ERM VIDEO INSIGHTS
Transcript of Frank Fronzo and Bonnie Hancock
Assigning Risk Owners

Bonnie: Hi I am Bonnie Hancock, the Executive Director the ER Risk of the North Carolina State University Poole College and Management and I have here with me today Frank Fronzo. He is VP, Assistant Treasurer and Corporate Risk Officer for Estee Lauder Company. Frank I know in Estee Lauder you place a lot of emphasis on the signing a risk owner to each of your credit corporate risk. And I wonder, just to get started, if you can kind of tell us. I think most of organization might not call them critical corporate risk, if you just define that for us and then tell us about how many you have in Estee Lauder.

Frank: We first started the program and we were determining where would look at everything instruction. We came up with the differences in critical corporate risk and that meet several guide lines we put together to recall risk capital statements. It is about six or seven risk capital statements and those were statements we called them "guardrails". They are able to let us have that conversation about how much risk is too much and things that cross those lines were critical corporate risk or quick cross those lines. So, that not necessary mean they did.

Bonnie: Ok, so things that are potential cross that lines.

Frank: And doing so we are identifying, proximally forty-six critical corporate risk in the company. Now, not all of those as I said we were at risk or needed things done to them or mitigations applied, so we ended up putting together three portfolios. We had an acceptable portfolio, we had a watch list portfolio and an escalating risk portfolio.

Bonnie: Ok

Frank: So the way our program work since we corporate risk management committee and we have risk subcommittees underneath that cover different areas of risk. The purview of the corporate risk management committee and the sub-risk are the acceptable portfolios and the watch list portfolios. The ones that we raise up above those committees to senior management or the committee of the board are the escalating risks. Those of the ones that we deem need a priority focus during the year. So that is how we kind of separate things and we get started.

Bonnie: Ok, ok, that make sense, that's good insight. So tell me about the importance of the assigning a risk owner to those critical corporate risk.

Frank: So as with everything, I think you have to give responsibility to people if you want to get things done. If you someone to look after someone- if it's owned by the entire organization is tough to get something done with that if you need something mitigated. So we wanted to try and establish someone to own each and every risk and whatever possible make it one person, if that is possible. We would start not from the top but from the bottom up, and go to the highest level needed to go to the authority and the commencing responsibility to be able to change that risk. If we went to high, you know the CEO could own everything. We wanted to keep it as low as possible but make sure that person can change the risk. Otherwise, we are giving him responsibility to do something he can't do it.

Bonnie: So they are also presumably having the resources within their organization such that they could deal with that particular risk...

Frank: So we focus around the risk owner as the one that own that particular risk. That doesn't mean that everything would be under control. Particularly mitigation for a certain type of risk could lie in an area that has nothing to do with it – let's say there's an IT component to the risk and that person is not an IT but they're still responsible for the overall risk because whatever IT is doing is mitigating to bring IT to an acceptable level, and so they actually responsible for having for having that person do what they need to do. We bring a responsibility down several levels also. When we have a risk, we start of the risk and the definition of that risk and then a risk owner for the overall risk. Below that we have mitigation strategies and mitigation tasks. The tasks are things that the people actually do to operationalize the strategy. So we have a strategy owner and then we have a task owner, so we can decide responsibility all way down the the chain. Now they're all high level, we don't really get down into the weeds. These are very high level risk - global across the company.

Bonnie: So what do you do to provide some oversight to make sure that the risk owners are properly assessing and following through on mitigation strategies?

Frank: So I mentioned before we have this community structure. So we have approximately seven risks sub committees that report into the corporate risk management committee. The corporate risk subcommittee is made up of the member of the Estee Lauder leadership team so a subset of that and then we have risk sub committees below those for instance in different areas maybe a IT, finance, strategy and is chairperson to each of those committees. Those committees are really charged with identifying risk. We populate those committees with anywhere from eight to fourteen people usually at the VP level or above, and they're multidisciplinary committees not just from one place, so a financial risk subcommittee is not just a financial people. Maybe predominately of financial people, but we have people from all around the organization, because we want to get it a look at it from all angles. You know typically if you ask me how my area is doing, "it is great." It is just a natural response. We want to make sure we get some outside comments and some outside views of that risk. So the other ones identify the risk and then look it over. So the risk owner once… so let me start back a second. At the beginning of the year, we do a survey or interview process which we set down with sixty key executives throughout the firm. And when we first started the program obviously that was where the list of risk come from. Since that we have two ways, we've got the list of the last year and we also do the survey. So the survey we go around to find out how many new risks have arisen - if they are and we don't try to generate more than we have, we try to keep pretty high level and keep them on a short a list is possible. And so then we mesh those two together and we start of with a risk list. We bring that risk list to the appropriate subcommittee where they end up assigning owners if they haven't already assigned. If they're an old risk we may already have an owner assigned, we may update it if people have changed or things have changed, if mitigation has changed, but then once the owners assigned that risk template that filled out goes to the owner and they're responsible for listing the mitigation strategies and tasks and getting the proper people to tell them what they need in there. That template then comes back to the committee and that committee as a whole rates different things on there. For instance, we rate the overall risk on an inherent basis and then we look at the mitigation strategies and tasks and rate those tasks on an effectiveness basis and kind of sum that up to the strategy. And based on the effectiveness on all the mitigation, we come down with a residual risk rating and we rate things on impact, probability and velocity. Based on that, we come up with a risk score combining those three and that kind of tells us what the committee thinks of those risks and depending on where it is, what portfolio goes into, if it comes up to the acceptable level, we're

good, we're happy with it it's a purview to the committee to keep an eye on it make sure it doesn't change and we'll update it throughout the year. The real ones we concentrate on, are the ones deemed escalating risk, if it's an escalating risk then what we try to do is try to find out what we need to do and that template has additional things besides the current mitigation efforts, it has future mitigation efforts are needed and so we task the various mitigation owners to come up with those. And then we say, if in fact we did this, how would that rating change both on an impact, probability, velocity basis and we come down with a future rating - so that's one thing we do. Another thing we do is ask the mitigation owner to provide a risk mitigation effort rating. So for instance, if you look at cyber in the world today, for as far as we can look out cyber is going to be a very high risk – and if you can use the colors – red. No matter what you do, no matter how much you spend but what we want to know from the risk owner is – have we done everything that's best practices, have we done everything that we should and that next dollar we spend is really a waste of money. So, when they may see a red risk but a mitigation effective risk that's green – so, we want to look at those two things in conjunction with each other to determine if, in fact, that's an escalating risk or not.

Bonnie: Ok, and so you use your committee structure really to kind of provide that vetting and oversight and kind of that - control really…

Frank: And that goes up from the subcommittee to the corporate risk management committee which then approves what we done and then with the corporate risk management committee we take them through all three portfolios, all the risks, just to get their buy in as to – do you still believe ratings are correct and that's kind of their responsibility is to let us know they agree with them.

Bonnie: So does any one individual person have risk ownership responsibilities for more than one risk?

Frank: There are a couple of times when you will get multiple people that they may have multiple risks. We have a couple throughout depending on how they fall, for instance, HR type risks, so the head of HR may own two of those risks or three of those risks and that can happen, it does.

Bonnie: So how often would the risk owner have to make a presentation to or meet with you know your C-Suite or your board of directors to talk about how their managing their risk.

Frank: Excellent question. What we do is the corporate risk management meets on a quarterly basis. We try to schedule two presentations from our list of escalating risks at each of one of those meetings. So that they can update the committee on the top risks and what happening with those and what's moving forward. If the committee deems it necessary, some of those will go higher and present it to possibly the audit committee or to the board.

Bonnie: Ok, just to sum up, what kind of advice will you give, you know another ERM leader who maybe is just starting the process and looking at assigning risk owners. What you kind of say is – what you really need to do this.

Frank: I might ask them what I need to do first because that is kind of what I like to find when I'm talking to people is how can I learn, how can I adapt differently, but I think one of the things that is incredibly important is one – is to keep a consistent language throughout the firm so when you're using words people know what you mean by those words. So you asked me at the

beginning what is a critical corporate risk, so we put together a dictionary of terms so that people can understand what we meant by each one of those words. We define escalating risk, we define watch list. So I think that is critical that everybody's talking the same language and then I think the risk owner is probably the most important thing I think in the program, if have somebody that owns that risk it will get action and it will get taken care of and whatever you need will get done.

Bonnie: Right, absolutely. Great insights, thanks so much for taking the time and sharing with us. Thanks.