South Central Connecticut Regional Water Authority
Audit-Risk Committee Meeting
May 26, 2022
Meeting Transcript

[AUDIT-RISK COMMITTEE MEETING BEGINS AT 12:31 P.M.]

David: First, I want to welcome Jay, RPB member. Thank you for joining us. Appreciate that.

Jay: Thank you, David. I'm happy to be here.

David: Good. Good. All right. And Catherine, I will hand it over to you for your committee.

Catherine: Good afternoon, everybody. First item on our agenda is the approval of the minutes of the meeting of February 24th. Entertain a motion.

Suzanne: I'll make a motion. I'll make a motion to approve the minutes as presented.

Kevin: Second.

Catherine: Okay. Is there any discussion? Any questions? Any corrections? See none. All in favor, signify aye.

David: Aye.

Kevin: Aye.

Catherine: I saw two ayes. Did you vote, Suzanne?

Suzanne: I did. Can you hear me?

Catherine: I can hear you now. Thank you.

Suzanne: Okay. Thank you.

Catherine: All right. Any opposition? No opposed, no abstentions? Motion carries. Second item on the agenda is the risk update. Donna and Amanda are going to walk us through the risk update.

Donna: Great. Good afternoon, everybody. I'm pleased to walk you through a risk update. Joined with me here today is Amanda Schenkle, who's the manager of EHS and Risk. So Jennifer, do you have the presentation that you could pull? Okay, great. Thank you. Can we go to slide two? Today, we're going to provide a high level overview of our risk strategy update of fiscal year 2022 strategic goal update and objectives, and update on our top 10 risks. We're also going to

provide an update on our commercial businesses, specifically related to the recent acquisition. And then we're going to wrap up with the summary and next steps.

Donna: We can go to the next page, just from an overall perspective of our risk strategy, the RWA established a cross-functional Risk Committee. You might have seen that back in our December report out where they shared the specifics of the team. That team is really focusing around helping identify risks, impacting the RWAs ability to deliver its products and services to our customers and constituents. The team consists of approximately 11 employees, who are cross-functional and focus on periodic and ongoing monitoring, risk ownership, decision making, and our day-to-day operations. So far, you'll see down in the methodology section, they have identified 47 risks in which we have identified using the four perspectives. So under the customer constituents, they've identified eight risks. Under employee learning and growth, five risks. And on the financial end, 16 risks. And with our internal business practices and processes, 18 risks. They are utilizing the COSO framework to rate each of the risks. And we're going to talk a little bit about that, because each of the risks are identified by gross, current, and residual risks, which talk about impact and likelihood.

Donna: The COSO framework, as I mentioned, is really to assess the internal processes. So if we move to the next slide, this one, the landscape, as part of our risk strategy, the Enterprise Risk management includes methods and processes to manage risks and opportunities related to the achievement of our objectives. So you'll see in the middle, we've got the ERM. And the objective of this landscape, overall, is to really help develop a holistic view of the most significant risks to the achievements of our most important objectives. So you'll see a whole host of things around the outer circle.

Donna: The inner circle, we have identified areas that have broader impacts, such as reputational and geopolitical. Reputational risk is a hidden threat or a danger to, basically, the RWAs name, or the standing of a business or entity unit. So these can occur through a variety of different ways. So that's why it's on the inner circle, because it does impact us overall. The geopolitical risks are things known as political risks that really affect the normal course of what we do. So you heard more recently the government relations report out in the last meeting, and that would be an example of political risks that impact our business.

Donna: In the outer circle, we have identified three major elements tied to this ERM. So you'll see the strategic risk, where we've identified three major areas. And basically what the strategic risk is, is referring to events or decisions that could potentially stop an organization from achieving its goals. Examples could be mergers and acquisitions. It could be contractual obligations, or maybe even some other liabilities. So we've identified business risk, obligation risk, and insurance risk in this area. On the financial side, these are risks that are related

to the possibility of losing money. Some examples include audit risk. It could be the general bond resolution compliance. It could be the rate application approval, or even failure to meet budget projections.

Donna: And then you'll see the remaining pieces are really tied to our operational risks, and these summarize the uncertainties that we may face in the course of conducting our daily business. It could be policies, procedures, it could be systems, it could be even activities. And I'll just walk you through a few of them. I won't spend too much time going through every single one of them. But as an example, going to the far right of the diagram, you'll see regulatory compliance. These could be environmental compliance. It could be functional risks as well. You'll see legal risks. These could be things that are tied to vendor contracts, or even events that are legal in nature.

Donna: Systems are kind of scattered throughout multiple areas, but the system side, it could be areas such as cyber security or even a breach of our systems, like loss of data. Physical assets would be another example, where we've got ATVs on our property, which are creating security concerns for the business. That would be another example. Safety injuries, that's obviously front and center and a goal for us, but that would be another one. But we could also be thinking about things like fraud, where we've got customers making payments, and we want to think about any internal, external fraud and what we're doing with that banking data and making sure that we're looking at that. And then water pollution and quality, this is really around things like chemical risks in our drinking water.

Donna: So this landscape, as I shared is really... It's just helping tie back to our strategy and really helping us just take a more holistic view of what are the most significant risks to our business. And this is going to be evolving as we further dig into our current strategy. Next slide?

Tony: Excuse me.

Donna: Yes.

Tony: I have my hand raised, but I don't know if that's the right way to do this.

Donna: Okay. Yes.

Tony: Over time, I've had a continuing view that the reputational issue is one that includes the chief executive officer as well, more so than any other employee. And to some extent, almost equal with the organization's reputation as such, because the chief executive officer represents the organization and gets epitomized as a leading element in the organization. So we ought to think about where that fits, if anywhere, because I think it's an important one.

Donna: I agree. And that, obviously, could be easily falling into a number of these categories, but definitely reputational, as you had referenced.

Jay: May I ask a question?

Donna: Of course. Yes.

Jay: The risks that we're exposed to, do we have any insurance policies that we have covered? Did I miss something maybe in the beginning?

Donna: The insurance risk is covered under strategic. So if you look up at the top, we have insurance risk.

Jay: Okay.

Donna: Mm-hmm (affirmative).

Jay: Thank you.

Catherine: Suzanne also has her hand up.

Suzanne: Thanks, Catherine. I have two quick questions building on Tony's point. I think it's not only reputational risk, but there's key man risk, or key person risk-

Tony: Yeah.

Suzanne: ... in terms of losing key or a number of key personnel.

Donna: Yeah.

Suzanne: And secondly, where would you be tucking credit rating risk?

Donna: Credit ratings would more than likely be under the financial, that would end up focusing there. We were trying to identify the higher level ones, but you've got rate application approvals. But I would see that as being strategic and financial.

Suzanne: Yeah. I think [crosstalk]

Rochelle: Just to add to that, Suzanne.

Suzanne: ... called out. I think it's one of our biggest risks, actually.

Donna: Okay.

Rochelle: And Suzanne, maybe just to add to that, I have that under the budget projections and funding, because a very key thing there is the impact from the credit rating agencies if we don't make our projections.

Donna: And credit risk is-

Suzanne: Wherever you want. It's a big factor since we are highly reliant on borrowing.

Rochelle: Yeah.

Donna: Absolutely. Absolutely. Any other questions on the risk landscape?

Donna: Okay, wonderful. So one point that we just wanted to share is the Risk & Compliance group sits under the corporate services division. The reason it is a standalone function is to ensure the pure risks of losses were managed appropriately and to mitigate liability. So as an example, Amanda has got a team of people, and she's here with me today that really is looking at overall risk and compliance, such as environmental.

Donna: So on the left hand side, you're going to see one of the strategic objectives is to really help cultivate a risk culture and mindset. And the way that we do that is by aligning our strategy to our risk appetites, bringing an objective voice to the table, driving basic risk values and norms, and really helping improve the risk mitigation execution. So as an example, if you take environmental, we've got a team of people that focus on the environment and doing things for the environment. But we have Amanda's team, who's focusing on environmental compliance, where they're auditing what they do and how they do it and how it compares to the regulatory environment and making sure that we have a distinct separation between those groups.

Donna: On the right hand side, you'll see our near-term objectives. This is really where we're trying to build the capabilities and improve. Our objectives are really to help, improve, identify, assess, control all the risks. And really, the way that we do that is by establishing robust operating rhythms and continually reviewing the risks and helping put plans in place. Handling the immediate issues as an example for safety. As an example, we've got a safety injury, how do we help mitigate that? If we've got a legal issue, we're resolving those. If we've got an environmental concern, we're putting those plans in place immediately. And even with BCP gaps, as an example, we're really trying to make sure that we're putting out those fires as they come.

Donna: But in addition to that, two other things that we're helping build risk control dashboards, so really, Amanda's doing a really nice job and looking at all the risk, and you'll see in the appendix a bunch of crafts and things like that, and trying to really help identify those risks, where are the warnings, and put mechanisms in place to help mitigate those. And then finally, improving our risk

mitigation tools and bolstering internal controls. So really helping look at the processes of how we do things, auditing our internal controls, and making sure that we put processes in place to help get us to a place where we can mitigate some of the liability across the business.

Donna: So I'm going to pause and just see if there are any questions on this, because we're going to now walk through the fiscal year '22 goals and objectives. I'm going to have Amanda focus on that. But any questions in terms of how the group is operating and what their focus is? Okay. With that, I'll pass it off to Amanda.

Amanda: Thanks, Donna. So we'll walk you through the 2022 goals and what our update is here. So as you can see, as part of our risk strategic goals, we are in the five year plan for 2025 to enhance RWAs enterprise risk by reviewing and improving upon 50% of the risks within our risk matrix. We're focusing on mitigating risk, improving redundancy, and safeguarding our resiliency as part of this goal. Our objective for this fiscal year was to reconstitute our committee and focus on our top 10 enterprise risk and their mitigation strategies. We were able to use, revise all of our divisional leaders, to make sure that we had a current committee that represented a cross-functional team. We introduced our new risk assessment guidelines as part of this objective, and we reassessed all of our top 10 risks against those new guidelines.

Amanda: As you can see here in our risk assessment, our top 10 includes 19 specific risk assessments that have to be conducted. All of those assessments were conducted using the COSO framework assessment guidelines Donna had mentioned previously. We rank those assessments with our gross risk, which is prior to any controls being implemented and then our current risk, which is with controls in place. The overall risk profile for RWA was impacted by the change in this framework, due to the multiple layer assessments that are provided in the guidelines versus a more simple process we used prior. You can see here in the framework, we did include a copy of what is one of our risk assessments that we perform. It identifies what the impact is to the business, what the consequences are of the risk, who the owners are, and then it works into what our existing controls are in place.

Amanda: As you may have been waiting for, here is our list of our top 10 risks as they were assessed with our new COSO framework. We have included the top 10 ranked by their current risk, which means these are all ranks and current controls in place. On the far right hand side of this chart, you'll see the change in rank that they received based on the change in framework, and we've also included all of the risk mitigation activities that took place this fiscal year.

Amanda: Within our business continuity planning, you can see we updated all of our plans, both overarching to the business and department specific. There are 27 department specific plans nowadays. We updated our incident management

plan, we worked on our water supply plan and our drought contingency plans as well, which all fit under the business continuity planning umbrella. Within our cybersecurity world, we worked on our cyber assessment, which was completed this fiscal year. Our continued penetration testing, launching new user training related to [phishing] exercises. Multifactor authentication was introduced on all of our privileged accounts. And then we also are working on planning our business continuity tabletop exercise, which will be a ransomware attack on our distribution system. I'm going to pause here just for a second to ask Prem if he has anything he'd like to add to this area. I know we had talked about it a little bit in detail.

Prem: Yeah. Before I can add, Suzanne, you have a question? I see your hand is up.

Catherine: Thanks.

Prem: Suzanne, you're still on mute. You want to-

Suzanne: Oh.

Prem: Yeah.

Suzanne: I have two questions. One is, how did we determine these were the top 10?

Amanda: So these have been our top 10 for the last, probably I want to say three years. They all have a risk rank that is higher than the rest of ours. So there are 47 risks within that risk matrix that we hold. These are 19 of those 47 with the highest risk level. So these are ones that are constantly being watched, constantly having controls updated. And we rank them here based off of their current risk level, which is their impact times likelihood of occurrences.

Suzanne: And how often do you do the rating that ranks them?

Amanda: We usually try to look at that at least once a year. The most recent ones were completed in April of this year as part of this framework change.

Suzanne: Okay. And are these in priority order, or just the top 10?

Amanda: These are the top 10, and they're currently in rank order by their risk level, which is just the impact times likelihood.

Suzanne: Okay. [crosstalk]

Catherine: Amanda, you said that this... I'm sorry, Suzanne. Did I interrupt you?

Suzanne: No. Go right ahead. My next question is less related to what I was just asking, so go ahead.

Catherine: Well, you said that the top 10 are constantly... There's a constant focus on those. That doesn't mean that the other risks are not reviewed constantly, does it?

Amanda: No. The other ones are reviewed as consistently. It's just with these ones, we like to provide a more updated assessment guideline, where we're not looking at just the controls in place, but we're really addressing what their risk levels are. Unfortunately, in the water world... So I came from a private sector prior to this role. And in the private sector world, I was in risks change very, very frequently. In the water business, I've noticed that our risks are fairly steady. They stay fairly similar across the board. We will always have a business continuity planning risk, just because of the nature of where we are and our proximity to the water weather events, and just the fact that we are a 24/7, 365 business.

Catherine: Thank you.

Suzanne: I have two other questions. One of the things we talked about at one point, I think maybe it might be when Linda was still here, I'm not sure, was that when we looked at the factors, we looked at factors related to urgency. I can't remember what the categories were, that helped drive how important these were. Because I just look at succession planning and recruitment, I just mentioned key man, but I don't see that as a top risk that has to be watched morning, noon and night, kind of urgency type of risk. So I was just wondering where that whole... We had some other layover that looked like an urgency factor and some other dimension that gave it some depth. So that's one question. Then the other question was... Well, I forgot my other question. So if you can answer that one, maybe I'll remember it by the time we get back to it.

Amanda: All right. I'm just going to... I'm going to flip through to the appendix just, to see if this is what you were looking for. So don't read ahead if anybody's looking. I think this might be the heat mapping that you had seen prior, where we talked about our urgency in process. Does this look familiar to you, Suzanne?

Suzanne: No, it doesn't.

Amanda: Okay.

Suzanne: But that doesn't mean anything.

Amanda: No problem. So when you were looking at that top 10 before, so this is the current risk map. So you can see where these risks are seated within our heat map. It helps us to really identify what needs to be addressed right now versus what needs to continually be watched, and what we may be able to maybe let not be a priority as much as some of the others. So when we look at them, you can see with our gross risks... So this little guy over here in the very far corner,

that's one of Prem's cyber items that, while we've taken down the likelihood quite frequently, the impact would still be fairly high to the authority if it were to occur. So it still has a fairly red marker, but the rest of them have all moved quite far into the yellow based off of our controls.

Catherine: David also has a question.

David: Yeah. Suzanne, you're all set? I didn't want to-

Suzanne: I am, David. Go ahead.

David: Okay. Thank you. Thank you, Catherine. If we could put that top 10 list back on-

Amanda: Absolutely.

David: ... I will tell you, I know that we've always had the business continuity planning as a very important one. I know even Kevin attended one of those, if I remember correctly.

Kevin: Yeah.

David: And some exercises with that. But this one, when I saw this the other day looking at this, it screamed out at me, COVID. And it screamed out at me, because of the fact that we were scared about our operators, the very important people that do the day-to-day stuff right inside our plants, that they had to be separated from one another and had to use extra precautions. And I wondered what came out of COVID and how that affected what your plans were here, because we've gone through a sea change in a lot of ways.

Amanda: Yes. So within the business continuity planning world, we used to have many plans built around how we would get all of our staff into remote trailers and specific areas. And we've noted that, barring connectivity, so as long as everyone has power and wifi, for the most part, we really don't need those emergency resources as much as we had before, because we can send our people out into the world as long as they have the connectivity plan. So it's really helped us drive down a specific number of people who are needed as the core business, that we're going to need them here, we're going to need all hands on deck. But we've found that a lot of the ancillary support function to the business really aren't going to need as many dedicated spaces, which is going to be a huge help in how we move forward in our business continuity planning.

David: I would-

Prem: [crosstalk].

David: Yes, Prem. Sorry.

Prem: I was just able to say, there's also a very key focus, David to your point, on things like manual intervention. So one is technology and wifi, like how Amanda was saying, but there was also the other piece where, for example, if there's a cyber attack or even the tabletop that Amanda was talking earlier, where I know there was a question about, can we operate our systems manually, like water treatment plan or distribution system? So there's a key aspect of the people there. And I believe the plan is that, as part of the exercise that Amanda talked about, we are going to be exercising that to showcase that we can operate. So there's the whole portion of technology and the whole portion of people aspect, and that's a great question. And the team is formulating that plan, and we'll be doing that exercise. So I just wanted to add to that.

Catherine: I see Suzanne has her hand up, but I also just want to follow up on one thing that Prem just said and the importance of the ability to operate manually. Because having access to the internet is great, but if we lose power, access to the internet goes away. So I really just want to emphasize the need to be able to operate manually as well.

Prem: That's right. Yeah.

Catherine: Suzanne, you got a question?

Suzanne: Yeah. Just one other question about, so you have an item on the list, I heard Amanda talking about assessments. I heard her talking about exercises and testing into risk. Do you have a model in which you have several steps in the risk management process of assessment testing, responding, re ranking, or action kind of thing?

Amanda: So we do have plans in play that we do, and all of that is captured, actually, by risk in their documentation. So we have what's known as a perspective, which was that the photo I had shared with you on the last slide, where it mentioned who the risk owners were. In there, it talks about how many times that paper has been updated, how many times we've added controls through it, what the dates are on those, what tests have been implemented, and what the ranking changes are. So we capture all of that by risk specific in its own documentation.

Donna: But I think to her point, Amanda, maybe you can elaborate is, the process in which we use to do that ranking. So for example, we're looking at growth risk, current risk, residual risk. We're also looking at the probability of the impact, the high, medium, and low, and how they are given different rankings. So if they're categorized as a low impact, they would be ranked one or two, where if they're a high impact, they'd be ranked four to five. And then we also look at probability. So can you just talk through that philosophy? Because I know that

was reported back out in May of 2020, but it's been two years, and I think that might be helpful for the group.

Amanda: Absolutely. Yeah. So as part of impact, we go back and we look at six specific categories based around our legal, compliance, health and safety, reputational risk, operational risk, and strategic goal risks, and we rate those based off of what the impact would be to the business. That ranking is then assessed against what the likelihood is based on the number of controls we have in place and how often that may occur. And that process is then updated by each risk that we see. Within that terminology, when we are looking at those assessments, we also make sure that all of the testing of those are completed, and that they have controls in place and mitigation plans in play. So within the top 10, there should be activities that are taking place that continue to further control out that risk. And then those controls are then implemented and categorized against each one of the risks.

Suzanne: So I just have one last question, and that is why the loss of the SCADA system has gone up in risk factor. Is that from last year it's gone up?

Amanda: Yes. So that... Yeah. And again, so our previous assessment process was actually on a one to three scale, and then it assessed it on a percentage probability. So we're now on a 25 point scale based off of the newest assessment guidelines, so a maximum of five in the impact, and a maximum of five in the likelihood. So we now have a greater scale. So what you're really seeing in the ranking change is that we went from a really rudimentary scale to a much more complex scale that takes into it very specific impact categories.

Rochelle: Maybe I'll just add to that. I think-

Suzanne: So does that mean that risk, the absolute risk has actually unchanged? It's just because you changed your rating system, it moved up in the process?

Donna: Yeah.

Amanda: Correct.

Donna: Yeah. So for example, for succession planning, two years ago, it was ranked at five. Now, here it's down at six. And the reason why that the ranking went up is because we've developed a framework and we've actually started the succession planning and we're starting to put plans in place. So as a result of that, it gets assessed on what was the work that was needed, and how did we progress against that? And therefore, the ranking shows that it's improving.

Rochelle: And I just want to also add, the COSO framework that we're now using, and I think we talked about this in the last update, is a very recognized framework across... In the know publicly traded companies and companies that have to

follow Sarbanes Oxley, it's definitely the recognized framework to use to assess risks.

Catherine: I also notice that business continuity planning moved from nine to one. And what I think is interesting about that movement... And I think it makes some sense, and maybe this is a lesson learned from COVID, and correct me if we're wrong, because if we have a number of employees that are working remotely because of a pandemic, and then on top of that, there is a weather event that takes out the electricity for a period of time, then I think that you're going to have significant challenges with respect to business continuity, at least for a period of time. So planning for that and being able to respond to those layers of challenges, I think, is something that needs to be of high focus.

Amanda: Absolutely. And I just wanted to, with business continuity planning, that's a very large bucket, because it is anything that has an impact to business that would prevent us from meeting our core mission. So any moment where we're unable to perform our duties as a water company, that fits into that bucket there. So when you see in there with the water supply plan and our drought contingency, so there's a lot of layers within that business continuity planning, which... And unfortunately, anytime we implement our instant command system, it really flies into that same area as well. So we do see that within... Just maintaining our core business, as well as weather events, we see the likelihood is very, very high for need.

Catherine: I don't see any other questions.

Amanda: Okay.

Catherine: And we can move to the next one.

Amanda: There we go. Okay. So we just wanted to provide a quick risk update on the commercial enterprises side of the house. My team has been working on the insurance pieces for all of our new asset purchases. So with the WSS acquisition, we were able to get them covered under our captive, which is Churchill Casualty, LLC. As a captive member, RWA was in a position to bring them in on a zero premium dollars based on the exposures falling below 10% of RWA's total exposure. When I mean exposure, that would be our revenue, our payroll, and our auto counts. As we continue to move through the M&A world at RWA, we will continue to reassess the insurance program. Based on our current exposures, we start getting into a position where these smaller companies we've put up against minimum premiums, and it's not cost effective to have them purchase their own policies over and over.

Amanda: So as we are able to get a good risk profile for this program and make sure they have a good broad spectrum of exposures, we're going to actually work on how

to get them their own insurance program that would better fit their needs. And then Donna, do you want to just mention the people risk side of the house?

Donna: I mean, we had a close and a start within a matter of a day. So we did onboard everybody contingent upon passing a background. So we've been able to successfully onboard the folks.

Amanda: Thank you.

Catherine: I just want to make sure that... I believe before we started asking a lot of questions on the top 10 update, Prem, I thought you were going to add something to that.

Prem: Yeah. I think we kind of touched... Thank you, Catherine. We kind of touched upon the tabletop exercise. That was my point. And one of the things I know in the past where we discussed about cyber security, there was a question really kind of understanding how authority can help RWA. And I think one of the things that we do a good job here, and this is tabletop exercise. We'll exercise it again, where we will include our board members as optional, so they can actually participate and see this exercise being done and how we could manually kind of operate our system, right? So I think this is going to give a good feeling. So more to come, but that was my point earlier. So we'll be kind of going through that exercise and we'll make sure that everybody feels more comfortable. But thank you, Catherine. That was point.

Catherine: I just didn't want to cut you off. That's all.

Prem: Thank you. Appreciate it. Yeah.

Catherine: All right. Back to you, Amanda.

Amanda: Thank you. All right. So as part of our summary, we just wanted to provide that we are on track to deliver against our strategic goals and objectives. Our top 10 risks have remained consistent as part of our recent review, and we will continue to see a significant mitigation against the gross risk to RWA. The committee will plan on it's continued momentum and processing through the mitigation plans for the top 10 enterprise risks. And then in our work plan here that you'll see for fiscal '23, we're looking to introduce five new perspectives to our risk register. As part of our review of our top 10 enterprise risk, we found that these five items deserved their own independent review. So we have added them to our to-do list as items that we plan to add next fiscal year, and we will give you guys an update on those as we work into the work plan for fiscal '23. [inaudible]. Go ahead.

Catherine: I think it's worth having a little bit of conversation, because this jumped out at me about the insider threat risk, and what the RWAs experience has been to date and what the industry's standards are with respect to insider threats.

Amanda: Absolutely. So I'm happy to report that we have not had any issues arise from this insider threat, both on the security and the cyber side. We have great protocols in place for when an employee is leaving RWA to make sure that their access controls are limited, to make sure that their SCADA access has been canceled, and that they don't have any way to access our systems. Within the industry. We are seeing the insider threat to be an emerging risk, especially in the cyber and the security area where outside our outside threats are targeting current employees as part of their way to infiltrate into a business, whether it be through a cyber perspective, whether it be through fraud or any kind of embezzlement type items. But what we want to make sure we're doing is that we're capturing what RWA's risks are to that and what controls we can put in place to make sure that we are not subject to those types of targets.

Prem: And I think, just to add to what Amanda saying, that's a great question, Catherine, right? And one of the key things that the industry, as I'm talking to our peers and others who are actually experiencing this, is that there's a concept called zero trust, right? And from an insider side perspective. So what that really means is that, voluntary or involuntary, somebody who's operating within our network can infiltrate and be a situation where somebody is hacking our system and a bad actor could gain control of that thread because of the practices that's inside. So you heard us talk about multifactor authentication of the systems earlier. That actually kind of talks about this concept of zero trust. So what that really means is that we are trying to create controls within our systems.

Prem: So for example, if somebody has access to our CIS data, for example, they have to actually go back and sign into another system. Although they're in the network, they're being asked to sign up with these critical systems. Let's say the same [inaudible] in this example. The employee goes into a SCADA system. He's asked to sign up. So there's a multifactor authentication concept, which kind of provides more control. That's been an ongoing discussion in the industry, and all our peers are looking to actually put that in place. So we did a good job on kind of creating that for the privilege account, especially for the administrators we have in our group, with an employee. But the idea is that we all try to expand that across the board for all employees so we can create that layer of control and protection. And then different lens, it's also very important from an insurance standpoint. Amanda knows it better than anybody else.

Prem: They actually had asked for the MFA. And just to give you some number and statistics, 65% of the companies have lost insurance coverage because they did not put MFA in place, because of the same reason. So insurance companies are asking of these things more and more. So we are trying to create that control.

And it's changing almost every day. So those are some of the... I would say high levels on what's happening in the industry and how the metrics are changing, especially in the cyber security world. And zero trust is going to continue, right? I think that's the whole idea. So hopefully, it kind of adds a bit more color.

Catherine: Thank you. Any other questions?

Amanda: All right. Well, we are down to the Q and A final here for this update. Within the appendix, you will see there is a slide on our top 10, how they were ranked prior to this new assessment. We've also included the heat maps for the risk, so you can see them in a more managed monitor and low impact quality. And then we've also included the two assessment guidelines from the COSO framework, which are related to the impact and the likelihood, in case you wanted to see what those rankings look like. Any questions? I will stop my share. All right. Thank you.

Catherine: Thank you very much. The next item on our agenda is a review of the work plan for fiscal 2023. Rochelle, can you walk us through this?

Rochelle: Sure. Thank you, Catherine. So for the most part, the fiscal '23 work plan does mirror what it has been in previous years with the external reviews, as well as the risk management update, as well as the cyber technology resilience update. But there is one new item, and it's actually listed under December. And just to give a little bit of background on that is, Larry and I have been discussing what we... Relative to internal audits and what we have done in the past relative to internal audits is, we actually had a third party firm that we had worked with, now a few years back, on internal audits, basically working as an extension of RWA, performing an internal audit function. And although we thought that that particular firm maybe wasn't the most effective for that work...

Rochelle: And then for a few years, we actually did more targeted internal assessments, but not quite an internal audit. And what we're proposing here is working with another third party firm. It's a firm that we now have some experience with. It's CohnReznik. They're doing some work for us on the transaction side, and they do have an internal audit practice. And so our proposal is to work with that firm, initially to do an overall control environment assessment. And then based on that, really focus in from a risk perspective, that you just heard a lot about, where we want to focus our internal audits. And although our external auditor does do certain control testing, primarily on the financial side as part of their like walkthroughs and their interim work, we want to reengage with a risk based focus on internal audits. So the December update will really be an initial readout of that overall assessment and what we would propose going forward for focus areas for internal audit.

Catherine: Thank you, Rochelle. Are there any questions or comments?

Suzanne: I have a question, Catherine. So in this presentation before, there was a slide that talked about a 50% improvement in something related to risk management, 50% improvement of our risk indicators. I don't remember what it actually said. It was at the front of the presentation. So do those get folded into the KPIs? And if so, how so? And is there an opportunity, or maybe Catherine, you do separately, as the chair of the committee, for the board to be briefed on less strategy, but more specifics in the last year, of items that have surfaced, how the team managed them, what it taught us about our organization? And I would presume some of that might need to be an executive session, but I just think it would be interesting, and maybe even more impactful, to understand the individual items and what we've dealt with.

Catherine: Okay. I think that's a great idea. Why don't we-

Suzanne: I think it could be next year in the update.

Catherine: Right. I was thinking we could maybe do that in February.

Suzanne: We can, or we can do it again next May, whatever you think is appropriate-

Catherine: Okay.

Suzanne: ... for the work plan.

Catherine: Mm-hmm.

Suzanne: It might go in sync with this. But the other piece is, how does all this get measured in the... Remind me, and maybe that's a question for Larry, and what that 50% was referring to in the previous presentation in terms of our goals.

Rochelle: I believe... Can I just... I believe that 50% was the review of the risk register, to at least review 50% of the risk register.

Suzanne: So that's what our goal is for risk... So what's the KPIs on risk management then?

Donna: Basically, the biggest good, the biggest goal is to improve 50% of our risk perspectives. So we had 47 risks that were identified. We have to improve those by 50%, which means looking at our internal controls, changing our practices and how we operate. I'm not familiar with this recommendation of the internal audit piece. This is the first I'm hearing of it, that's what this team is supposed to be focusing on, is looking at the internal controls, the processes, and improving those by 50%. That would be the strategic focus for the goals.

Suzanne: What does that exactly mean? Improving them by 50%?

Donna: So that means... Taking, for example, the BCP process, where you look at an area that has a concern that's been identified as a critical area, so going back to those top tens, and then saying, "Okay, we have a major gap." For example, let's say succession planning. There's no succession plan identified. There's no framework identified. How do we improve that? Well, we got to put in place a framework, and then we got to go ahead and start assessing our people. So once those processes start to get completed, then you look and assess, "Okay, what percentage of what you need to do to achieve a hundred percent of that particular area so it's no longer a risk, if you've identified..." Let's say you've done 50% of implementing those new processes and framework and everything else. That would be the 50% improvement.

Catherine: So the measurement mechanism is built into the COSO framework. Is that correct?

Donna: Yes, in some capacities, because she's assessing each of those individual areas.

Catherine: Okay. Okay. So we'll-

David: Catherine?

Catherine: Yes.

David: Oh, if I could just... In reference to Suzanne's comment, the strategic focus on page three is to enhance the enterprise management by reviewing and improving 50% of risk perspectives. So there's 47 perspectives. So you're going to improve 24 of them. You're not... That's how I read it, not quite the way you explained it. That's not how I read it. Or this maybe needs to be reworded or whatever, but my understanding is that if there's 47 of them, you're going to improve 24 of them.

Donna: Yes. But the way you improve them is by updating the processes and practices and implementing all that stuff. So that's how you do it.

David: Right. But Suzanne's question, how do you measure the 50%? And my way of reading what the goal is that 24 of the 47 get improved in some way, and that's how you meet your goal, not 50% of each of the 47. And how do you know what the range is for each of the 47? So I think that's-

Larry: That's correct, David. We're going to improve. 50% of those risks are going to get improved.

David: Yes.

Larry: Not by 50% percent.

David: Right. Thank you. And thank you, Suzanne, for bringing that up. That way, we know what the goal is.

Amanda: And I just want to provide a quick update. We have addressed 35 of those 47 perspectives since 2020 to 2022. So the reason you saw our work plan was to add additional risks to the risk register was because we have, in a sense, already delivered upon our strategic goal plans.

David: Okay.

Catherine: Okay. Are there any other questions? All right. Seeing no further business for this committee, I will entertain a motion to adjourn.

David: Well, I would like to move then that we adjourn as the audit risk committee and meet as the environmental health and safety committee.

Suzanne: Second.

Catherine: Yep. Been moved and seconded to adjourn the meeting of the audit risk committee and begin the environmental safety committee. All in favor, please say aye.

Suzanne: Aye.

David: Aye.

Suzanne: Aye.

Catherine: Any opposed? Any abstentions? Motion carries.

[AUDIT-RISK COMMITTEE ADJOURNS AT 1:19 P.M.]