HARLAND CLARKE®

Harland Clarke Webcast 10/25/2017
5 Governance, Risk, and Compliance Scenarios (and How to Navigate Them)
TRANSCRIPT

Presenter Karen Salamone, Vice President, Marketing
Presenter Kevin Malicki, Director, Product Management, Governance, Risk, and Compliance

Nathan: Good day, and welcome to Harland Clarke's webcast Five Governance, Risk, and Compliance Scenarios and How to Navigate them. This webcast is being recorded and a replay will be sent to you within a few days. If you have questions, please use the chat box located in the control panel. Your questions are private and are only seen by the presenters. I will now turn the call over to Karen Salamone, Vice President of Marketing at Harland Clarke. Karen, you have the call.

Karen: Nathan, thank you so much and welcome, everybody, to our webcast. I'm joined today by Kevin Malicki, who is the Director of Product Management for Governance, Risk, and Compliance here at Harland Clarke, and delighted to have him with us today.

Kevin brings over 20 years of banking experience, he's held senior-level positions at SunTrust Bank and Fidelity Southern Bank where he was responsible for driving risk management activities, and he's also the host of a video blog that you can find on our website on inside.harlanddclarke.com, which is called Keeping up with Kevin where he discusses issues and tips related to governance, risk, and compliance. Welcome, Kevin.

Kevin: Thank you.

Karen: In our webcast today, we're going to be discussing five real-life scenarios that financial institution compliance departments may face in today's regulatory and governance environments. I'll set up each scenario, and then Kevin will provide his insight and expertise on how to think about the situation, important questions to ask, and actions that financial institutions might take in each scenario.

I think this will be an informative webcast and we'll enjoy our time together this afternoon, and I hope you all walk away with a few action items. Let's get started with our first scenario, and this one is on the topic of regulatory change. The current administration is looking to deregulate certain aspects of Dodd Frank.

This is a scenario that's of really high importance to the Chief Compliance Officer. The CCO wants to stay abreast of regulatory changes because he or she knows that their institution's account holders will be concerned about how this repeal will affect their money and their overall consumer safety. Kevin, how does an institution navigate in this type of a scenario?

Kevin: First off, thank you, Karen, for the introduction and welcome, everyone, to the webcast. Addressing your first question, for months now we've been hearing from the new administration that banks should be seeing some sort of regulatory lease, but we have yet to see anything with any teeth on it with regard to deregulation of Dodd Frank. It appears we are still some time away from seeing any type of overhaul. However, we are still seeing a steady flow of regulatory changes and enhancements. The CFPB certainly doesn't seem to be easing off, either. We might even see the pendulum swing the other way.

Now, a Chief Compliance Officer in this scenario needs to be clear on what these regulatory changes mean, the impact they will have, the policies that will need to change, the training and communications involved so that they can effectively communicate these changes to employees and account holders. To get clear on this, whether it's a new regulation, change to an existing regulation, or the removal of a regulation, which seems doubtful, several things need to be considered. On the next slide are just a few things to look at.

Next slide, some of the processes that will be impacted. When identifying and reviewing your processes, ensure you are considering an end-to-end process. Process flow amounts may be handy in this case. Also consider what policies and procedures will be impacted, what changes this creates for risk tolerance, what third and fourth parties are impacted, does training need to change, what client impacts there may be, and any changes to communications. Once clear on these questions, then the communications plan needs to be put in place.

A Chief Compliance Officer in this situation can try and manually manage the plan, but using spreadsheets, Word documents, PowerPoints, Outlook, and shared drives would make this cumbersome. Manual can include a certain level of risk that all areas were not discovered and thus overlooked, which would not fare well during the next audit. We really recommend a technology solution that allows institutions to store and maintain all your regulations, controls, risks, third and fourth parties, policies and procedures, and client communications allowing for a searchable tool to easily identify all aspects that would be impacted by such a regulatory change.

Now I don't know if you saw, but even the OCC 2018 Supervisory Operating Plan that was shared last week identifies the focus they will have on ensuring banks are complying with regulations. Karen, did you have another question for me?

Karen: Yes, Kevin, thank you. Let's move on to our next scenario if you don't mind, and this involves third party and vendor management. I know this has been a really hot topic among clients we've been speaking to. In this scenario, an institution has received a first day letter from the FDIC and they're going to focus on the Safety and Soundness exam on vendor management. Kevin, what does a scenario like this mean for a financial institution?

Kevin: Letters like this mean the FDIC is putting your financial institution on notice that they'll be going through a series of customized evaluations. You'll always want to be a few steps ahead, prepared, and ready to undergo these rigorous examinations. In the past, institutions had to find the contracts for your third-party relationships, all of its amendments ensuring they are understood and up-to-date, find the SLAs and figure out how you were monitoring them, get your complaints logs in order, ensure your risk assessment was completed and up-to-date, show evidence of your site visits and identify any issues or gaps, and this is just the start. I've already seen several indications that in 2018, cybersecurity will remain the focus of review, and that goes beyond the walls of your financial institution and includes your third-party relationships, as well.

With all this information, it could be very easy to misplace critical documentation and put yourselves in a situation where you would receive a lower rating. When thinking about how to navigate this process, think of the following on the next slide. What does this mean for the institution, what all is required, and most importantly, how do you manage it?

Again, it's easier with the right technology. The GRC Spotlight Vendor Management Module allows you to identify, assess, document, and store adequate due diligence needed to properly monitor the relationship, as well as monitor any controls, policies and procedures, business continuity, complaints, and gaps or issues associated with the relationship all while working out of the same cloud-based software solution. In addition, it allows for reporting to include graphs and charts that will visually help identify any opportunities.

Karen: Kevin, are you ready to go to our third scenario?

Kevin: I sure am.

Karen: This one is on consumer complaints. What if an institution receives a notification that the CFPB is making inquiries into complaints regarding unauthorized credit card accounts being opened?

Kevin: Karen, a lot of this comes down to asking the right questions. How do you identify a complaint? How do you get the entire company to understand the complaint policy? How do you manage complaints? How do you retrieve documents and manage complaints from a client as well as from third parties? Analyzing this data is critical. It could help direct you to the problem. Even with the right plan in place, you will have consumers complain about your institution. That's just the nature of the beast; you'll never make anybody happy.

When this happens, you'll need a platform that will allow employees to enter and manage complaints, allow them to be shared, prioritized, and monitored to determine any relationship impacts with your third parties. The GRC Spotlight provides an instant management module to enter and manage complaints, allowing for them to be shared, prioritized, monitored, what the complaint relationship is to the third party, and to open projects as a result of mitigating the incident in one centralized solution.

Karen: Kevin, we're rolling along here, and just for our audience, I'll mention that we are taking questions. We've got a couple of them already lined up in chat, but if you do have questions, feel free to put them in the chat box in your control panel and we'll get to them at the end of our session here today.

Kevin, I'm going to move on to our fourth scenario, and this one involves policy and procedure management, which could include policy development, review, and implementations. In this scenario, we have an account holder who is badmouthing the financial institution on social media. An employee took it upon herself to try and correct the account holder, and in doing so, provided inaccurate information on social media. Because of that employee's action, the institution was sued. Fortunately, the financial institution had a social media policy which outlines the proper way to address such circumstances and the employee signed an acknowledgment that she had read the policy. The employee couldn't rationalize her actions and the financial institution ultimately was able to terminate her.

Kevin, managing social media policy can pretty tricky, I imagine. How do financial institutions navigate in situations like this?

Kevin: Great question, Karen, and you're right. Social media has just taken off and we're seeing it be used for a lot of different ways. Clients are voicing complaints. Some of the employees may take it and try to address it themselves not really realizing that a social media policy even exists. Institutions today are not only required to develop policies and procedures, they're also responsible for communicating, updating, and providing evidence that they have been read and understood.

Many of the banks may be supporting policies with educational courses like BSA, AML, fair lending, etc., but that hardly covers every policy. Remember, it's critical that they're not only posting them but that you're ensuring that your employees are reading and understanding those. That's often hard to show evidence.

Today, this means policies may be in various folders and drives, and record our manual process to create, review, and share them and not necessarily capturing if they were even opened. Policies, while they may seem administrative and cumbersome, can also be subpoenaed in court and could save a bank from reputational risks, fines, and penalties.

To cut down on administrative frustrations, institutions should employ a technology that allows them the ability to create, approve, store, assign, acknowledge, version and archive policies and procedures, as well as assign them the various controls all within the same application. There are many technologies out there now that do live document edits, but few like GRC Spotlight that can also detect and note any exceptions or exemptions to the policies. I find this is often overlooked by banks, that they are not really capturing any exceptions or exemptions to the policy, and then when auditors come in and identify that somebody did not exactly follow the policy, they're scrambling to find some proof that it was either an approved exception or an exemption.

Specific to our hypothetical scenario, the GRC Spotlight would have allowed the institution to store their social media policy on the dashboard, and they'd be able to share it with the entire institution as well as capture proof that the employee read and signed the policy. This could be priceless in the circumstance in defending the financial institution's reputation.

Karen: I think we'll probably be coming back to this one with some questions. I'm going to pose our fifth and final scenario, Kevin, before we get into questions, and I've got quite a number of them here lined up. This scenario involves risk assessment and management.

We all know that credit card and debit card fraud is at an all-time high. In this scenario, a financial institution is employing a new technology to significantly reduce loss while maintaining a solid reputation for security and prevention among its account holders. One of the newer controls in our scenario that they're using to mitigate risk is issuing chip cards. They're taking other preventative measures as well, such as monitoring account activity and notifying the account holder when they observe unusual activity. Cards is just one area of risk. There are lots more, of course, as we know. How does an institution navigate both finding and managing where their risks are?

Kevin: Good question. Technology solutions today are really driving banks to answer the demands of their customers by providing convenience and to remain competitive. As a result, they take on challenges that may not have been considered in the past. However, properly mitigating the risk with balancing control is critical. Institutions know managing risk is critical, but conducting risk assessments and obtaining the view of multiple subject matter experts to weigh in on risks associated with the item being assessed is problematic and without proper tools relies on the manual process.

The solution to this scenario is to probably map every kind of risk with a control. In order to do this, banks should consider some of the following on the next slide. Conduct an assessment. Obviously, that's where it all starts, but making sure that you have a very thorough assessment involving various lines of business and expertise through your IT security, all areas of the bank to actually weigh in on this, evaluate the process, the product, the system, whatever it is, to identify all the risks. This is often challenging. Also allow for multiple areas to provide the assessment, which requires a great deal of coordination. When you're looking at IT, and legal, and compliance, and risk, all these areas to weigh in, it obviously requires a great deal of coordination and timing.

Also want to make sure that they link the risk to the control, provide any residual risks, track and monitor the risks, identify gaps, provide gap analysis and solutions, track the implementation of mitigating factors. If this sounds exhausting, it is. It's easy to see how things can fall in between the cracks without the assistance of a tool. The GRC Spotlight Risk Management Module allows institutions to do all the above, and it also allows for a more holistic view of risks impacting the business.

Karen: We're going to come back to a number of these things in some of the questions, but before we get to questions, I would like to see if we can go to the next slide, and would you mind talking about the giveaway that we're offering to the folks who are attending today's webcast?

Kevin: I sure would, Karen. This is pretty exciting. I wish we could actually offer this to all the participants, but we do have a great opportunity to own the GRC Spotlight Solution, and we are offering three attendees of today's webcast a free one year, which is a $60,000 value. You've already taken the first step in qualifying, and that is that you must attend today's live webcast in addition to participating in a phone-based needs assessment with a Harland Clarke representative to become eligible. Winners will be contacted directly, and I just wanted to wish everybody luck on that and thank you all for attending. I think we do have some questions out there. Is that right, Karen?

Karen: Yeah, we do have a number of questions. Kevin, I just want to clarify on this giveaway, if I could. It's available to folks who are attending in attendance today, correct?

Kevin: That is correct.

Karen: The other requirement, if I understood, is that there will just be a needs assessment that we'll do by phone with those who are attendees, and that would then qualify – completing that needs assessment by phone would then qualify them to receive one of these free tools?

Kevin: That is correct. A Harland Clarke representative will be reaching out with that needs-based assessment call.

Karen: Okay, cool. That sounds like a great value. Alright, questions, here's a big one. When do you think banks might get some regulatory release?

Kevin: If I had a crystal ball, that would be great, but it's really hard to say. Unfortunately, it seems as though banks continue to make headlines, and as long as that continues it's going to be a really hard argument to make any movement on deregulation. We see quite a bit going on with fraudulent activity, cybersecurity issues. It all goes back to banks. It's going to be a hard argument to say hey, you need to – the government to ease off on us a little bit, yet we continue to remain in the headlines. It looks like we're a bit out in the future on that one.

Karen: Here's our next one: it's with respect to vendor management. The question being asked is based on some current events, do you think banks will get more federal guidance with respect to vendor management?

Kevin: It's hard to get away from the headlines that are out there and I definitely see more guidance and more scrutiny, especially in the area of cybersecurity. With banks, one of our most important assets is our customer's information and we need to really ensure that we are safeguarding that, not just within the brick and mortar walls within our institutions, but it goes even beyond that when you start to consider our third and fourth parties. I think our oversight should extend to them and also be very aware of what they are doing to secure our clients' information or your clients' information.

Karen: Kevin, another question is on that same track of vendor management, and the questioner is asking earlier in your presentation, you talked about a technology that could help you keep track of documents, and store due diligence, and that sort of thing, and so how is that more advantageous than the ways in which this person's financial institution is doing things today?

Kevin: The GRC Spotlight cloud-based solution really is – it takes seven different modules. You have audit, you have risk, you have compliance, you have business continuity, vendor management, information security. It brings them all into one solution. With my experience in working with the banks I have and also in visiting with other banks, they tend to be using tools like Excel, Word, Outlook, or they may be using a software solution but only using it for one specific purpose.

With the GRC Spotlight solution, what you do is bring all that into one solution so it gives you a more holistic view of the risks. It allows you to identify the controls; it allows you to document and keep all the evidence in one central repository. The benefits of this solution far outweigh anything that's being used in most of the branches that I've talked with today. At the end of the day, when auditors or the Fed come in, they want to see evidence and you have to be able to show it. if you can't find it because it's out in some drive somewhere or it's in a tab in an Excel spreadsheet embedded and you can't seem to find it, it's not going to fair too well on your audit.

Karen: Kevin, one person has asked a question. Actually, I've got two questions here that are very similar. One asks even if they aren't the recipient of one of these free GRC Spotlight solutions, how can they find out more about the tools that they might win? Someone else asked a related question, which is we talked about a few scenarios here. Where can they learn more best practices? I'll just go ahead and answer that for our audience and tell you that more information about that is at harlandclarke.com/grc. You'll find lots of information there, and also in the Insight Center, which you can find in the top navigation tab on the Harland Clarke website.

We have a CFPB question that came in. The CFPB really seems to be focusing on complaints. What can be done from a proactive perspective?

Kevin: They definitely are focusing on complaints and they're doing some trending and trying to help banks really understand some of the issues that they may have. The CFPB is also about communicating, being transparent, and educating your clients. I think this is an area where improvements can be made. I don't think we're maybe communicating as well as we could or should be, and certainly may be not as transparent as we could or should be, as well. Educating the clients, providing them with tools to explain some of the complexities of banking might save yourself from having to address a complaint in the long run.

Karen: Thank you. I'm going to remind our audience that chat box is still open for questions. I've got a couple more here in queue, but if you do have questions get those in and we'll make sure that we get to them before we finish up here.

Our next question, Kevin, is if we're talking about automated platforms, should there be multiple teams that have access to the platforms or multiple parts of the organization, or should these platforms or the platform be available only to the risk teams?

Kevin: I think certain aspects should be accessible to everybody, but then other aspects should be reserved for various groups. If it's talking about a risk assessment, do branch personnel really need to be aware of that? Probably not. That would be more for the risk group or a chief risk officer. Again, with the GRC Spotlight solution, you have the ability to limit the use or the view of the recipients or your team members out in the bank.

Karen: I see one last question here in chat unless some others pop in. This is a big one. Can an automated solution predict or even prevent a major event like a breach, and if it could, how would that be?

Kevin: It's hard to say. Could it prevent or predict? That's pretty strong. I think with the proper tool being the GRC Spotlight, its goal is to identify risks and make sure that you have controls in place. If you don't, you have a gap and that's where vulnerabilities can happen, is in the gap. If you don't see that, how will you know? When we talk about some of the current issues that are happening out there, I think they're more of a technology-driven issue. Could the solution have helped that? I think so. I think certainly it can allow you to be more proactive and maybe cue in on some of those areas and allow you to go beyond just checking the box but actually managing a relationship or managing a process. Once you really understand that and know it from end to end, I think it will allow you to be better positioned for when the next breach happens, and it will happen. We all know that. It's just a matter of when.

Karen: Right, just a matter of time. Kevin, thank you. That was our last question in queue so I just want to wrap up and say thank you to everyone who attended today. We've appreciated you being with us here today. I hope if you're interested, you'll take advantage of a needs analysis by phone and the possibility of receiving one of our GRC Spotlight solutions, which Kevin, you mentioned it was a $60,000 value. For those of you who are looking for more information, whether it's on the solution or on best practices, if you'd visit harlandclarke.com/grc, there's lots of information there. Thank you all very much. We appreciate you joining us today.

Nathan: I would like to remind attendees that we will send out a brief survey after this webcast and we welcome your feedback. Thank you, and that conclude our