IBM Podcast

[MUSIC]

GIST: Welcome to this IBM Rational podcast, Surviving an Audit: is Your Software Development Process Ready? I'm Kimberly Gist with IBM. For software and systems development teams in regulated industries, the ability to demonstrate compliance with a complex and dynamic set of regulations including internal control of software development processes is costly and challenging.

IBM's Collaborative Lifecycle Management -- or, CLM -- solution provides project to process definition and enactment with application lifecycle traceability. This podcast is a precursor to an upcoming Webcast on ways to apply CLM capabilities to address compliance and auto reporting needs including support for segregation of duties, work authorization and audit report generation.

Today, Cindy VanEpps, Strategic Industry Solutions Lead for Rational Software, and Nick Norris, Solution Architect for the IBM Rational Software company, join us with some key ideas on how you can reduce cost and the risk of software and systems development compliance. Cindy, Nick, welcome to the podcast today. Why don't we get started with our first question? Nick, what exactly is regulated collaborative

lifecycle management?

NORRIS: Collaborative Lifecycle Management is about a focus on the entire team contributing to the development, delivery and maintenance of software systems, packaged apps like SAP or custom apps or even IBM BPM [wada] maps that are used to run a business.

IBM Rational is a market leader in this space, breaking new ground with the IBM Jazz platform upon which the Collaboration Lifecycle Management tools are built. This platform and tooling are especially designed to meet the demands of the new world economy and technologies with a heavy emphasis and focus on collaboration, transparency and flexibility. These are key capabilities that help organizations be more agile in the way they deliver high-quality software more quickly.

But for software development in regulated industries and environments the right balance has to be struck between agility and governance. Compliance with the Sarbanes-Oxley Act in the United States, for example, requires organizations to protect the software systems and data used for financial reporting. And it applies to every publicly traded company in the United States.

Some of the implications of this are the need to put

policies in place to support work authorization and association of duties. Each organization has some flexibility in the details of how they implement these concepts, so we have examples of the most common things these regulated organizations will need.

GIST: Well, that's a great definition, Nick. Cindy, why don't we give the next question to you? What would you say is the cost and risk to software development organizations that you're trying to address here?

VANEPPS: Thanks, Kimberly. You know, we see news headlines every day of organizations like large banks and financial markets where things go awry. And the impacts to those companies are often devastating, but more importantly, the impact to world financial markets and even national security can be at risk.

So while the root cause can be proper definition and enforcement of controls or proper education and adherence to controls by individuals in the business, there's almost always a link to the software used to run the business. So it's not just the cost and risk to the software development organizations; it's really the cost and risk to the entire business.

One of the great values of automation of the business with

software is the ability to ensure use of proper control. But when the business comes to depend on that software to enforce the control and if the software's not properly updated and maintained, then the company is exposed to risk.

So the cost of implementing and maintaining improving compliance is also a huge burden to these organizations. We are helping to reduce the cost and risks by embedding compliance directly in the application development. I think it helps to understand this with kind of a personal analogy.

So what if we determined that the risk of drunk driving was so great that we required every car to have a breathalyzer. And then when you got in the car to drive you tested your breath, then you got to make a decision whether to drive. Then every month, you had to print out your breath analysis results and send it in to the Department of Transportation to review. And if you were found to be out of compliance you would be sent a ticket.

Many people would argue for that model because it gave you, still, some personal choice. But what if you could configure your car so that it did not let you drive if your blood alcohol level was above the legal limit? Well, you and your family would likely choose to do that to reduce the risk and cost of drunk driving. And you might even encourage others to do the same for the safety of the

community as a whole. So that makes sense.

Well, what we are talking about here is allowing businesses to choose to automate the enforcement of the controls that protect their businesses as well as their community of stakeholders. This reduces the cost to the business of implementing compliance as well as reducing the risk and cost of being out of compliance.

GIST: That was a great illustration, Cindy. Nick, our next question is, why are you emphasizing audit survival and what kinds of audits are you talking about?

NORRIS: When we talk with our banking and insurance customers about the ways they develop and/or deliver software they tell us about the compliance pain points in the context of audits. Audits are a forcing function for organizations to stay on top of their software development compliance responsibilities. They often start with a very manual and spreadsheet-driven solution. They are not even connected with the way the project is executed.

As a result, the process of preparing for, supporting and responding to an audit is not just about these direct costs but also about the cost of being distracted from doing the real work of the project.

They tell us they love our Collaborative Lifecycle Management solution because everything you need to know about a project's process and how they follow it is baked into the CLM solution. But like many other application lifecycle management or point solutions, they find that they are still spending too much time supporting audits than they should.

So we have developed examples and templates into a software development compliance solution that works with and augments our CLM solution to make audits less disruptive and costly. This software development compliance solution helps organizations by first establishing what they have to prove to an auditor and then baking ways of proving compliance into the project's process and enactment environment.

Regulated businesses also have corporate governance risk and compliance organizations. They can be centralized or distributed, but much of their missions are the same. They define the controls that ensure the business is complaint and can prove compliant. And as part of their responsibility they perform internal audits to ensure compliance with those controls. An audit of the software development and/or delivery projects and processes are a common practice.

Another type of audit that must be addressed is

post-incident audits. These are audits that are performed after a negative event happened with the software systems used to run the business. These audits may happen weeks or even months after the event.

So software development teams and organizations must be able to reconstruct the stage of the development at the time of the event or the delivery of the software involved in the event. The IBM CLM and software development compliance solutions enable organizations to better conduct these types of audits as well.

GIST: Wow, Nick. Some really great insight there. Cindy, our final question. What kinds of businesses will care about this and why?

VANEPPS: Another good question, Kim. You know anyone who develops software cares about the process is carried out. Small, very agile teams can be self governing by their very nature. So, for companies where there are no mandates like Sarbanes-Oxley to worry about and they have a small development staff, their compliance to internal policies may be trusted to communication and transparency.

But consider that banking, insurance, financial markets, transportation, aviation, automation, automotive, defense, electronics, telecommunications -- I could go on and on --

are all subject to industry-specific regulation, so they are legally bound to have some types of controls in place. And they are certainly more regulated industries than non-regulated.

But honestly, if I'm a business owner and the software is running my business, regardless of the size I'm going to care deeply about governing how the software is developed and protecting it from malicious or involuntary harm even in an outsourcing situation the risk is owned by the company who owns the software.

And these concepts are straightforward: work authorization, segregation of duties, process change control, artifact traceability and audit support. Anyone who doesn't care about at least some of these things certainly is accepting a lot of risk.

GIST: Thank you Cindy and Nick. A great overview on software development compliance and our Collaborative Lifecycle Management solution. We sincerely appreciate you joining us to share your time and expertise today.

We'd also like to encourage our audience to look for a deep dive into this subject. You can check out our bank systems and technology Web page and listen to our Webcast entitled, Audit Survival for Regulated Collaborative Lifecycle

Management.

That again was Cindy VanEpps, Strategic Industry Solutions Lead for Rational Software, and Nick Norris, Solution Architect for the IBM Rational Software Group, with some key points to consider on our topic today, Surviving an Audit: Is Your Software Development Process Ready?

To hear this specific podcast or to browse additional topics, check out our Rational Talks to You Podcast Page at www.ibm.com/rational/podcasts. This has been an IBM podcast. I'm your moderator Kimberly Gist. Thank you for listening, and we hope that you will choose to keep tuning in as Rational Talks to You.

IBM Podcast
[MUSIC] [END OF SEGMENT]