously while maintaining the proper security around any assets that store, transmit, or process CUI or other data. So you still have to be creative in your problem solving, and that still happens even when you're inheriting some compliance controls from your cloud service provider.

00:09:41 Josh Baker
Interesting. Okay, well, I think we're gonna leave it at that, Josh. The next time I'm gonna ask you one more favor, if I can. Go for it. Okay. I'd like to come back a third time and really dig into the even more particular requirements for working in national security, particularly the Department of War. And so if you don't mind, I'm going to get you to come back and talk about that in a third and final episode. How does that sound?

00:10:07 Josh Baker
I would love to. Yeah, I've got a lot of thoughts about that.

00:10:10 Anthony Curcio
Okay, great. Until the next time, this has been the latest episode of Federal Credit Fridays.