Sponsors: Corpedia Inc.
Speakers: Alexander Brigham, President and CEO, Corpedia Inc.
Neil Belloff, Executive Vice President and U.S. Securities Counsel, Deutsche Telekom

ASSOCIATION OF CORPORATE COUNSEL
Title: Corporate Compliance Risk Assessments – Methodologies and Benchmarks from Leading Corporations
May 11, 2006
1 p.m. ET

Operator: (Alex), please go ahead.

(Alex Brigham): Thank you. All right; well welcome everybody to this Webcast. We did a Webcast last year on corporate compliance, and this is the next generation with a deep dive down on risk assessments. What we will be discussing here includes discussion of a survey that ACC and (Corpedia) last year with a focus on risk assessments and the results from that. And that survey report is available from ACC, as well as an info pack about how to conduct a risk assessment.

So today, we are honored to be joined by (Neil Belloff), EDP U.S. Securities Counsel from Deutsche Telecom. (Neil's) background Executive President and the U.S. Securities Counsel for Deutsche Telecom since 2003. And he interacts with senior management, the board and all departments as well as the board and executives of major subsidiaries and business units. For those of you, Deutsche Telecom owns substantial presence in here in the United States, his more than 20 years experience in the business legal matters and specific knowledge of telecom, IT, software entertainment and emerging technology industries. And prior to joining Deutsche Telecom he was an attorney with several New York based law firms, including (Propase Rose) and formerly before that he was Senior Attorney Advisor in the division of Corporate Finance at the SEC.

So (Neil), before I get into a little bit more background, is there anything that you wanted to share that I missed?

(Neil Belloff): Sure. First, I have to do the obligatory legal disclaimer, which is that the views expressed are my own, and do not necessarily reflect those of management of Deutsche Telecom or any other enterprise. (Alex) mentioned Deutsche Telecom has a significant presence in the United States. A lot of people don't realize that Deutsche Telecom is the parent company for T Mobile in the United States. And it is the largest telecommunications company in the world.

(Alex Brigham): Thank you, (Neil). And I am, as was alluded at the outset, I'm (Alex Brigham), President and CEO of (Corpedia). And (Corpedia) does compliance and ethics e-learning code of contact training in the risk assessment and software services for corporations over the last eight years, and we're proud to be here.

So risk assessment what we affectionately call elephants in the room. And in going around and discussing this various corporations, you know, it's being driven, obviously by federal sentencing guidelines being a critical component of it. People are finding that one line in federal sentencing guidelines, there's a lot of elephants in the room surrounding it as we call. And for those of you who don't know how elephants get in the room, according to this photo here, they take the elevator.

Some of the major elephants is meeting industry practices, does that equal an ever rising bar and that is one of the elements written in the federal sentencing guidelines is you are expected to meet industry practices, to have an effective compliance and ethics program.

The second major elephant is the hypotheticals, the documents and the attorney client privilege erosion. I'm sure many of you are familiar with federal sentencing guidelines guidance on benefits of waving privilege or at least cooperation with the government and that element was just

eliminated from federal sentencing guidelines definitions. However, it is still in existence under the Thompson memo interpretations which are being challenged slightly into this KPMG prosecution in New Jersey right now.

(Neil Belloff): ((inaudible)) a couple of great articles in this month's (Corpedia) newsletter, you should all read it.

(Alex Brigham): Yes, you can sign up for that on our Web site or on (PLI's) Web site that's correct. And one of the things about hypotheticals is if you go looking for problems or potential problems you're going to find them. And the question is, when you go and do a risk assessment what kind of – what did you write down? What kind of documentation do you have? Because we've encountered companies that have an extensive list of potential problems that could go wrong, and then they find well practically speaking, they might not be able to cost effectively prevent every single problem from potentially occurring, because business is risky. However, if it was improperly put together, then you have the risk of creating essentially a smoking gun if one of those problems were to occur.

Third and fourth is the confusions between enterprise risk management and internal audit, what they might be doing, and who owns the function. Is this an internal audit function? Is this a compliance and ethics department function run within the legal department? Do they do it jointly together?

And then, finally, you know, as noted, risky behavior cannot be prevented. I mean we are in business, we're all in business, and we all assume some form of risk. So the question is if you know that something could go wrong, what's going to be the form of analysis report that's going to be most defensible and (Neil) can certainly weigh on that. (Neil) has experience back at the SEC when he talks about his slides.

Some of the – some of the statistics that come out of it, this is the slide that I probably call empathy, if I had a subtitle to this slide. And that is, a lot of people say we don't have a lot of budget, we don't have a lot of staffing. You know, to get a sense of where companies are, one out of every three companies has somebody who's a chief ethics officer overall, and that's usually chief ethics and compliance, and very rarely is it an entirely separated function. And it doesn't necessarily have to be titled exclusively as that. They could have multiple positions inside the company, we come and we see them. Sometimes, in some companies call the general counsel, depending on the size is that same chief ethics officer as well.

But what is the full time employee equivalent in your organization. And this is an important statistic to look at and naturally it varies dramatically. This is just in aggregate by, you know, all companies that respond to our surveys in our database. We have over 800 companies in there. But 30 percent of them have one employee or viewer. They really don't have a substantial department, so they lean on outsiders, they try and be creative. And that certainly limits what they're able to do, whereas there are, you know, a fair amount – some organizations that are very, very well staffed. But more than anything else, it is not a highly staffed function in your average company. And we find the disparity even within industries is pretty significant.

(Neil), do you have any insights that you can share, or be willing to share in terms of ((inaudible)).

(Neil Belloff): Yes, it's also a function of the type of organization you are. If you take Citicorp for example, that's a banking institution that's worldwide, they have over three thousand ethics officers world wide and it's – you know, you can understand because of the nature of that business but it also depends whether you're a multi national enterprise and, you know, how large you are. I know that our company is – we have 400 subsidiaries, 250,000 employees. We're in 69 countries. And I can tell you that our ethics department is rather small comparatively speaking. And our budget is comparatively small as well. And we're constantly battling to try to raise that.

And that's one of the jobs of the chief ethics officer, is whether or not the chief ethics officer has a seat at the table with management, senior management and can get the budget it needs. You know, my company it's a little more difficult, I think, than in most because it's a foreign enterprise.

And for example, the internal audit department is not permitted by law to report to the audit committee. So foreign enterprises have unique problems, but even U.S. domestic companies with foreign subsidiaries will have similar problems.

(Alex Brigham): So if you pull the report from ACC on the overall survey, you'll see that there is a disparity even in – and some of it, as you alluded to (Neil) it also effects whether it's a U.S. based, you know, global headquarter company or one that's overseas. There's a different approach towards the compliance and ethics function.

Moving on to the next slide, so what are they spending? Well here's just two data points, I couldn't put too many on the slide right here, but, when you look at between five and 10,000 employees and 10 to 25,000 employee companies which is a large, large segment of the U.S. based business economy, that is focused on these compliance and ethics activities, and compromises publicly traded company which naturally have a greater interest in it, you can see that the disparity is broad. I mean there's also three to four percent within the company that has – within an industry even, and obviously it's more heavily skewed on certain industries that have high compliance spend. But there is a substantial amount of substantial amount of companies, even under 10,000 employees, you know, five to 10,000, and I know this is a little bit of an eye chart, but this pie chart on the left, that' biggest black slide says they're spending less than $50,000 and between 10 and 24 – $25,000 employees, there still is a substantial portion that spends $150,000. There is a lot of upward pressure certainly, and these budgets will grow, but historically this is a brand new function.

Now, you need – why are statistics like this interesting? Well they're interesting to find a snapshot of where your organization may be versus peers. And, you know, we do help companies run this on an industry specific basis, you know, actually benchmark specifically against others in their industry and then similar size. But remember one of those elements under federal sentencing guidelines and the overall interpretation is your level of commitment to the program. And this is, you know, one of those few actual metrics that can be shown to a government prosecutor who says, you know, show me that you're actually committed to this whole thing, that you actually made an effort to prevent it. And unless you have some very novel way of doing compliance and ethics, showing something that well, you know, we really spent like $20,000 last year, when you have a $5 million insurance bill and, you know, lots of expenses elsewhere it's hard to defend so it's kind of an awkward position for companies to be in. So it's a good idea to keep an eye on what other companies are doing.

(Neil Belloff): To keep it in perspective, look at your 404 budgets, your SOX 404 budgets. I know that General Electric has publicly stated it spends $33 million in each of year one and year two of SOX 404 implementation. I can tell you that Deutsche Telecom spent far in excess of that, but that our risk assessment program, which is in my view more important, because 404 is part of that program, our budget is much, much less than that.

(Alex Brigham): Now on this next slide, current state risk assessment, we have a couple of hundred people listening in on this call and why, you know, why are they interested? This is who's doing it. Over three out of our four companies that are publicly traded will say yes, we do conduct a period risk assessment. They're not necessarily required to, but clearly the emphasis has been there, whereas private companies are far less likely to conduct a risk assessment, one out of every two.

If you were to dig deeper in these statistics in asking people well were you happy how it was conducted? They probably would say well it's so painful I'm never going to do it that way, again.

So yes, while we did it, we're going to try to improve upon it and do it better. Because if it's done wrong, as I mentioned, you can raise exposure, it can be one of the riskiest things that a company can do is to do a poorly designed risk assessment, but also it can be disruptive. And, you know, from a political career standpoint, you know, you need to consider the messaging that you're doing when you're going out to the work force, and making sure people understand that this is separate from that 404 work that's just recently been completed.

(Neil Belloff): If you also look under Delaware law, for those of you who are Delaware companies, there's a (Care Mark) case which says that directors have an affirmative duty to determine whether they have compliance programs, and whether they're effective. So it's not just a public Sarbanes-Oxley SEC issue, it's really, it's a state law issue as well.

(Alex Brigham): And then looking at the current state of risk assessment how are they going – how are you categorizing risk. And again, big difference between publicly traded companies, I've done it and the private that are doing, which is as I mentioned, private companies are less likely to do it, but this is among those companies that actually do conduct a risk assessment.

Four out of five are saying we're going to prioritize by the likelihood and the impact of any violation. And we are strong believers that that's the right way to do, I mean whether it results in what some people call is a heat map quadrant or some kind of measurement or quantification of the risk, you do need to know the likelihood and impact, or some people use severity instead of impact. But private companies are certainly less likely to do that.

I think, you know, there's very few standards and risk assessment, but I think this is one of those standards that will emerge is the likelihood and severity will become sort of standard protocol, and we're seeing it well on the way in that direction.

(Neil), do you want to talk about – can you talk about the proactive approach? I think this has been a good way, you know, looking at it on an integrated basis.

(Neil Belloff): Sure. It's really, you know, from my perspective, the risk assessment is part of the overall corporate compliance program. Every company as (Alex) mentioned under the federal sentencing guidelines and case law and things of that nature, should have a corporate compliance program, should have an effective corporate compliance program and risk assessment is an integral part of that.

I call it a proactive approach and use the acronym proactive as follows, you can see that up on your screen. One is to promote best practices. Look at what your peers are doing. Looking at what the standard setters are saying. But, you know, just because your – you know, the industry or your peers are doing it one way, doesn't necessarily mean that it's right or right for your company. So you really have to kind of look at your own circumstances.

You must review your existing compliance programs. I know in our experience, being a company so large, it's very, very difficult for us to know what's going on at all subsidiaries throughout the company, what's happening with our subsidiaries in Singapore and other places around the world. So for us to get a handle on our compliance programs, and to do an effective risk assessment, we really – you know that's a challenge in and of itself.

We must oversea our compliance initiatives and the program implementation of those to determine whether or not they're effective, or that there's risk involved here. That usually is a lot of coordination on a lot of people and a lot of departments.

A company should actively support and assist in setting the property tone. This has got to come from top management, there's no ifs ands or buts about it. If your management has not bought

into this concept of compliance and risk management and assessment you can end up beating your head against the wall. So it's very important that top management really believe in this.

And as was mentioned, I don't know if anybody on the call listen to the SEC roundtable Webcast yesterday, I did, and there was some excellent anecdotal evidence as opposed to empirical evidence that came out that indicated, you know, good corporate governance, good internal controls, good risk assessment programs and management will yield better business results and performance. There's a lot of anecdotal evidence out there. There's some empirical evidence, but, you know, it's just tough to quantify. So a company should conduct risk assessments on a periodic basis and report the results to management. This is just a critical process.

Also employees must be trained, and you always start with management. We always start with the board of directors, the audit committee, the senior management. And training goes well beyond what you might contemplate; it's not just sexual harassment training. It goes through all sorts of laws and regulations improvement and ethics and culture and professionalism. And what we're talking about here is a corporate cultural revolution, and in my view it's a good thing.

Where there are violations of laws and policies, you must have an effective enforcement policy. You must investigate these problems. You must determine, you know, why this happened, if there's a breakdown in the control structure, maybe your risk assessment program is not the right program and needs to be modified, you must make those modifications. If you look at the sentencing guidelines, that's a critical element of the sentencing guidelines as well.

And you must be able to verify the effectiveness of your compliance programs, particularly if you're – you know, you want to stay within the federal sentencing guidelines, and that requires documentation. Anyone who is involved in SOX 404, knows about documentation and the importance of that. And, you know, the goal is to ensure that risks are minimized, and take appropriate remedial measures. You must follow up on these things. You must use appropriate

IP tools and automate things as much as possible. And that's what I call the proactive approach to integrating risk management into your corporate compliance program.

(Alex Brigham): So there's federal sentencing guidelines. If I was tracking (Neil) and (Neil's) words and mind, we probably mentioned it eight times all ready. So that is here on the screen. FSGO in section 8.21. That is one of the reasons to conduct a risk assessment but it's not really the only reason. So this is my why conduct it or also why – also how to go into risk assessment with wide open eyes. And I'll tell you an anecdote of a company that wasn't able to do that in terms of the some of the repercussions.

Why assess risk? Well certainly federal sentencing guidelines. And then you have prevention mitigation. I mean it's intended to prevent or mitigate potential risk from occurring. The needs GAAP analysis is going to show where – a good risk assessment will show exactly where you need to put your emphasis. I mean you cannot – I think being a compliance and ethics officer or responsible for that function inside a company is one of the most difficult jobs humanely possible inside a company. It's a cost center often times, you know, and cost centers always called into question. It's very hard to measure the return on investment of what you're doing. And inevitably people do push back, push back against, oh gee, we have to train in this, or push back another policy comes down. Now they've taken the gift and gratuities policy and hammered it, so, you know, I can't even entertain clients any more. They blame that all on the compliance department.

So a good risk assessment is actually a documentation, it helps you support what you're doing to the executive team. But it prioritizes it, so that you really do focus on what's important from preventing risk, recognizing that you can't prevent every single problem from happening. And, you know, that's one of the complaints that people had had about SOX 404 is it made you look at all controls. And, you know, materiality and focusing on a risk based approach historically was not there. Now they did do updated guidance in May 2005 on being able to use a risk based prioritization approach towards 404. But, you know, that's one of the challenges for a compliance

and ethics officer. So if you have good documentation it's going to justify and help you prioritize. It can also prioritize your budget. A good risk assessment also will address (Koso), internal controls environment self assessment elements. And naturally be an affirmative defense before organization and oversight personnel. So there's a lot of good reasons why to assess risk. And (Neil) did you have something that you wanted to add on that on the SEC guidance?

(Neil Belloff): Well just that there's going to be more SEC guidance. The SEC roundtable yesterday was very informative and there will be more guidance on SOX 404 issues and Sarbanes-Oxley in general coming down the pike. So we won't just be looking at the May '05 guidance.

(Alex Brigham): Right. Now – so that's all of the good reasons to assess risk, now how about why to not assess risk, and as we saw those statistics, not every company does. We've talked to a fair amount of the ones that don't and, you know, about whether it's a conscious decision or whether they just haven't gotten around to it, because you aren't necessarily legally required, but you certainly aren't meeting the measurements of what an effective compliance and ethics program is defined to be.

Well first off, results must be acted on. There's nothing worse than finding gee, there's some enormous risks here, and then not being able to get the budget, or the political will internally to actually take action items on preventing those risks. If you don't, obviously, you're creating even more liability for the organization and even yourself personally. That's one of those elements that we've talked about in the past.

Second poor execution on risk assessment is not defensible. So if you do an absolutely terrible risk assessment it's highly subjective, that's really not going to help you when it's pretty obvious, and that's what we call the elephants in the room, hence why we show them at the outset. There are certain companies and certain industries which know they have massive risks, they just don't want to tackle them head on. And they'll pick and pack and look at everything around those risks,

but there will be that elephant in the room, they're like well that's potentially risky but, you know, it's a big profit center for us or those employees are a big source of our revenues, or that region. So we really don't want to hit it on, and we turn a blind eye towards it. That's pretty dangerous.

Third, leadership may not be supportive. They may say, why are you doing this? Why are you – didn't we do this under Sarbanes-Oxley all ready? And, you know, that's a risk ((inaudible)) that's one of the first priorities you need to get on board.

Fourth, documentation, and this is one of my little anecdotes, but the documentation is the number one issue in a risk assessment in our book if you're doing it right, who's going to have those documents? Are they under attorney client privilege, and even if they are, how are you going to protect? What are you going to keep? And what are you going to do destroy? And how you go about collecting that documentation is critical because we ran across a situation where a company had come to us, and they said, you know, what we went through a presentation at a conference, and this company talked about doing a bottoms up risk assessment where they sent out this questionnaire, 10 to 12 questions, to a big portion of their work force going deep into the field and asking the employees such questions, as well what do you think could go wrong? What almost went wrong? What could go wrong in other departments? And they got a lot of hyperbole responses and hundreds of areas of things that could go wrong, and the compliance officer was not prepared to receive those. And all of a sudden this poor officer said I have hundreds of these e-mails now, I can't believe I had gone about and done it this way. I wish I hadn't gone to that presentation at that conference, can I delete these?

And of course you can't just flat out delete those type of things, because in – even if you were deleting it, how do you that you really deleted all of this work product that might not be in the field as well. You know, when there's an investigation, you know, one only needs to look at the AIG situation with Spitzer. Spitzer is a master at discovery documentation, in part because he has almost endless resources. Why? Because his office is very close to NYU law school and he has

tons of students as interns. And they'll dig through all of that discovered information until they find something that may be relevant, and that smoking gun or that e-mail which was not intended to be a smoking gun could become a problem.

Now this company, unfortunately, later then had some major compliance failures. And in some of these areas that people were talking about and they hadn't been prevented. And so as this plays out over time, it's going to – whatever the cost of the compliance failure will be to them now, it probably will be five times as much because they have a highly undermined jury, you know, presentation if they were to take it to court, so they're looking to settle it.

And then, the last two, certainly cost of doing so and disruption. So what we counsel people is have your elevator pitch. You have to have an elevator pitch, because you're going to have to defend it. You have to explain to people who have been involved in the Sarbanes-Oxley process 404 why this is different, why this is focused on compliance and ethics specifically. And this not the same as looking at financial balance sheet risk or enterprise risk of currency change. And this is focused on the likelihood of employees breaking the law, you know, have major compliance failures inside your organization. And, you know, you're going to have to have that same short elevator pitch tested out for the leadership team to convince them why to do this.

There is that one question before we move to the next slide I just anted to address it that was written in which says for private companies, because one of the big issues is what does periodic mean? So for private companies, what is the reasonable frequency of updating your risk assessment? Is a biannual update reasonable?

Well public companies certainly focus on – it ties into more of annual almost auditing type cycle. And – but for a private company, doing it every two years, while there's no definition out there, we've seen that to be an acceptable practice, with one (provisio) exception and that is if there's been a material change in your business. Have you gone into a whole new market? Have you

made a major acquisition or merger? Well the no, you need an updated risk assessment. Otherwise, generally if it's same business status quo and no major changes in the industry either by any laws is acceptable.

(Neil Belloff): Also risk assessments can be targeted. For example, if there's been no turnover in your antitrust group and you want to know, and the laws haven't changed all that much I mean and you did an assessment last year, do you have to do another one this year? Probably not. So it really depends on what, you know, what are the high areas of risk, versus the low areas of risk? It's, you know, similar to this SOX 404 risk based approach to SOX 404. You have to test everything every year, year-after-year, when there's been no change or modification, the answer is probably not. So what is reasonable really depends on what it is that you're testing.

I'll give you just one other anecdotal story, but I'll withhold the name of the company. It's a foreign company. And there was some remote sales organization that, you know, kept bidding against it's three or four known competitors in each market. And finally, these guys got tired of bidding against each other. And they said look, why don't we just all have the same pricing structure. And this way, whoever gets it, gets it, and we're all in the same boat. And they thought it was a good business idea. What they didn't understand is that's a violation of antitrust laws, even overseas.

And the European Union, for example, they have the authority to show up at the CEO's office with what is, I guess, the equivalent of a federal marshal over there. And this particular CEO of a major corporation, the European Union and the local authority showed up and took his computer right off this desk to see whether or not he was in collusion with these four other enterprises to fix prices in some remote market somewhere in the European Union.

Well, you know, that's a problem. And a good risk assessment would have detected that, you know, you need better training of the sales organization staff and antitrust and export controls and things of that nature. So it is a small relatively minor thing but it had huge consequences.

So that leads to the next slide, which really is why we do this, risk assessments. We do that – and this is similar to most governance initiatives. And, you know, what prompted the Sarbanes-Oxley legislation, and there's similar legislation pending in the European Union and in Japan and other parts of the world. Everybody is kind of moving to this good corporate governance.

The – you know, augmenting operational performance, that right now, there's very little like I said empirical evidence, but there's some good anecdotal evidence that, you know, when you change your corporate culture into one of high ethics, and compliance is valued throughout the organization, you get better production from your employees. It's anecdotal but every CEO, every CFO I've spoken to about it really believes it, that it will translate into better operating performance.

Good risk assessment and compliance programs will improve investor confidence, which is one of the reasons for the Sarbanes-Oxley legislation. Strengthening corporate governance and accountability, employing best practices is critically important and will be a direct result of a good program, enhancing the effectiveness of your control structures, whether that's internal controls, disclosure controls and procedures export controls, you know, whatever processes and procedures you have in place. A good risk assessment program and compliance program will enhance that.

And, you know, one of the goals is to ensure compliance with laws in all jurisdictions. And again, the ultimate goal is to minimize potential risks to the company. So these are the things that we have to keep in mind. These are the things that management really has to buy into in order to make a compliance program and they do a risk assessment program effectively.

So that leads to the next slide, which is OK, who's going to do all of this stuff? You know, there are so many aspects of compliance, and risk assessment program, I guess there's export controls, there's human resources issues, there's, you know, there are so many plus all of the training and stuff like that, it's really a coordinated effort.

And if we turn to the next slide, I'll just give you a brief – (Alex), can you turn the next? Thanks. Just a brief organizational structure at Deutsche Telecom, and it is a foreign enterprise, so that's why you don't have a direct reporting line to the board and the audit committee, because in the German corporation it's a two tiered management system, where you have a supervisory board and a management board. The management board is very much akin to our executive officers here in the states. And the supervisory board is very much akin to the board of directors, except, whereas in the United States, the board of directors is really ultimately responsible for everything that happens in the company. In a German and Austrian corporation that is not the case. The supervisor board is not permitted to be involved in the day to day operations of the company, that is strictly the domain on the management board, which is your CEO, your CFO, and heads of the major divisions.

So that is why the internal audit department cannot report directly to the board of the audit committee, because that would be getting the audit committee and the board getting involved in day to day affairs in running the company which is illegal in those countries, and there are exceptions to the Sarbanes-Oxley legislation and the New York Stock Exchange rules, to which we are subject, specifically for this circumstance.

But if you look at the organizational structure, it is way more complicated than this. I did not even include the operating units, which you see at the lower left of your screen, in the purplish pink. There's, you know, our organization chart is just gigantic. But the point of this organizational structure is that underneath our CEO we have many departments, but I picked a few important

ones, which are IT, internal audit, our strategy department, external communication department. That's really under our CEO's guidance.

Under our CFO's guidance, there's a – your corporate control which is our chief compliance officer, investor relations, our general counsel and the legal department is under the CFO's direction and of course, the accounting group. Underneath the chief compliance officers guidance would be risk management, which does a lot of our risk assessment. We have a separate SOX 404 project.

Human resources is run as a separate unit. It is not under the CEO or the CFO. It's kind of a separate organization, anyone who knows the labor laws overseas will understand why that is. And underneath the human resources director's tutelage is security and (forward) management program. So you have the items in red are really those folks who need to be involved in risk assessment. And they're under the direction of different people in different units.

The thing that brings them all together is public reporting. And that's public reporting if you're an (NCC) company, or if you have some investigation ongoing. I mean this is where all of these people are related. That's why all of the dotted lines go to the public reporting aspect of the company. So in our company, for example, having these units under the direction of different people is quite a challenge for us.

If you turn to the next slide, we'll try to make it a little bit more comprehensible for you. So I mean, these are the main risk process organizations, your chief compliance officer, and his department which includes the SOX 404 folks, it includes the risk management folks. Their accounting function is done by a different set of people. Your security forward management IT related is also – that's under the CEO.

Internal audit should remain independent to the extent that's possible. But all of these processes, and the CCO generates a report, SOX 404 project generates a report, the risk management folks generate a report, the accounting department generates reports, security forward management generates reports. These are all separate IT systems. They are separate reporting change. And, you know, it's your guy out there on the front line. That means you're getting five questionnaires and that doesn't even include what internal is going to do and it doesn't include what our external auditors are going to do.

So front line troops are getting bombarded all of the time with questionnaires and surveys and interviews, and all sorts of ways that these reports are generated. And the challenge for us it so coordinate all of these systems into one or two systems if we can get it down to that. This will all have a positive impact. If we can converge all of these automated processes, it will bring down the costs. It will ensure efficiency. It will ensure an effective risk assessment and compliance program. So that's kind of our goal. And it will lead to better public reporting. As (Alex) said, it will lead to making a better case if we ever trip up the federal sentencing guidelines and we have to defend ourselves there. But to have five central processes running with the left hand not knowing what the right hand is doing, and in my mind that's a risk in and of itself. So I raise this anecdotal organizational structural issue to show you how complicated this can get, especially in larger organizations.

(Alex Brigham): Well (Neil) I think you just – you made the case with the those organizational structure and the systems for what the supporting documentations might be so that being in the compliance our ethics officer position in any company is one of the most difficult positions around.

(Neil Belloff): It is. And like I said, the chief compliance or ethics officer has to have a seat at the top level of management, whether that's, you know, with the audit committee, or in our case with our management board or both. And there's got to be a commitment from top management and the board, that this is an important function. Yes, there's a lot of cost involved, but cost can be

streamlined. We can make this process more efficient. And – but it's got to come from the top down.

(Alex Brigham): Right. Well I mean you've given us a good little anecdote. I mean it's one thing to go to the board and say and – or to the CEO and say look, you know, here's the federal sentencing guidelines, here are these eight steps, chapter this, chapter that. Or say, hey, you know, there's this fellow, this CEO of this other company and these people walked into his office, picked the computer off his desk and left. I think you'll get his attention.

(Neil Belloff): Well they actually wanted to arrest him even more so.

(Alex Brigham): All right, 10 steps to conducting a risk assessment. Because there is no, you know, because the government and regulatory bodies have been vague about it, there is a lot of flexibility in how you want to define it, but here are some of the best practices that we've identified. And this is in a ACC (Corpedia) info pack, this documentation.

Under full disclosure I have to say that we do, do risk assessments on behalf of companies, and we do work in partnership, so just be aware of that. But this is – you do not have to work with an outsider, you can work entirely an insider, a lot of these same processes will be exactly the same, whether you're working with outside counsel, us, or doing it entirely in house.

Now, there's another question that did come in, which was do we have to do a risk assessment this year? And, you know, I did neglect to mention at the outset, we do love getting these questions, and you can submit a question down on the lower right hand corner of the Web screen then click send, so type it in there and hit send and we'll address it as we go through this presentation, but there's a person who said do we have to do a risk assessment this year? Or when do we have to do a risk assessment? Is a plan to do it sufficient?

And it's what I – well a plan to do it, as long it's not too far in the future is essentially efficient because we do want people to really plan this whole process out. It's what we call punting. How far can you punt it? You can probably punt it until late 2006, or some time in early 2007, but you'd want to do something. Now don't be so daunted that you cannot – you don't have to do soup to nuts and turnover every single rock. There are – you can do versioning of doing something light and getting started and see how it works. And particularly if you're doing it by yourself internally, that's what we'd recommend, but it is good to get started. And frankly, there's other reasons to get started too, partly depending on if this is your primary job function inside an organization, this is part of your critical job definition.

And if you don't take some form of leadership on it, there is a risk, and we've seen this in other organizations that it will entirely run by internal audit and you won't be able to do your job, because they will have said, we've taken this over. Oh no, we've looked at those risks. And it can be frustrating for you, because you know that they haven't necessarily looked at the risk, the risk that employees know what they're doing in not breaking the law in certain countries as (Neil) had alluded to. You know, the risk is some of these policies aren't actually being followed, you know, because it's not their historical strength of an internal audit function to be looking at legal elements. This is an opportunity for the compliance and ethics office to really step up to the plate and get a much broader exposure inside an organization.

So with that, I'll mention on punting, and how far you can punt it, the 10 steps, defining objectives, criteria and documentation and that is what are we going to keep? And what are going to go about creating it? How are we going to do that? You know, stuff that ends up on networks these days, ends up living forever. And we've seen companies go to the point of where they're taking interviews. And no one wants to take all of their notes – hand written notes, I mean that's almost a throw back for a lot of people. But if you do it electronically, if you're networked, you may have an archived copy before you even know it. We've seen companies actually do it on a laptop that is not on the network and then take that laptop and plug it directly into a printer that is not on the

network, print out one copy or two copies, of the notes from the work product that came out of it and then just erase the files. I mean there's just that sense of about it, because you don't want this floating around because what you don't know that's out there, as mentioned can come back and hurt you. So a lot of definition of objectives criteria and documentation up front

And, you know, hand in hand, planning the process. What are the tactics? How far we going to go? Are we, you know, going to be doing interviews of employees and if so, how far down into the organization? Are we going to use electronic means at all? Or will it be in person? And, you know, that's a planning. And the plan has to be somewhat flexible, because obviously if you find a risk that you need to go deeper on, then you need to go deeper on it, and the plan can expand.

Third, profiling the organization. You know, what are the business drivers? What geographic markets?

And then, four you're going to get a cataloging of the risk universe and what could go wrong. And you want to get a lot of input on that. And that's a pretty good area to get outsiders to weigh in on it because there are some catalog risk universes out there. You know, we talk as other people do and say, there's, you know, hundreds of potential risks for any company, well of course, there are hundreds of risks, but the key is you've got to (winnow) that down. You shouldn't be doing and chasing hundreds of risks, that's just time inefficient and somewhat clueless. You know, the whole thing is to take that risk universe of hundreds of potential risks that could go wrong and get it down to something manageable that you're actually going to examine. And that's where people can bring input. And then you still haven't gone out to the field and really done the risk assessment. You're still getting input from the co centric circles in the leadership about what you're going to be looking at. And you might get it down to 25 to 35 core risk areas that you really want to focus in on and address.

And importantly, we would recommend that you do get other people to sign off on what you're going to be looking at. You want other people to input and say this is what we're going to be looking at. Do you agree that these are the 25 most risk areas? And they can add on to it, or they can delete it, but that's also, you know, protection for you. You want to be able to say hey, you know what, these other four people inside our leadership weighed in, and as a committee we decided these are what we're going to look at as opposed to just me personally.

You know rating risk areas for severity, what is the impact? Again, outside expert counsel.

(Neil Belloff): (Alex), can I jump in for a minute.

(Alex Brigham): Yes, absolutely.

(Neil Belloff): There are a couple of questions that I think relate to that. I alluded to it earlier, one of the questions that somebody wrote in is what about compliance programs an policies that are all ready in place and do you have to go back? How do you do a risk assessment with programs in place, et cetera? Because you don't want the employees to respond, but they are all ready ((inaudible)).

That's one of the, as I mentioned earlier, one of the challenges for Deutsche Telecom. You know, we're 400 subsidiaries and all of those people and so many countries, and to try to get a handle on exactly what we have because it's not centralized, it's done on the local level. And that's something that we're doing right now. We've created an IT tool, actually, and we're in the process of gathering all of that information to route our vast organization to find out exactly what program we do have in place.

Then we have to actually take a look at those programs and do some sort of, you know, back of the napkin kind of assessment as to whether or not we think that's a right program for these

particular group of people, and it's an effective program. And if it's not, we have to recommend changes to the program. And it's difficult to do that on the central level. I mean we can have a general oversight view, you know, the 30,000 view. But if we look at it real closely and we say, you know, your export control program in Albania is really not that effective, our response would be you guys got to go fix it, and you've got to implement a new one that's more effective and that works and then we'll reassess it. And we'll get internal audit there, or a risk management folks in there and we'll reassess that program.

You know, we'll certainly lend assistance where we can, but there are certain local laws that even I'm not that familiar with and my input wouldn't be all that significant.

So, you know, it's critically important to get a handle on what you have in place particularly if you're a large organization and you're not centralized. And then, to systematically catalog that as (Alex) just alluded to, and then determine what your risk universe is. You know, where do you think that there are gaps? And where do you think there are programs and policies that are not as effective? And that's the first challenge, and then, you know, because I agree. You just don't want to inundate your employees with all of these questionnaires when they might have a very good program and it works quite well.

(Alex Brigham): Well one question (Neil), that came in too was about legal areas would we suggest probably trade ((inaudible)) for risk assessment purposes? I mean there's really not a material difference, you know, obviously financial controls are more important in representations in terms of potential liability to stockholders are more important in public companies as opposed to private, and therefore maybe the protection of confidential information. But outside just a few areas, it's very universal, and it obviously depends on what industry you're in and what markets you operate in. But there's – you have to keep an eye on the overall exposure level for your organization.

For example, I mean always at the top of the list if competitive practices these days. Competitive practices, you know, violations of law can result in two major elements, certainly huge criminal and civil penalties, but also can actually have a lasting damage operationally on your business. And we don't have time to go into the details exactly how that happens. But we have great case studies about when you take the eye off the ball and you are competitively profitable based upon illegal practices. And once that quote unquote competitive advantage disappears, you've actually not really invested in your business. And we've seen cases where companies have gone – you know, collective companies and their cartels have gone from upside down on their market share, from having 80 percent market share in certain industries to dropping to under 10 percent in a period of five years because of some anti competitive practices that they were caught on.

But also, you know, product liability, if that's in your industry, that's a big elements. Export controls as you just alluded to. And international, it's very different internationally. There's been just two quick examples, actually, (Neil), you had alluded to our newsletter, which you can get – sign up for free at our Web site at (Corpedia). But I mean there's two new interpretations, if you're a government contract, they just broadened the definition under case law of whistle blowers, and who could sue a government contractor who gets grants from the government. A dramatically different and broader definition which dramatically raises the exposure in that area, where you're going to have whole practices of attorneys just pop up as whistle blowers, because they can now do so under the Freedom of Information Act, to gather information.

Now, in Europe, when you're looking at competitive practices, they've changed the legal liability of dramatically expanded it where any consumer can sue over losses, and more easily sue over losses for, you know, price fixing activities that have occurred. And that's scaring the heck out of companies.

You can – you know, in a third article from that newsletter, if you look at what's going on in Florida, a company spent $5,000 for a DMV drivers license database that they wanted to market

to, and they marketed to it, and they got sued because they had violated privacy laws the weren't fully aware of. And the Supreme Court, the U.S. Supreme Court for now has decided not weigh in on it, they're just gong to follow it. But the potential penalties in this case are $1.4 billion for that $5,000 acquisition of information and how it was used.

So it's going to vary but if you get some good counsel you can do it.

(Neil Belloff): Yes. There's a – you know, I can just give you an off the top of the head list, I mean you have your code of ethics, and your code of conduct, workplace discrimination, harassment, antitrust, conflicts of interest, document management and retention, confidentiality, customer privacy, product liability, trade secrets, intellectual property, money laundering, the U.S. Patriot Act, export controls, (Foreign Core Practices Act), Sarbanes-Oxley Act, insider trading restrictions, environmental health, financial integrity, whistle blower, labor issues, government contracts, and the list goes on and on and on. But as (Alex) said, you have to determine where the risk lies.

(Alex Brigham): Yes, and I can't write as fast as you just talked (Neil), but on the last slide, we – our contact information is available, so you can contact either one of us for more information because we do have a lot on it. Now there are no risks – you know, we talked about just on the previous slide, you know, we're going through the final steps, the risk event probably, likelihood determining aggregate risk or finalizing risk assessment reporting and create a mitigation action plan. You know, you have to allow for common carrying and versioning on the final report.

But the final report is what you're going to want to have on the shelf. The final report is going to be what you want to show in a proceeding and to defend what your activity is and what you've done. But you're going to have to come up or use an external party, to talk about what the tracking or measuring standards, how are you going to know what's a high likelihood, high impact type event. How are you going to know that the actions that you're taking are actually reducing

risk or mitigating risk in the absence of just the fact that nothing happens, which is, you know, you want that happen but that's such a (bully) and extreme, it either happens or it doesn't. You know, a major blow up is not entirely a way of tracking risk.

Feel free because, you know, we're going to be tight on this call to contact us and we can talk more. And we do discuss that in our info pack.

Now here's some – just a deeper dive on the methodologies of doing the risk assessment. At a minimum, as you can see here, almost four out of five companies, they're doing interviews. You can't just sit around in a room, there's four of view, and say hey, what do you think the risks are, let's write them down and we've done a risk assessment and move forward. You actually do need to get input from functional leadership. And as you see we're looking at internal document reviews, litigation and audit reports, hotline reports, looking for trends. That, and obviously interviewing key functional areas, talking to the heads of marketing, talking to the heads of customer service. They're going to be at the front end and they will know good stuff. But how you ask the questions is important. This is not an investigation, this is a collaborate element, you're asking for their input. If it comes across as an internal investigation, they'll shut down. That's an important element.

And one thing, you know, an interviewing technique that we found works very well is to talk about well not only our own department, but talk about other departments. So when you're talking about the marketing department, you say well what could do wrong in the sales department do you think that could cause some major problems for our organization based on what you know in the marketing? And people like to talk about other people's departments first and actually open up. It's a great interviewing technique. And, you know, again, a lot of these interviews are done in person.

Now what are the areas that they're examining? Again, this comes out of this database. And why we put those green arrows there, because actually those are tying back to some of the major elements of federal sentencing guideline definition. And what's interesting is the internal policies, processes, employee understanding, you know, it's reporting system and tone from the top, are all of the things that companies are trying to examine as part of their risk assessment but at the low end they're not looking at age and compliance that much. They're not looking at the incentive plans, less than 40 percent of the time, or the capabilities of the employees for the jobs that they have in times of substantial authority. I would argue that a lot of these should be, you know, built into the risk assessment. Certainly, you know, some of the ones at the lower end of the scale, there are ways to build that into your risk assessment, and how you're going to analyze that.

If I skip to the next slide here, what are the outcomes? Well how is the data to used derived from risk assessment? According to our surveys it's at the high end, it certainly effects internal processes and controls not surprisingly, policies over 80 percent of the time. But, you know, as (Neil) had alluded to, it is used as the basis for driving employee training program, very, very often. And it's an extremely wise application of the risk assessment because employee training programs are effective, but they're also very high profile and you want them to be efficient. And this is that basis that they're using it to drive it.

Now at the low end, if you look at the very top, you know, less than 25 percent of the time is it really being used to drive the compliance budget, to help you determine the budget or the staffing. Why is that? Well I mean part of it is, think about, if you use the risk assessment, you did it and you said we have all of these problems and we need a bigger budget, because that's what compliance budget justification is, if you don't get it, and they say no, well that looks bad right now. I mean you've asked that we need all of this budget to be able to do it, and you get shut down, you've done your analysis. Now it's going to be sitting on the shelf saying we're under budget and understaffed in compliance. And almost anything that you do, no matter what you do if something goes wrong now, that is going to be a smoking gun that's going to come back and

say look you guys knew that you were understaffed, you knew that you weren't doing it. So we strongly counsel against that. The compliance budgets should be ((inaudible)) expectations should be set up front …

(Neil Belloff): It also depends on what the risk is that you find. I mean for example, if you don't have a SOX 404 program, well, you know, or a disclosure controls and procedures program, your CEO and CFO cannot certify under section 302 and 906 of the Sarbanes-Oxley Act in your public reports, and that's a serious problem.

(Alex Brigham): Yes. So when the training- when they do train, they typically focus on code. And when code training is mandatory because this is, you know, part of our survey that we've done, it's interesting is they really do meet that federal sentencing guidelines element of you must train at all levels from the board down. And when there is a mandatory training program for code, over 70 percent of the companies are hitting over 90 percent of their work force, some very impressive statistics. And as you can see, 80 percent or 90 percent are hitting at least half. And naturally, it's going to factor by industry, but there's a lot of creative ways to get there, and e-learning is certainly a very well accepted way of helping to achieve that.

When you have that final report, who gets it? Well certainly, you know, executive team two thirds of the time. But what I think is particularly interesting is how infrequently it's given to outside auditors, very infrequent. It can still be used, I mean excerpts from it, but they don't just say hey here you go, here's the work product, here's the final risk assessment to your outside auditors, but, you know, if it's used sadly, if it's a well put together report. We've been able to work with clients, for example, to actually reduce their transaction costs on 404 work, by saying this is what our risk assessment shows where we want to focus first, and be – go deeper.

That being said, there's still a disconnect between the risk analysis, risk assessment and the training. Now coming back to – someone had asked what should be looking at as a public

company? We have very good statistics and some of those are published in an ACC survey that we did last year, about what's keeping compliance and ethics officers up at night. What do the feel the likelihood of something that could occur and the severity of it? And the four biggest areas, financial assurance naturally, lots of confidential information, document retention practices, and antitrust competitive practices are the four areas that they're most concerned about. However, the training inside our organizations you can see those barely, you know, resonate at the top. It's all about employment law, that's a high profile area that get a lot of attention, but antitrust is down at 43 percent document retention, you know, one in three companies have a mandatory training program. And that's even just for a portion of the workforce, it is not throughout the whole organization. So there's a disconnect but we see it closing over time.

(Neil Belloff): It's also a function of whether or not you're a global enterprise or not. I mean I can tell you that our U.S. subsidiaries do annual sexual harassment and discrimination training, but overseas they do not because they're not – the laws are not that strict. And it's not as much of a litigious society in many countries.

(Alex Brigham): Now these – just so you know, these are two of the reference materials that we've been alluded to, info pack from ACC on risk assessment programs, research things that we have and these are available to people who participate on this Webcast, just get in touch with myself or go to our Web site, or go to ACC's Web site and see that.

Now, some parting thoughts on risk assessment. And as you can see, thematically, now the elephant has come out of the elevator and all the way basically into the board room here, hiding in the back, not hiding very discreetly. Now that's the – we talk about this as you will get that question. Somebody pointing at you maybe in that board room saying all right, justify your program, that might be the question that they have. Or tell me, why wasn't this uncovered in the risk assessment? Or tell me what the risk assessment showed? It's that sort of accusatory element of the elephant in the room. So there's some of these things just to hit them head on is

one don't rush into it. That is the worse thing you can do is to say, you know, what, we're going to try and do a big risk assessment in the next six weeks. And just a bug got in my ear, and we've got to do it by the next board meeting. I mean if you have to, you have to, but if you can avoid rushing into it, a better plan process and even going – not going a little bit lighter, not going as deep, you avoid those big elements of potential creating more risk than you're solving in the process.

Second, strive for objectivity, you need objectivity. Objectivity in terms of categorizing the risks, what you include, but also making sure that you really are willing to hit some of these things – you know, ask those tough questions. I mean every organization that we find generally there is a risk or two that they prefer not hit head on, but, you know, what an outsider is going to be aware of that if something goes wrong if they're looking at from a prosecutorial standpoint they're going to know that you avoided it. So you need to be as objective as possible in this. And that's probably the number one reason, often times, aside from expertise, why some compliance and ethic departments do use outsiders.

Document structure is key; I've all ready hit on that. I've just got to reiterate it because it's so important. Open ended questions, number four very important. I mean these are not (bullion) do you see a risk here or not, yes or no. But more what do you think could wrong? How could it go wrong? And it's funny, we've asked the same question three different ways, and sometimes it takes a third way to get a response. You know, in talking to people in charge of employment practice, you have, you know, we've asked do you have major employment practice concerns that could go wrong? And the answer is no we don't have any problems. Are you aware of any major employment practices that competitors have ended up in lawsuits and is that a concern to you? And they go not any problem. And then if you just say much more specific, and say do you think you have FLSA issues? And they go we've got huge issues, we've got huge exposure there. And sometimes, you had to ask it a third time through.

Fifth, know what measures will be. How are you going to measure what these risks are? And again, if you have your measurement and some kind of performance element to it, another thing to consider is federal sentencing guidelines talk about measuring the effectiveness of your program. And measuring the effectiveness of your overall program can be tied into risk assessment. So if you have an objective measurement on why this risk has been reduced, you know, you have fewer smaller incidences, you have fewer calls on the hotline on the subject, et cetera, that is a measurement of effectiveness and that you're being effective at your job personally.

Six, you know, consider the narrow light if need be first, not going as deep. Seven, getting your message, clear, concise and unique from internal audit and what they're doing and that's where we talk about the elevator pitch. And then, finally, be prepared to deal with what you find and steer leadership accordingly in advance. It is just going to be a disaster, if you don't have either the resources and the will. I mean resources is not just about money. It's the will to address some of these risks that would come out of it head on the heals of risk assessment, because if you don't take action on it, it was a wasted cause, and it created more problems than it solved.

(Neil Belloff): If I can, I would just add to that. Like you said, this is not just the check box exercise. This is a change in culture and attitude. It is sweeping the entire corporate world. It's here to stay. Good governance and effective compliance and risk assessment programs will yield better results and make you more productive employees, all of the anecdotal evidence is there.

The problem – the biggest problem, I think, the biggest challenge from companies like mine is getting management to buy off on it, and buy into that it will result in a bottom line increase. And for them, that means an increase in the stock price. If you look at the rating agencies, there are these governance rating agencies now, where they actually rate companies. And there are certain institutional investors like CALPERs, for example, where they will not invest in

corporations that don't have a particular governance rating. So this is becoming of critical importance. It's not just a check the box exercise. This is really a cultural revolution.

(Alex Brigham): One question that came in here towards the end I know we just have a couple of minutes, should you assess your risk initially without considering any compliance measures currently in place? Do you have any suggestions on how do to that realistically?

(Neil Belloff): I think that's the one I responded to earlier with, you know, trying to get a handle on what you have within your organization that currently exists. You know, for large companies that is a challenge, particularly large companies that are not centralized. That's why I put up the schematic data to kind of show, you know, what we're trying to do. We have many systems in place, and we're trying to coordinate those systems. We're trying to reach out to our divisions, to our foreign subsidiaries, find out what they're doing, put it all in a big database to kind of look at the – and then, you know, as time goes on to look at these things periodically and make some judgments together with internal audit, together with our risk management folks. And we have a committee system set up to assess these types of programs. And, you know, we'll bring in expertise if it's a foreign country law or something like that that we have to look at.

To see that it exists. It's being implemented properly. It's effective. The training is effective or not. And if it's not, then it's got to be fixed, and that's a massive undertaking.

(Alex Brigham): Yes, I mean when we've looked at when training is effective, people said well we have the training but you can do random knowledge tests out in the workforce, we have done that by functional area and we find some gaps. But the danger in doing that is alluding back to if you start finding these gaps of knowledge, you know, where people don't understand, for example, international bribery conventions, yet they're doing, you know, they're at the forefront of your business in Far East Asia and in the Middle East, you've got a problem and you have to take remedial action on it, or you really undermine the whole reason for doing it to begin with.

But also as follow on, on that, I mean when you're doing the cataloging, do you consider your compliance processes that you have in place before you catalog the potential risks for your organization? My answer is actually no, you're doing it. But if you're looking at it sequentially, you know, just logically in your final analysis, obviously you're doing the cataloging on a concurrent basis. But when you're actually analyzing it, you have to look objectively on what are the risks for your industry? Because if you fall into the trap and say we all ready have great programs in place that are going to prevent international bribery and we've all ready addressed that, and we haven't had problems for years. You're all ready putting your imputed bias on it before you even get started. And there may have been some major changes out in the marketplace that you need to take into account. For example, we've had other clients come up to us and say, you know, what we hear the SEC and DOJ are looking to make a huge example out of somebody on the Foreign Corrupt Practices Act and somebody with a big brand that everybody is aware of, and we just hope it's not us.

(Neil Belloff): It wasn't us, I'll tell you that.

(Alex Brigham): So they're looking to do something like that. And that whole increased emphasis, it means that the impact, and probably likelihood of it occurring in your organization just like any other organization because the government is looking at it is higher. And if you had had your imputed bias that no it couldn't happen here because we have a training program, you didn't look at in your catalog of looking externally on doing those risks, then you wouldn't be hitting that head on.

So with that, (Neil), I'd like to thank you for participating in this program. I think it was a great program. I do have to ask you (Neil) as we wind up here, why does this guy have a handcuff to the phone?

(Neil Belloff): If you find yourself in that situation and you have one phone call to make I don't think you'll want to be calling me, but if you have any other questions, I'd be happy to answer them. You can send me an e-mail or give me a call, not a problem.

(Alex Brigham): Terrific. Well thank you so much (Neil) and everyone thank you for participating and listening in on these Webcast and getting these great questions and my contact information is here on the phone. And with that we'll wrap up. Please have a wonderful weekend.

(Neil Belloff): Thanks.

END