

---

TORONTO – Contractual Compliance: Audit Strategy  
Wednesday, October 17, 2012 – 15:30 to 16:45  
ICANN - Toronto, Canada

MAGUY SERAD:

We will be starting in three minutes. Good afternoon everybody. Today is Wednesday, October 17, 2012. The time is 3:30, ICANN 45 Toronto. And this is the Contractual Compliance Audit Plan Session. Thank you for those who stayed for the next session, and for those who just joined us is just a couple of minor introductions so you know who some of the key audience members we have with us today. I would like to recognize my team, always I like to recognize them first.

I have with me in Toronto Pam Little. I have Paul Redmond, Jacks Khawaja, Atif Beg, Victor Oppenheimer, Sumi Lee, Leticia Castillo. Did I forget somebody? Also I would like to say a special thanks to one of our Board members who's been an amazing supporter and follower for our team Judith Vazquez. And a special thank you to our VP or IT, not IT of VP Ed Beck. He joined ICANN about a month ago and has been amazingly supportive of our activities. We're happy he's here so we can turn to him now for all of our systems needs and enhancements. He's going to help us carry that load.

And if David Clausen is still here I want to say a special thank you to David. He always saves the day. I don't know where he is. Okay. So with that, our objective, this is our last session for Toronto. We use Wednesday afternoons, we started that tradition in Dakar. We use Wednesday afternoons to have focus sessions for contractual

---

*Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.*

compliance to address either updates or latest discussions or programs we're working towards.

This session is going to be focused on the contractual compliance audit plan, strategy, approach, methodology, timeline, all of it. Jacks Kawahja who is the manager in my department for risk and audit. Jacks joined our team last March, has been amazingly working hard; I've never seen an effort of this nature and scope, hit the ground running in such a short period. This audit strategy is part of our three year plan that I had shared with the community when I first came on board after we did our assessment.

We addressed what are the gaps; where are some of the challenges and the areas of improvement for our organization; focused 2012 on putting that foundation together. A key element of that foundation is the audit plan which you're going to hear about today. If you guys remember and have been following the contractual compliance we are a culture of; the culture of compliance is about the multi stakeholder model and it is a bottom-up approach.

If you've been following our activities since I got here this should be familiar. We had announced in, I think, Costa Rica that we were doing a self-assessment, but when we started that effort we had to table it. Even though we ran a successful pilot with registrars and registries, we realized then that we still need some of the elements to be turned up, some of the processes, procedures and all the staff to be able to really say "okay guys, here is the guideline. You can now do it on an annual basis and we will come and work with you."



---

We realized that we still need to complete some of the activities in the preventive space. And with Jacks joining our team it helped us make this come true. So audits is in the preventive activities and it is to help us really gain insight into the reality of the contractual compliance world as it relates to our contracted parties. We want to establish a baseline and this is what we're starting with.

With that I'm going to turn it over to Jacks. If you don't mind please hold the questions until the end. I promise we will have plenty of time to have that dialogue.

JACKS KHAWAJA:

Thank you, Maguy. Can everybody hear me? So thanks for having me, I appreciate it. I'm the Risk and Audit Manager. This is probably something that's never been done before in ICANNs history. And most of you are probably familiar with the types of audits you see up there – the financial audits, the compliance audits, operational, investigative as well as IS audits. This audit is a bit different. This takes a contract between contracted parties as well as in that contract and looks at both the registrars and registries across the board.

These are the types of audits you're probably familiar with. The audit that we're going to introduce to you today – and it's also been introduced in three outreach sessions that have been conducted in September, so the same information is on our site already. But these are the types of audits that you'll see. The audit that we're going to show you today is strictly contractual compliance. It doesn't get into the financial end of it at all, but it is a compliance audit.

---

So I'll share with you the details. Like Maguy said, if you could hold your questions till the end I'll be more than happy to answer those. Okay. So the overall topics for the discussion – we're going to go over the audit plan, the approach and the process we're going to take, as well as the various phases for this audit and then the audit provisions and the timeline.

So our message here, and as well as what's been stated in Costa Rica and Prague, is that this is a consistent methodology and approach. It's going to be applied over a three year period. I'll get into the details but I want to make sure that I state that up front, so that everyone knows this is going to be a completely documented methodology that anyone can reference to on our audit program site.

Okay so the goal – to be proactive. That's what it comes down to. In the past we may not have been as proactive as we would have liked. I think that we've heard the requests from the community, and hopefully this will answer all those requests. The goal of this program is to identify the deficiencies and assist with remediation where needed; where a contracted party just needs guidance in terms of remediating an issue. We'll be there to assist. This is a collaborative approach. It's a three year program. Our intention is to audit all our contracted parties across the board. No one will be excluded.

In year one, we'll do a random sample of a third of the registries and registrar agreements. Year two, same approach. In year two the third that were audited in year one will not be included in year two, so this is a balanced approach. And in year three we'll audit the remaining one-third. Something else to note, and we'll get into it on the next slide, but



what we're stating there in the terms of the consistent process and methodology, it will apply each year. We will allow for flexibility in terms of thinking. If we get feedback from the community and it was too time consuming or it was something that you just didn't think was accurate, by all means we welcome those comments and we'll tweak it where needed.

But ultimately this is going to be a consistent approach across the board. So the overall audit plan that we're going to roll out will include the registrar and registry agreements. In addition to that we're going to look at IRTP, the Inner Registrar Transfer Policy, the Restored Names Accuracy Policy as well as WHOIS Data Reminder Policy, the WDRP. In 2013 to 2014 we are preparing for the new gTLD registries as you guys can see up there. What we're going to do is roll them into the plan as they become active and begin to collect history.

And that's important to say – collect history. We're not simply going to throw in the new gTLDs as soon as they go online. We have to make sure there's historical evidence there to be able to roll them into the audit plan. And they of course will be randomly selected based on who's rolled on. That's going to be rolled up into the rest of the audit plan which will include the existing registries and registrars.

In addition to that, if there are issues that we identify during year one or year two or year three of the audit where we note that there are registrars and registries that may have issues and they're of a significant nature, we may have audits outside of the three year plan, which will evaluate those existing registrars and registries to ensure that they've



remediated any issues that were discovered during the annual audit process.

So we want to make sure that we are collaborating with the registrar and registry and that we are assisting them where needed, but we also want to make sure that these issues with non-compliance are being cured in a timely fashion. And then finally, the last bullet there, leverage third party services. What we've done is we've evaluated our internal resources and because of the breadth and the depth of this audit, it was necessary to consider a third party for assisting us in performing the activities in order to make this thing successful.

So the overall approach and plan – hopefully all of you can read that, but basically there are six phases. You can't read it? Can you blow it up a little somehow. We'll try to blow it up, just one second.

MAGUY SERAD:

And this deck will be available on the webpage.

JACKS KHAWAJA:

And actually this deck is already published, well not the deck but this actual slide. If you refer to the ICANN website under compliance outreach, this actual flowchart is displayed in the outreach that we gave back in September. But essentially what's going to happen is there are six phases. The very first phase is the planning phase. Of any audit these are the typical phases, I just broke it out in a flow so that it's easier to understand. Maybe it's not easy to see but it's easy to understand.



---

So the planning phase, it requires creating an audit scope and building the audit schedule. It's a timely task, even though it says "Build audit phase – two weeks," sometimes there are changes, sometimes we look at risk and decide "oh you know maybe we should be looking at this then that"; that's always a part of an audit process. But that's the essential planning phase and I'll really drive into each one of these in a little bit.

The second phase is the organizing phase. In that phase that's where we develop the metrics goals and establish the roles. The metrics goals are the reporting – what do we want to see in terms of statistics. The roles – what are we going to assign to assist in this audit process. And then the organizing phase, which is later on in the process, is where we assign the resources, whether internally or outside. And then the pre-audit notification – this is to give the registrars and registries notification as to the plan basically; the scope, the timing, what the impact will be.

And just to note, the pre-audit notification does not mean – it's going to go to everyone, but it doesn't mean that everyone is going to be audited in year one. The sampling is going to be based on the audit phase, which is the next phase after pre-audit notification. So two weeks after the pre-audit notification letter goes out we're going to issue an RFI, which is a "request for notification." It's a typical, standard audit process.

The request for information will go out just to those that were sampled for the audit, for year one's audit plan. That will go out and essentially what we'll do is we'll take the information that we're collecting and we



---

will collate, sort, we'll evaluate the information that we collect against the provisions. And in the event where – and I'll get into this in a little bit more detail, I just wanted to show the high level flow – but in the event where we identify issues after evaluating the documentation we've collected, we'll immediately contact the registrar or the registry and say “hey look we've found this issue. Is there anything that we need from you that would remediate it?”

So this is a collaborative approach. This is not one of those approaches where we start the process and the next thing you know you see your name on the web saying that you've failed an audit; that's not the approach we're taking. And then finally there are two more phases – the reporting phase and the remediation phase. So two weeks after the audit phase closes we'll do the reporting phase.

And what we'll do in the reporting phase is we'll report the results by registrar and registry, the provisions we've evaluated and the issues that were discovered. And then the last phase, and the reason it says “TBD” is because the remediation phase will probably take the most time, where we'll assist the registrars and registries to help correct those issues, because our ultimate goal is to ensure proper compliance with the contracts. That's really what our goal is.

Okay, so I went through the flow just a moment ago, just to break down the first three phases. The planning phase is simply to define the scope, the purpose, the schedule and the reports. Obviously we've already conducted that process. We are ramping up into – we're wrapping up the organizing phase right now where we're assigning resources,



developing metrics and goals. And in November, and you'll see the timeline in a moment, we'll get into the pre-audit notification phase.

And that notification phase will be a fax and an email to you, which will identify basically the scope of the audit, the timeline. When you can expect to see the RFI; when you can expect to see the reports and things of that nature. I think everyone's probably more curious about the audit phase, so the audit phase itself, which includes the request for information, what we'll do is we'll collect all that data into a secure environment.

So essentially what will happen is there's going to be an upload process where you'll have the provision, you'll have the request and you just simply click on the upload option and just simply upload the document into a secure environment. That information is completely, it sits behind a DMZ, it's SSL protected and it requires certain access provisions in order to access that data. The access is only going to be administered by a few people.

So just to ensure that everyone understands, the data will be protected very strictly. Again, the second point up there, sort, collate and store the information against the appropriate provisions. When you upload a document that document will be uploaded against the provision, so we won't have to sort through all of your data to figure out what document goes with what. The questions will be clear, concise and they'll ask for specific documents, and that should help everyone go through the process.

And if issues arise, like I mentioned earlier, we'll ask for validation, we'll reach out. We'll say "hey we have an issue with your liability policy, can



---

you please assist us with this.” We are not going to report anything until we reach out to you first, that’s the key. And then finally, on the last bullet of the audit phase, what we want to do is in the event where the audit is closed, we’ve reached out to the contracted parties and we’ve given them ample time to respond and we’re simply, we’ve received a remediation plan – we’re going to publish the report where it shows the registrar and the registry, the issue that was identified, the remediation plan with the date you anticipate remediating that issue.

It’s a common process in the audit, but we want to be clear and transparent for the community. They want to know what’s going on. And when we say “publish online” it will be posted on our website. So, the reporting phase – on the reporting phase we will double check and validate the results to be reported. We will ensure that the data is clear and concise; that it will be clear and the registrar or the registry has agreed to them. We’re simply not going to publish something just to publish something.

We want to make sure that everyone is on the same page here. And that information will be published on the ICANN.org website. Some of the types of reports you’ll see – the list of the audited registrars and registries; deficiencies report where we have those. And there’s different types of deficiencies. There can be a deficiency where a registrar or registry just failed to report information when we’ve requested it. I’m not going to say that will happen, I’m just going to say that that could be one of those cases where it does, and that would end up being a deficiency and showing up on the report.



There could be a case where we collect a document and the document does not meet the standards of the contractual obligations requirements in the provision; that will show up as a deficiency. Ultimately every registrar and registry will be notified well in advance. And ten finally, turnaround time, lack of response, non-compliance – those are stats that will be published.

The remediation phase – if anyone has ever been through an audit, this is the type of thing that doesn't really occur in a firm or audit or contracted party that comes in and assists. What we want to do is take a collaborative approach with the contracted parties. We will assist you in addressing those deficiencies. Some of them may be easy, such as the liability policy not having the right requirements for the threshold. Some may be more difficult, and we understand that, and we know that some deficiencies will take longer to fix than others.

So as long as we have a proper remediation plan and an anticipated date, we'll just look for that data and assess where we can assist wherever possible. We'll track and report the deficiencies, and in some cases we'll have to do follow-up audits to complete the remediation. So if a registrar or registry comes back to us and says "hey we fixed X or Y," we'll go back and we'll evaluate that. And we'll determine whether or not it's remediated. And if it's remediated then we'll just check that off, it's done.

So for the RAA provisions under consideration, when we say under consideration, they are under consideration. We do not have enough time, resources or money to audit every one of these provisions. However, we will scope it down, we will evaluate which ones we're



going to review and those will be part of the audit plan. We'll be privy to that in part of the pre-audit notification, and you'll also see that in the RFI if you are one of those randomly selected in year one. But again, these are the provisions that we're considering and that we're reviewing and that we've built the audit plan test steps against.

Same for the registries, the common provisions amongst the registry agreements, we've looked at these, we've built test steps around them, we've built an audit plan around them and those are the ones. We're going to evaluate which ones we think are the high risk, and those are the ones we'll consider for the audit plan. So the timing – this has been displayed already in the outreach sessions that we conducted with the registrars and registries back in September.

But as you can see, it's taken months to come up with a planning phase with the audit scope and the schedule. The organizing phase where we started in September and ended it in October, we developed what we want in terms of the goals and the roles of responsibilities. As you can see for the pre-audit notification, we're looking to launch that in early November. Obviously this is subject to change as we are still evaluating support vendor to assist us in supporting this effort. It's obviously quite a big effort.

The audit phase, you can see in the audit phase we've listed just the high level bullets – the request for information; the audit; the follow-up questions. And you can see that it starts in December where we'll send the requests for information and we may send it out sooner, we may send it out around December. We'll send out a request for information



asking for the documentation that we need against the provisions that we're auditing.

And then on the reporting phase, you see that April 1<sup>st</sup> through April 26<sup>th</sup>, obviously that's flexible because we want to make sure that we do this audit right, we don't want to rush it. We want to make sure that we evaluate all the evidence and that we follow the right methodology and process and approach prior to issuing the report. And then finally the remediation phase, we want to manage and track and support. We have May 1<sup>st</sup> to June 5<sup>th</sup>, it may take longer. It depends on the issues that are discovered.

But obviously we're going to collaborate with the registrars and registries to make sure that we address those issues. So the audit program next steps – I may be blowing through this, so I apologize if I'm talking too fast. If I am let me know please. So the audit program next steps – obviously we've developed the audit strategy, the process and methodology. I've communicated that information to you just a moment ago. We've also developed a vendor management scorecard methodology and vendor selection process.

We've issued the RFP, or the request for proposal to five vendors. We've completed the RFP reviews and vendor presentations. We've presented that to – well the steering committee conducted their evaluation of those five vendors. In addition to that we've obtained approval from the Board Finance Committee in terms of the approach and the process. And we've obtained approval from the Board in terms of the overall three-year plan. What we're doing now, the current process as-is, is we're conducting final vendor evaluations.



Obviously if anyone has ever been exposed to a vendor evaluation process, it takes time. We want to make sure we find the right vendor that can accommodate, not just the right vendor, the vendor that can support us and be a cooperative with us in this endeavor. Obviously it's a new type of audit and we want to make sure that we follow the right processes to ensure that that vendor, the final vendor that's selected for the three years is one that's going to support us.

And the next step after that, according to the timeline is the pre-audit notification and then the rest of the process is onboarding and executing the program. So for additional resources you could go to the ICANN website, the audit program. I think if you've been on there lately you'll notice that it's been revised. And the audit program side actually explains this exact process that I've showed you today. The deck will be published, the presentation I just went over will be published on that site. In addition to that, we'll publish the audit plan.

This is a new concept I think, where most audits you do not get the audit plan in advance. This is different. We want to make sure that it's a clean environment and that all contracted parties are complying with provisions. And because of that, we've made the decision to publish the audit plan on the site. So for those that have asked, and I've heard your requests and I appreciate them, the request for checklists – you don't need a checklist. You see the audit plan and it tells you exactly what we're going to ask for. You can go through the steps and you'll see it.

And when the RFI, the request for information comes to you, it will follow that exact audit plan, it won't differ. So that should give you very good comfort that it will help you prepare I think. And then finally, if



you have questions or comments or you look at the audit plan and you're scratching your head and you're just curious about something. By all means, send us a question to [compliance@icann.org](mailto:compliance@icann.org). in the subject line, please put "ICANN 45 Audit Outreach" so that we know that's specifically regarding the compliance deck that we've presented today.

I think that overall our goal is to make this successful and we want to work with all of you to make it successful. And because of that we welcome any comments that you have. Okay. So I kind of figured there would be a lot of questions in this program, so we wanted to open it up to the floor.

MAGUY SERAD:

Please come to the mic and state your name before you speak.

CHANDRA:

Hi my name is Chandra, I just had a quick question. You mentioned that the new gTLDs would be rolled in I guess after there's some historical evidence to review. But I'm just wondering since they're randomly selected how many registry contracts do you plan to review per year.

JACKS KHAWAJA:

Good question. That's actually dependent on what rolls into the queue. We can't, at this point we can't anticipate how many new gTLDs will be online. Some new gTLDs can sign a contract, but it doesn't mean that they're fully operational and functional. So until we collect six months



---

of data from that new gTLD registry they won't roll up into the audit plan. Okay? Did that answer your question?

CHANDRA: Well I guess there really is no answer to my question yet. I'm just wondering if there is like a potential for 1500 names let's just say in the next two years, how many of those new 1500 contract numbers will actually be audited per year.

JACKS KHAWAJA: So if you're using the number of 1500 for instance...

CHANDRA: Or 1000, let's just say 1000.

JACKS KHAWAJA: What we do is we even it up equally amongst the years, just like we have with the existing registrars and registries. So currently it's a three year plan with the registrars and registries, where we have 1000 plus registrars and 20 registries, we've divided that into three and we've evenly randomly selected 317 registrars in year one, 6 registries in year one, and in year two, same process. So we'll roll that same methodology to the new gTLDs.

CHANDRA: Got you. Yes that does answer my question. I had another question about sort of the criteria that you emphasized that would be standardized and published in advance, but there was another slide



where you said these are the things that are under consideration that you sort of created the program to be able to test but that you would narrow that field. And I'm just wondering if it has the capability to test all of those things, is there a way for you to sort of vary the provisions that are tested in each audit, if that makes sense.

So if you have 25 things under consideration and you have the capability to test 25 things, maybe in the first audit if you were testing 10 things per registry or registrar, those 10 things would vary, but they would be one of the 25.

JACKS KHAWAJA:

I see. So, one thing that you think about when you're planning an audit is resource load, timing and cost. If we could audit every provision within a timely fashion and not impact the registrars and the registries in an adverse way, we would do that. So the way we're scoping this is to ensure that it's efficient and it's effective. If we do year one and we choose an option of say 10 provisions for the registrar that will be the same for three straight years. Because we want to make sure that it's even and consistent across all the randomly selected registrars.

We don't want to roll in new provisions because it's unfair to the registrars in year two and the registrars in year three.

CHANDRA:

Is there another mechanism outside of the audit to address the provisions that won't be included in the audit?



---

JACKS KHAWAJA: In the event where a registrar or registry is identified to have issues, whether it's through or ticketing system or other mechanisms or somebody sends us evidence, we will evaluate that registrar or registry outside of this three year process. And that's what I mentioned on – can you go back a couple of slides? That's where I mentioned it right here under the third bullet, or actually the fourth bullet, we will audit those based on issues that may arise.

So we have flexibility in the plan, but the 317 that we audit up front, as long as there are no issues, will not be audited in year two and year three. We rotate those.

CHANDRA: Thank you.

JACKS KHAWAJA: You're welcome.

MAGUY SERAD: So Chandra I'd like to add one point to that, the question you asked. The audit is a new thing we're introducing and we want to publish it and make it a standard approach and baseline for the first three years. So if there is a need to investigate in other areas, everything in compliance is still going to run the same. We will run through it based on that. I don't want people to think we're just going to do audit now for the next three years, focus on this. This is in addition to the other activities we are doing.



---

CHANDRA: Thank you.

JACKS KHAWAJA: Any other questions? Okay Michele.

MICHELE NEYLON: Good afternoon, Michele Neylon for Black Knight, rather worried registrar. I don't even know where to begin. I'm looking at this and I've got a bunch of questions, you'll have to bear with me as I try and get these to you coherently. The first obvious one I have is what happened to self-assessment. I mean the self-assessment concept is not a foreign concept. It seems to be a concept a lot of people can deal with. You started doing self-assessments and now that's gone out the window.

You're talking about an audit which was supposedly going to random, yet you're talking about publishing the results of these audits, which is then going to be picked up by third parties. Those third parties are then going to publish reports. The reports by the third parties are going to make out that the various contracted parties are the scum of the earth, even when they're not. That's what keeps happening continually. Isn't ICANN a little bit concerned that some of these, that they're publishing some of these things which could be taking a tiny little issue and blowing it completely out of proportion.

You do realize you're opening yourself up to liability? Because for example, if you audit us and you publish something on there and blow something small out of proportion I will sue you, just so you're aware. And the other thing is there's a cost implication. ICANN has a compliance department, you had the option of self-assessment and not



you're contracting with a third party. So the question is who is that third party and how are they qualified to assess something with the technical complexities inherent with the RAA and its implementation. Another thing as well, that I don't see here is, timelines with respect to actually providing you with the answers to these audits. And how are you going to cope with language difficulties as well?

How are you going to deal with registrars in countries that do not speak English? Is this all going to be based around a US view of the world? So for example, you speak about insurance, up until relatively recently the language on the ICANN website with respect to insurance didn't translate into anything and a European underwriter would actually provide. I mean there is something that they do provide, but all the terminology was very American based. I think I've almost finished.

And then on the secure environment, you're talking about providing very highly confidential information potentially in a secure environment, which could possibly include registrant details. Have you thought about how that's going to impact our data privacy restrictions under European law? Does ICANN have a safe harbor provision? Are you registered for that? I think that's about enough for now. Thank you.

MAGUY SERAD:

So Jacks, if I may help you. This is a great example of filing multiple complaints. Thank you Michele, you're testing us. Jacks, if I may facilitate through some of the questions I'd like you to respond. I took notes as much as I could keep up with Michele. And Michele if I ask your question wrong please correct me. What happened to self-assessment?



JACKS KHAWAJA:

So, on the self-assessment, when we evaluated it we evaluated the goal of the self-assessment and what we were ultimately trying to achieve. When you do a self-assessment one of the issues an auditor has with a self-assessment is that it doesn't necessarily validate the accuracy of the data. It's simply a Q&A. It asks you "are you compliant with the policy." Well okay that's a good question but how are you complying with the policy. What an audit actually does it is requests the specific information to validate that answer.

I think the community would want to know whether or not the registrars and registries are complying with the obligations, and I don't think that a self-assessment gets you there. So what we did was we evaluated it, and it took some months to evaluate it, and we evaluated the results. And what we ultimately found was that an audit seemed more logical and more effective. So that was that question on the self-assessment. Did you want to add anything Maguy?

MAGUY SERAD:

Yes the other thing I wanted to add was we need to have a baseline for audits. So self-assessment started with the assumption that we were going to be able to address a lot of the challenges we're facing. So to Jacks's point, the audit is a baseline and once that baseline is established, that means the discipline is established. The contracted parties understand what that consists of and how we want to operate going forward. And then that way we will turn on self-assessment because the knowledge is better and it's consistent, and self-



---

assessment then will take place based on what was built from there. So the next question is the random selection and the publishing.

JACKS KHAWAJA:

This is Jacks Khawaja again, for the record. So on the random selection and the publishing; if you passed we would publish you. If you failed we would publish you. So no one is excluded from being published, number one. Number two, what is the purpose of publishing the results of the audit. I think it's to give everyone in the community an insight as to what the results were. If we decide to do an audit and not publish the results I think the question would be "Well why did you do it? What was the purpose of the audit if in fact you didn't show the results of that audit?"

Again, like I'd mentioned earlier, we go back to the registrar and the registry and ask them if there is any other evidence that they want to provide to cure that deficiency before we even consider publishing it. So we give ample time, and when I mean ample – immediately when we discover an issue we contact that registrar or that registry. So in the event where the registrar or registry doesn't provide the information, we'll let them know. We'll give them a report letting them know what we're going to publish before it actually gets published on the web, so that's in advance. So the registrar and registry has advance notice of that.

MAGUY SERAD:

Random selection.



---

JACKS KHAWAJA: So on the random selection, what we're doing is we're doing a random selection by IANA number, not by registrar name. So essentially what we do is run it through a program. That program collates and comes up with 317, which is the sample size we've selected, it's evenly across the board, 317 registrars and 6 registries. Those IANA's will return through the program with those 317 registrars, those are who we're auditing. We are auditing based on the IANA number, so we are not making a selective approach on the audit.

We're not basing it on anything other than a random selection and that's it. So hopefully I answered your question on that. Maybe not to your liking.

MAGUY SERAD: Let me run through them. Again we want to give the courtesy to other audience members to ask questions – cost implication and use of third party.

JACKS KHAWAJA: On the third party, as I had mentioned earlier on the other slides, we have a very rigorous process when it comes to evaluating vendors. At this point we've reached out to five and of those five we have a multitude of documents that we have to go through. Those documents take a lot of time. We want to get this right. And we don't want to rush it. And because of that, we're still going through the process of vendor evaluation.



---

With that said, the third party will be announced once we enter into a contract we will notify the community of that selection and what that process was. Did you have anything else to add Maguy?

MAGUY SERAD: No. Timelines to provide answers.

JACKS KHAWAJA: So, you had asked for a timeline for response. In the request for information, we're going to follow the one, two, three process based on our normal operating procedures. If everyone has seen in the last probably three or four ICANN meetings Maguy has shown the one, two three process, where notice one, which is in this case 15 days. The registrar will have 15 days to upload their documents. Notice two will be another five days, and notice three will be five days.

In the event where a registrar or registry needs more time we'll allow that, because we know there is going to be some documentation that's going to take some time to gather. However, it's not open ended. We'll try to stick to that one, two, three process, but we will allow time to upload all of that documentation. Okay?

MAGUY SERAD: Cope with language difficulties and is this a US view of the world.

JACKS KHAWAJA: One of the considerations of a vendor is to seek a vendor that has a multinational approach, has knowledge of international laws and has



the skill sets to handle translation when needed. So when we evaluated the five vendors and we'd reached out to those vendors, those vendors had to meet certain requirements. Those requirements specifically entailed having a multinational model so that they can address those types of requests when we get documents in.

If we're looking for language in a document, they'll need those services to be able to translate that. Hopefully that answered that one. Okay.

MAGUY SERAD:

Actually it's better than just translate, we require that they are speaking that language and not just translating. The last question I have Jacks is secure environment and the impact of data privacy.

JACKS KHAWAJA:

What we've asked of each vendor that we're evaluating is to provide their diagrams and their scope of how they intend on securing the data. One of the biggest things that we've considered is registrant data and how important that is, as well as the different laws, the privacy laws and so on and so forth. We've obviously considered that. And what we're doing is we will select a vendor that has the proper support tools that sit behind the DMZ that are fully encrypted, fully secure and that is fully protected.

As I said earlier, access control is big too. We want to make sure that only a few people have access to that data. We'll have an NDA and a contract with that individual company, whoever that company is to support us. And that information obviously will be secure between us. So the liability – well I don't want to address the liability issue because



---

obviously it's always under consideration. Hopefully I answered your question.

SAMANTHA EISNER:

This is Sam Eisner from ICANN Legal. ICANN itself as a not for profit actually does not qualify to apply for safe harbor protections, but I know that that has been one of the considerations within the RFP itself. And so I think we do need to take a little bit more look about the further transmission of the data. But we expect that any vendor that we select will be safe harbor compliant.

MAGUY SERAD:

Thank you Sam. I saw some hands, Ray.

RAY FACET:

Hello Maguy, this is Ray Facet from dot jobs. If you don't mind can I pick on Jacks a little bit, can I do that, is that allowed. Alright, so I'm going to share what you shared with me outside Maguy about one of your words that you hate using the most, and I hate using the word hate but I think one of them was "I," right. So I think we need to be a little fair here in some of our choice of words, in that when we say that I think Jacks, "I think that the community wants to see this information," another way to say that would be "I think the community wants to have some reasonable assurance that compliance within ICANN is effective."

Now one way to get there would be "I'm just going to publish everything," right. I'm just going to turn around and publish everything. So I think why don't we ask the community what they would find

---

reasonable in terms of measuring, or what they want to know in terms of how effective ICANN compliance is before we just make the decision we're going to publish everything, which is basically throwing somewhat to the other gentleman's comment, just throwing the contracted parties sort of being your mechanism for showing the community that compliance is effective. Does that make sense? And I have some other questions, that's just a general concept.

JACKS KHAWAJA:

Good questions, point taken. We, in terms of ICANN compliance, developed this program to be successful. It was not to put people on point. I think – I – when I say I I'm referring to the contractual compliance department in this regard. It's incumbent upon us to ensure that the contracts are being complied with. One of the mechanisms to do that would be an audit. I don't think anyone here would argue with that concept. Maybe not the program itself, but the concept itself would make sense to people.

And we have heard from the community. Every single time we come to an ICANN meeting we hear from the community. And so I think that's pretty fair for us to publish an audit and the results of that audit.

RAY FACET:

Okay.

MAGUY SERAD:

So jacks, if you don't mind, can you go back a few slides up where we say "why are audit." If I can show a raise of hands, how many today in



---

your companies today get audited whether it's financial audit, IT audits, all kinds of audits exist in this world. Right. Do your departments do it to show their effectiveness or the effectiveness of the department delivering a specific service expected of them? You're right Ray, compliance has been under the fire since my arrival. Everybody tells me I'm five years late, there it goes again. It is a step to show effectiveness, that means we're doing our job.

So publishing is part of many things the community wants to see published. And as you are very aware of our process, the one, two, three step, and I think I have many representatives here even from ALAC that want even information from the first step. And what's my answer Holly? Not to put you on the spot.

HOLLY RAICHE:

Quite happy to. I'm absolutely thrilled that this is going on, I have to say. Poor Maguy has had to front the ALAC meeting for the last two years. We've given her a most miserable time because we are frankly not convinced by the self-assessment process. And I think if she goes through one more year of facing up to the ALAC she's probably going to quit because we might make her. But I'm frankly thrilled and I think this is a terrific process.

So when you say who's asking for it, I can tell you a lot of us are asking for it and a lot of us are just pleased about the steps.

MAGUY SERAD:

I don't want to turn this into a Presidential Debate, but what I would like to do is remind everybody when I first joined we also established a



vision for this department. It's to become a trusted contractual compliance service provider. And trust takes time. And in this multi stakeholder model obtaining this trust has to be based on fact based decisions. For us to deliver fact based decisions, to measure not only the effectiveness on the compliance department delivering a service that's expected of us, but of each and every contracted party delivering a service that's expected of them.

So that's all I would like to say and close it.

BRET FAUSETT: I'll go on to the next if you don't mind.

MAGUY SERAD: Well can we give the courtesy to another person, so that we have [Asish] on the line and I see Matt and we'll come back to you. We have time.

[ASHISH]: Just a simple question, you mentioned roll out in 2013, but then when...

MAGUY SERAD: [Asish] we cannot hear you and please announce yourself.

[ASHISH]: One of your slides mentioned roll out to be 2013 and then another one mentioned pre-audit notifications going out in November, so I'm just



---

trying to figure out because you also mentioned that the vendor is still being selected. Just some clarification, thank you.

JACKS KHAWAJA:

Good question. You're right. I did notice that. But there was a point in there, because it is a flexible schedule. Because the vendors are still being evaluated this schedule may change. We're shooting for those dates. Going to the point where November is mentioned, November is the point where we send a pre-audit notification letter. It's simply to give people the heads up, to outline the different provisions, to outline the process, to make sure that everyone is aware.

Because not everyone is listening on the phone, or in this room today, so we're going to make sure that everyone understands what the scope is of it. When I say a December timeframe, the request for information, the audit itself of evaluating the data will take place in January 2013. The request for information will go out in December to collect that data, it's going to take us time. It's going to take a lot of time. Not a lot, hopefully not a lot on the registrars and registries, but it will take time to collect that data. That will start in December.

BRET FAUSETT:

And on that example, the pre-notification audit letter comes in how much in advance of the actual request for records? I thought you said that there would be a pre-notification letter I was just curious about how far in advance.

---

JACKS KHAWAJA: What we're going to do, under pre-audit notification under the flowchart on the screen it says "two weeks prior," so we'll send it two weeks prior to when the request for information comes.

MAGUY SERAD: Matt? I have Matt then Ray?

MATT SERLIN: This is Matt Serlin, I'm the Chair of the Registrar Stakeholder Group. I apologize I was late, so I might have missed some of this. The RFP that you're talking about, was that a public call for an RFP; was that something that was published on the ICANN site?

JACKS KHAWAJA: In the October, number one it wasn't made public. Number two it's part of the Board minutes October 3<sup>rd</sup>.

SAMANTHA EISNER: We have just published the RFP as part of the Board meeting materials posted on the Board meeting page on the website. So if you go under the October 3<sup>rd</sup> meeting, if you go into the Board briefing materials in the second book you can actually see the full RFP.

MATT SERLIN: So it's there, it just takes some navigation, maybe Michele could find it for us.



---

SAMANTHA EISNER: I'll drop a link actually into the Adobe room.

MATT SERLIN: Perfect. Cool thanks. Because you're right there, you're close, I can pop you in the head. Secondly, is the contract once executed going to be published?

MAGUY SERAD: The contract with the vendor?

MATT SERLIN: The contract with the party that wins the RFP, the vendor.

MAGUY SERAD: You know, I do not know. Can I get back to you? I do not know.

MATT SERLIN: You can yeah, sure. Mine will be brief, so not a lot, maybe a lot of questions but quick answers, sorry Ray. Jacks, I heard you talk about the timelines to Michele's question and you used phrases like "ample time" and "ample opportunity" and from a registrars standpoint I get a little nervous about that. Is there someplace that a registrar or registry can go to see the specific timelines. So in your view it might be ample, and what's ample to one person isn't ample to the next.

One registrar may get – so is there something that says "once presented with the results the contracted party has X number of days," is that information out there somewhere? Do you mind answering again?



---

MAGUY SERAD: Let's see if Michele was listening.

MICHELE NEYLON: Oh Michele is doing more than listening Maguy, I'm taking notes.

MATT SERLIN: He's tweeting in real time, come on we know that.

MICHELE NEYLON: They referred to their famous – it's one of Maguy's catch phrases, she's got swim lanes and she's got three step. So it's the 15 days, 5 days and then 3 is it? 5; so it's 15, 5 and 5. So 15 days, then they get upset with you and send you a reminder you've got another five days and then another five days. The bit which isn't 100% clear to me, and I'm not sure about anybody else, but then maybe they all read your minds so I'm not sure, you said, on that note that if the contracted party was having issues or difficulties that you might allow them extra time.

Now you said you wouldn't let them kind of roll on forever and I can understand that and can appreciate that, the kind of fear that Matt's pointing to is extra time an extra day, an extra week, an extra...it's just from our perspective, and the other thing is when you're talking about December that rang alarm bells for me considering that from about the 15<sup>th</sup> of December onwards staff kind of disappear, lawyers disappear.



MAGUY SERAD:

So Jacks, let me take this one please. I do apologize on behalf of the contractual compliance team for saying ample time and I think that's something I've worked with Jacks on. I don't like the use of adjectives either, where's Ray? I don't like the verb hate, I don't like to use I or believe. We are fact based. Ample time is not measurable, you are correct. So Matt if I may answer your question briefly. A lot of that timeline will be defined further with specific dates deliverables, but until we have approval to proceed, vendor selected, we know what we would like, how we'd like to proceed.

To the community members who it's not just a close where you don't know where these dates are. We will publish a calendar. Our objective is to publish a calendar start date, next milestone, all these measurable steps so everybody can keep track of where we are. And the question of I think a combined Matt Michele question, if a registrar needs help or there's something, it has to be on a case by case otherwise it becomes chaotic. We don't want a forever open audit program. We need to be able to make measurable milestones, close it, report and move on to the next phase. So with that did I answer your question?

MATT SERLIN:

You did and just one more, I promise I'll be quick. And I agree with that, and let me also just be clear that we are supportive of this program, so I want to make sure that the criticisms or the questions that we're asking are understood in the light that they're meant to be in. That does make sense, thank you. The only last thing that I'll comment on is what Ray and Michele both touched on is the notion of publishing the results. And you talked about doing that to basically prove effectiveness of the



---

program to the community, and I think that's great. But I might suggest that you could do that without naming names essentially.

You can take the aggregate numbers and indicate, at least in the, this is the first time basically – hold on, thank you. He gets a little overzealous sometimes but I don't mind biting back. Since this is the first time that we're going through this program, I think that it might behoove the entire community to see that aggregate data right. So that out of the 317 in year one, just whatever the percentages were, whatever the numbers were. I think you understand our fear frankly is that registrar X failed an audit and it's splashed...

It's just a concern that I think all of the contracted parties are going to have. And so I don't think that you have to publish that specific data to prove the effectiveness of this program in the first round.

MAGUY SERAD:

I'm going to take that one too please. You can tell how passionate, it's like Michele and you, Jacks needs to be here so. Regarding publishing, I've heard what you are requesting, but what I would like to say as we are planning designing reports and all of that, we are going to work first, and I'm saying it very transparently, with our contracted parties, because they are the parties impacted by this from a workload perspective, from showing their compliance. But we will come back and inform everybody else also what's going on.

For example, before we came to this community sharing what this contractual compliance audit is about, we held three sessions in September open to all registrars and registries to dial in so we can



share this information with them. And that's where I think we had a registry, I think it was Desiree if she's in the audience, and another registrar that asked about an audit plan or what they referred to as a guide. That was actually a recommendation that came through to help drive what is it and how do we look at it, because we all know businesses run and are operated differently.

What is interpreted with registrar or registry A or B is going to be different. So we want to make sure that consistent approach that Jacks referred to is clearly understood by all so we can truly do an apple to apple regardless of the size. So again, to the reports Matt, it's like a report card we would publish, but the designs are not completed. There will be a generic report, but there will also be an individual report that will go just for the registrar.

And as Jacks stated, we will work specifically with the registrar to try to mitigate and close on those before the reporting period, if you see the timeline. There will be opportunities to collaborate and clear these things if there are issues. So what I'd like to do is take another question from the audience before we close. Do we have somebody on the...okay. Can you read it Atif, please?

ATIF BEG:

This is Atif Beg, ICANN Compliance for the record, reading a question from Barbara Knight from VeriSign. The question is: "If a registry operator operates multiple TLDs will you be auditing all TLDs operated by the registry operator when the registry operator is selected?"



JACKS KHAWAJA:

So, in the next few weeks, something that we didn't mention here which needs to be mentioned, is we're going to publish an FAQ, a frequently asked questions, regarding the audit program, and it will be addressed there. But to answer your question specifically, because I've actually had this conversation with the liaison teams, in the event where a registrar has multiple TLDs we are looking for, we'll do a random selection of the domains, it's not going to be an extensive amount of domains, and we'll request the information to address those specific domains.

In the event where you have multiple TLDs, and you just happen to get selected – how do I put this – you just happen to get selected as a luck of the draw, you have 10 domains that have different TLDs, we are going to collect information based on the audit request. So if you say that I have the same document that's applicable to each one of those that's fine just let us know, because that means you have the process in place.

MAGUY SERAD:

So if I may summarize what I think I heard you say, we will audit by agreement if the information is consistent across the agreements that you support you can say so and we will note that. Is that right? Thank you. Any on Adobe, Atif? Ray? I skipped you because we went from Matt to...sorry about that.

RAY FACET:

The scope, you talked about scope. There are actually a couple of slides up there that actually had sections out of the RAA and the registry



agreements, is that the scope itself or will the scope vary by – for example I’m a registry operator so, this is Ray Facet from dot jobs by the way. Will the scope of these audits vary depending upon whether it’s a community TLD or a type of TLD, that’s one question.

Two will the questions, will there be human interaction on these questions? For example, I can tell you from our experiences in what’s being called an audit now is we used to call a compliance review. And in compliance review questions that we’ve received there were some that the questions were just flat out wrong, but we weren’t allowed to sort of modify the questions. We would discuss this with ICANN staff, that the questions were just invalid. How do you answer an invalid question? And the answer we got was “just answer them the best you can.”

So we would try to correct the question by the response. It was very challenging. So I’m wondering if there is human interaction on the questions or not?

JACKS KHAWAJA:

Thank you for that Ray, and that’s actually a really good question. There will be human interaction. And essentially what will happen is we’re going to publish the audit plan, the audit plan outlines the test steps and the provisions that we’ll review. That is the basis of the request for information. So if you’re looking at the audit plan that will be published soon and you see issues with it or you have questions with it, please send us an email and let us know. We’ll address it.



---

And the other thing, so what you see up here, this is just the registrar agreement. It's not going to increase beyond this. It's actually going to be scoped down for the timeline and the resources that we're going to need. So we are not going to audit all those provisions. We will select the high risk provisions and those are the provisions that you'll be notified about in the pre-audit notification letter.

RAY FACET: So if I understand the answer correctly then, the scope of the audits for both registries and registrars are going to be very much standardized.

JACKS KHAWAJA: Absolutely. Yes.

MAGUY SERAD: The scope will remain the same across the three years so we can do an apple to apple comparison across all the contracted parties. Human interaction, I think since I've been here, have you guys been able to do human interaction with compliance. No, yes.

RAY FACET: Well that's fair Maguy but I mean upon receiving the questions will there be an opportunity to discuss those questions, potentially modify those questions if necessary, if agreeable, I'm not saying one way or the other. I'm just saying in the one experience that we've had there was no opportunity for that. It was just shut down.



---

MAGUY SERAD: So what I'm hearing is maybe an opportunity for you guys to review the audit plan and provide input if it's clear or not. Because once it's issued it's preferable if we have questions and it's not clear, then whoa that's a problem.

RAY FACET: And again to be fair in our own experience with that job it was a very one off type of review, but you're talking about a standardized program and that changes the context of my question. So I think you've answered it very well. Thank you.

MAGUY SERAD: Thank you.

MICHELE NEYLON: Oh don't look so scared Maguy for God sake. Two things, you've got a list up there on the screen which is actually perfect because this is the list for the registrars. And one thing I noticed immediately is there are several provisions that you're focusing on that are specific to the 2009 RAA. They are not in the 2001 RAA, so therefore your entire "comparing apples with apples" analogy falls flat on its face.

And secondly, when the randomization by IANA ID, while an interesting concept, also has a, well not inconsiderable issue. There are several registrars who have several hundred accreditations. How on earth are you going to manage to do this in such a fashion that you basically don't end up auditing every single one of enoms accreditations and a couple of others from, oh I don't know, the moniker snap names group of



---

companies and the rest of us will be left alone? Not that I don't mind being left alone, don't get me wrong.

JACKS KHAWAJA:

On the first question with regards to the provisions, we haven't chosen which registrars will be audited yet. Obviously there are 2001 agreements and 2009 agreements and we're taking that into consideration when we consider the scope. That's number one. The scope meaning the provisions that we're actually going to audit across the board. Okay? So we used 2009 as a baseline, just so you know. That should give you perspective as to what you're seeing on the screen.

Number two, I'm sorry. Can you repeat number two?

MICHELE NEYLON:

The IANA IDs. Basically the problem being that if you've got a registrar with 250 accreditations, another registrar with 100 there's 1000 accreditations realistically that's only 250 companies.

JACKS KHAWAJA:

So in that regard, if in the event where an individual receives 10 RFIs, 10 requests for information, it's because they obviously have what you just described, different contracts. If they operate under the same procedures we will take one document. Meaning that if they have different TLDs, different registrars, like a family for instance, we will take just one document to compare against the provisions. Because

---

ultimately we just want to know if there are policies and procedures in place and if those obligations are complied with.

So we won't ask you to upload the same exact document 50 times. That's not the process. It's a good question.

**BRET FAUSETT:** This is Bret Fausett. Can I just rephrase what I think you heard so that I make sure I understand it? So the audit will be by contract that you signed with ICANN, not by companies or credentials, is that right? Is that the grouping?

**JACKS KHAWAJA:** That's correct. We have one question online, this is Jacks.

**ATIF BEG:** Atif Beg, ICANN Compliance for the record, reading a question from Mick Moran from Interpol. The question is: "How many people are currently in the compliance team at present and how many do you plan to hire to put this ambitious plan into place?"

**MAGUY SERAD:** Mick hi, this is Maguy. Where are you, what part of the world? So you answer your question, we did provide a brief update to law enforcement but we are at a total of 15 head count. And to leverage an exercise of this nature and be able to turn around to the community in a timely fashion, what we did was engage with third party vendors to be our extended team members in this exercise. But the leadership of this



---

exercise and the communication link between us and the contracted party and the community, the publishing, all activities that touch the community are lead and done by our contractual compliance team, which is ICANN staff. So I hope I've answered your question. The gentleman over there, you had a question. I'm sorry I don't remember your name.

MARK:

Mark from Microsoft. I have I think more of an observation than a question. Since you will be maintaining the same audit process for three years there's a very good chance that you will encounter ambiguities in the questions, errata in your mechanisms and things like that. please consider publishing in your FAQ some information about the cadence at which you will roll out the new changes for the people going forward and information about whether people who have passed under the old regime compared to the new people coming in, whether they're grandfathered in or whether additional information will be – I wouldn't ask you to answer this question here today, but please consider that and publish that in your FAQ.

JACKS KHAWAJA:

That's a great comment and we'll take that under consideration.

MARK:

Thank you.

MAGUY SERAD:

Matt?



---

MATT SERLIN: Yeah thanks. Sam, thanks for sending the RFP. Matt Serlin for the record, and I might have again missed this so apologies for coming in...so the RFP has anticipated announcement of vendor selection October 8<sup>th</sup>. Now I'm confused, I think we're after that.

MAGUY SERAD: Anticipated.

MATT SERLIN: Right, so clearly that didn't happen. So what's the new anticipated?

MAGUY SERAD: We will inform you when we close on the review and evaluation of this. As you understand, as you heard us say, it's very complicated. It's not a standard audit that's been accomplished in the past, so we're doing very good due diligence and reviewing the documents and then the selection. We will announce that as soon as we have a new date.

MATT SERLIN: Okay.

MAGUY SERAD: Ray?



---

RAY FACET: Just a point of clarification, Ray Facet from dot jobs. Real quick, in these slides when we talk about contracted parties, there's going to be the trademark clearinghouse, there's going to be contracted parties with that, you have contracted parties for your office lease and things like that. The focus of this is really registry and registrar contracts. So not all contracts are following this compliance program, it's registry and registrar contracts. I just wanted to point that out. Thank you.

MAGUY SERAD: Yes.

MATT SERLIN: Can I ask another question? Sorry. Are we over time?

MAGUY SERAD: No we have until 4:45.

MATT SERLIN: Okay cool. So maybe can you just explain to me what is meant as – sorry I'm looking at the RFP again, thanks Sam. It says "To provide such services it recommended that the vendor have" and it has six criteria. The first is "Experience in auditing DNS environment." Can you just maybe talk through what, if I was reading this RFP and I received that what would I demonstrate as a qualification for that?

JACKS KHAWAJA: This is Jacks for the record. So what we've asked is we just want to know if they have exposure and experience in auditing a registrar or



---

registry. We want to understand whether or not they've been through this before in any capacity, and they understand the mechanisms that drive how a registrar or a registry operates. And that was part of a clarification follow up set of questions that we gave to them because that was the first question they asked us. Good question.

MATT SERLIN: Thank you.

JACKS KHAWAJA: Thank you. Well if there are no more questions, I'd like to thank all of you for participating. This has been obviously educational for all of us. And if you have any questions by all means send us an email to the [compliance@icann.org](mailto:compliance@icann.org) and we'll be more than happy to entertain any questions that you have. So thank you all.

[End of Transcript]

