BEIJING – DNS Risk Management Framework Update
Thursday, April 11, 2013 – 10:00 to 11:00
ICANN – Beijing, People's Republic of China

CHAIR: We might as well get started on time. Welcome to the Risk Management Framework Working Group meeting. This Working Group exists as a Board Working Group as an indication of the importance that the Board allocates to getting a proper Risk Management Framework in place for the DNS in the ICANN context; and I emphasize in the ICANN context here because we of course don't want to overstep our bounds.

The last couple of meetings – I guess we met in Prague and worked through the Terms of Reference for a request for proposals. We met in Toronto with the consultants, Westlake Governance, and provided them with feedback on their preliminary plans.

Today they are going to deliver a significant chunk of their findings so far and this is really intended to be a really interactive session between the community and the consultants, with a view to providing substantive feedback for the next and almost final state of work, which is to deliver the draft report.

That will be tailed well before Durban so that there is an opportunity to review it and comment and then we'll have another meeting in Durban, face-to-face, to go through a final round of comments and so forth before the first phase of this project is finalized.

So I'm very happy this morning to have with me Richard Westlake and Colin Jackson of Westlake Governance. And perhaps we should go around the room – should we? – and find out who else is with us, and then we can start with the discussions. So if you would indicate your name and affiliation, if you have one please.

FUNG: Hello everyone. My name is [Fung? 00:04:56], I'm from China, the China Academy of Telecom Research. I'm from IT, so I was sitting here listening and sending emails, but I find your topics very interesting so I'm going to stay here for a while to listen to the… That's all.

JOE ABLEY: Joe Abley, ICANN Staff. I work in DNS Operations; we do L-Root and other DNS stuff.

JULIE HAMMER: Julie Hammer. I'm on the Board of .au. I'm also on the SSAC and the ALAC Liaison to the SSAC.

MIKEY O'CONNOR: I'm Mikey O'Connor; I'm Chair of the DNS Security, Stability and Analysis Working Group. It's been so long since I've said those words that I can't even remember them. I'm also a Member of the ISP Constituency.

DAVID MORRISON: David Morrison from .nz country code TLD.

DENNIS JENNINGS: Dennis Jennings from a company called Knous Limited. I've been doing some work on IDNs for ICANN up until the end of last year, and I've become particularly interested in the risks associated with moving forward with IDNs.

JOHN CRAIN: John Crain with ICANN, working on security matters.

JAY DALEY: Jay Daley from the .nz TLD.

RAY PLZAK: Ray Plzak, Member of the ICANN Board, Member of the Committee. Mikey, I thought you were just going to start by saying you were the Chairman of the DNS? [laughs]

PATRICK JONES: Patrick Jones, with the ICANN Security Team. I've been helping to shepherd the Board-level Working Group and [less lake? 00:06:50] through this process.

JACQUE LATOUR: Jacque Latour with .ca TLD, and I'm on the DSSA Working Group.

WARREN KUMARI: Warren Kumari, Google and SSAC, oh, and NomCom. I don't know if any of you have considered the wonderful opportunities afforded to you by serving on the Board? [laughter]

CHAIR: That was an advertisement in the middle of all the messages.

WARREN KUMARI: Hey, I work for Google; you get ads all the time. [laughter and applause]

UM: [inaudible 00:07:25] from the .jp registry.

PATRICK FÄLSTROM: Patrick Fälstrom, Chair of SSAC, and I'm also working for [NAC NODE? 00:07:34] running I-Root and ISX and a whole bunch of other things. I'm also on the Board Risk Framework Working Group.

SUZANNE WOOLF: Suzanne Woolf, I serve as the Root Server System Advisory Committee Liaison to the ICANN Board. I'm on the Working Group and my day job is with ISC, which runs the F-Root name server.

MATT STOFBERG: [Matt Stofberg? 00:08:00] from the .se registry.

UM: Okay, so obviously everyone is saying hello. My name is [inaudible 00:08:07], I'm with .ae and around here in my capacity as being a Co-Chair for the DSSA for the ccNSO.

JOE ABLEY: Joe Abley here again, since Warren has started it, if anyone wants an L-Root node in their network they should see me afterwards. [laughter]

CHAIR: Okay, and anyone that's not sitting at the table, please feel free to join us at any time. There are lots of seats here. So, I don't think I will take up any more time, I think I'll just turn this over so we can get to work. So, Richard, take it away.

RICHARD WESTLAKE: Thank you. We are English-speaking New Zealanders working here in China today, and so I would like to say first, *ni hao* [Chinese] – good morning ladies and gentlemen. My name is Richard Westlake, as you have already had introduced to you. Colin Jackson, my colleague is with me.

Some of us… We have worked with ICANN in a number of areas over the last few years, and one of my other colleagues, Vaughan Renner, was with Colin in Toronto when this project started – some of you will recall Vaughan both on that project and earlier; he's attended both ICANN meetings and IETF meetings.

We have a business, Westlake Governance, which is a governance advisory business. We work heavily in the risk management area. We all have backgrounds in governance. I have something like 20 years as a Board Chairman and a Board Member.

My own business has been going now for nearly 15 years and both Colin and Vaughan, who are two of the principles working with me, also have extensive governance experience. Vaughan; Senior Management Chief Executive in multi-national companies and he's an engineer. He is currently also on the Board of Standards New Zealand.

Colin to my left is a former President of .nz, so has extensive experience in DNS, in policy and also in TLD operations. And I have a varied industry background, long technical background and I hope – the ability to identify smart people to work with. One of my previous boards in fact I also chaired Standards New Zealand for about seven years.

Our business is to build boards into effective teams and of course a large part of that, and perhaps an increasingly appreciated part of that is identifying, managing and mitigating risk at all levels – so we're delighted to be here. If I can perhaps hand over to Colin, who can provide the bridge from the Toronto meeting to this, to start with, as a lead-in to the next phase.

COLIN JACKSON: Thank you. Kia ora everyone. This slide – in fact the last slide as well are things we put on the wall for Toronto, so anybody who is both attentive and was there will recognize them. I just wanted to make the point here

that a risk management framework is a framework. It is a structure, it is a series of processes, and it is a way to think about risk.

It is a way to avoid all those things like confirmation bias, groupthink, messenger shooting that we as humans are all too prone to do and I know, I've done this myself and I think probably everybody here would have to agree that they've found themselves in those situation.

So the reason we do frameworks like this is simply to provide some kind of structure that enables people to say: "No, wait a minute, this hasn't been adequately address and I can demonstrate it using a process or a structure here."

Thank you. Now, there are quite a lot of generic risk frameworks out in the world and that's not surprising really, they all do substantially the same thing. We identify quite a number of them, and here you can see the NIST one, ISO one, COBIT's got one… There are several.

They ultimately do some quite generic things over identifying risk, assessing risk, mitigating and then going back to a residual and looping back around and determining what needs to be done. And this is well understood, frankly. It's really not rocket science, to use that horrible buzz-phrase.

But ICANN of course is in somewhat of a special situation and the DNS is a particularly special object and that's why we were asked to come up with some way of tailoring a standard risk methodology to suit this situation. Thank you Richard.

Again, this slide is largely what was presented in Toronto. We have filled in rather more ticks on the boxes since it was shown to you in Toronto. As you can see, we did indeed come to Toronto. We developed principles, which we will show you shortly.

We have indeed analyzed candidate frameworks and tailored them to fit the Multi-Stakeholder environment, and we are hoping today to test it using some example risks from the DSSA. And of course, right now we are presenting here our interim results at Beijing. Thank you.

So what we thought we would start with was, let's begin with the principles – what is it we are going to try to achieve and how are we going to try to get there? These are some of the ones that we identified and we have used in forming our… Taking our framework to forming the framework.

First and perhaps one of the most important is that ICANN is a unique identity heavily embedded in a community of shared interests with a shared outcome. In simple terms – I'm open to challenge, but in simple terms – that shared desired outcome is the stable operation of the DNS.

The second principle is that the DNS itself is technically unique and important and perhaps as importantly, nobody actually owns it. Nobody owns it, nobody controls it. Thirdly, what we are going to do, what we intend to do is to provide a means to foster an enduring risk culture right within and throughout ICANN.

We proposed to adopt what has been done in many ways. For example, with the root server system, of avoiding a monoculture – one approach

does not always fit all, and in fact one approach may not be the right approach for some.

And also, we do not believe in doing work that's already been done. So where possible we are and have adapted rather than reinventing. For example, we have taken the extensive work that Mikey and the DSSA Working Group Team have completed – they did extensive work there, and we have used that as a significant input and tried to build on that.

We have taken some of the frameworks from the ISOC risk management standard, the ISO 31000, which I might say, by the way, with my proprietary interest, did originate as the Australia/New Zealand risk management standard for 360, about 12 or 13 years ago.

We've also taken a lot of work from academia and from other sectors, other industries – from banking, where I have a significant involvement and also from flight safety, which goes back to my earliest career of all, where, for example, any major respectable airline that any of us in this room would wish to fly with, will have a core purpose in terms of its risk culture of passenger safety.

And every assessment, every piece of risk management, every strategic decision is measured against, how does this contribute to passenger safety; to making sure we have the same number of landings as we have takeoffs?

One of the most important principles – and this is one that we will come back to time and again – is that whatever process one develops, whatever process one invents, process on its own is useful but not a substitute for thought. If it were a substitute for thought we could

simply give you a process, plug it in and go and all walk away. Please never allow that to happen.

And finally, we are intending to cover risks that are within ICANN's sphere of concern, for want of a better word, but let's accept that ICANN's own remit and ICANN's own sphere itself is limited, so many of these risks are not necessarily under ICANN's control.

Now, the other thing that we've recognized is… And recognized really early in this, is that we are not the technical experts. Some of the smartest technical people in this field are sitting in this room right now. Our job however is to provide a framework and to help; by which you can then identify the various technical risks, in particular, and populate that framework.

But not all of the risks will be technical, and we'll come back to that aspect as well. One thing around risk management as a whole is a principle. And this is something that takes a bit of appreciating. It's that risk management itself is not a natural process. It flies absolutely in the face of our natural can-do instincts.

So risk management is a process that you have to try and embed into a culture, but you then have to continually reinforce it because it flies absolutely in the face of almost everything else that we are trained, conditioned and willing and wishing to do.

And the second point is that a risk culture is not the same as simply risk avoidance, and most of you will be aware of that. We'll come back to that time and again. From our own business, we have three principles

that we tend to work with, whether it's with ICANN or whether it's with other organizations.

The first one is that we operate by practitioners, for practitioners. We want to give you something that is actionable. And in order to be actionable and worthwhile, it also has to be measurable. So those are the three principles that we're working to and when we get to Durban that is exactly what we intend to deliver.

So – first stage. We looked at the type of framework. One size, as I said, does not fit all. There is a category of risks that are controllable. These are risks where there is actually no strategic benefit if they crystallize. So there is only downside. And therefore the strategy or the policy should be, as long as the benefit to cost-ratio stack up, that we will reduce, eliminate or avoid those risks.

This is a well-understood process, well-practiced process, and there are many, many approaches to doing so and we can simply adapt or adopt existing practices to encompass those. Secondly, there is a range of risks that are external events, over which we have no ability to control or influence their occurrence.

For example, there is no point in building a set of rules telling the San Andreas Fault that it can only rupture once every 3,000 years. It may not listen to you. Within that there are perhaps three segments. Time-bound segments. The first one; the immediate risks are the natural hazards or perhaps economic catastrophe or major political change.

We can't control the incidents. All we can do it understand what some of them might be and develop a mitigation. Secondly, there are the

medium-term ones. Disruptive technologies, for example. Some type of competitor moving into the market. And in the longer-term ones there are the geo-political changes, there are the environmental changes.

They're quite often described or referred to under the catchall category of *force majeure*, when you're writing your contracts. In other words, no one of us could have foreseen these; none of us has the ability to have managed it in advance of happening.

Now, the point about these risks, again, is that they are easier said, easier talked about, than genuinely managed proactively. Because, like it or not, our thinking is anchored. It is anchored in the known knowns, and even in the known unknowns. It's anchored in our bias to listen to advice that confirms what we think and to discount advice that disagrees with what we think.

It's anchored, dare I say it, in a sense of groupthink, where we have a bunch of very smart people sitting around a room. You may well have a team of champions with a very dysfunctional team, because they get a sense of groupthink or a sense of momentum, and it's very difficult to stop or break that.

And as I said, risk management and assessing and dealing and accepting risk is not a natural action for individuals to do. And then there is the third category of risks. And for this entire model I do owe acknowledgement to Robert Kaplan, one of the world's leading management proponents and thinkers. Many of you will be aware of his work.

He was one of the original [eaters? 00:22:33] of the original triple bottom line form of reporting, of planet, people and profits. Harvard University and regular author within the Harvard Business Review. And he put together this, if you like, described the framework in this way. And this third segment in the circle is the strategic risks. Those are risks that actually, quite contrary to the other two, we don't try to avoid.

Those are ones we consciously and deliberately go and take. They can arise from a decision that we might take, or in some cases from the failure to make a decision. They're also different – not only are they discretionary, because we choose to incur those risks, but they're also, if we categorize them properly, they're also temporary.

Because once we have made our decision we go ahead, we see which risks crystallize or then our potential risks that may crystallize, and those residual risks then transfer into the other two segments. So this is a very generic, very basic, fairly simple outline to start with.

What I'm proposing to do now is to show how we can apply this model in practice and then Colin will speak and will take us through how this applies in ICANN's unique position, ICANN's unique role. So the first one is the controllable risks. This is the one that is very well accepted, well proven, well-tested methodology. I'm sorry that the script is fairly difficult to read, but the process won't be strange to most of you.

We start with identifying, brainstorming whatever it might be and then assessing risks. And then we work through a risk process. We do this because there is no strategic benefit so we want to set a set of rules, a set of mitigations, a set of process, to in a way where the benefit of

doing so exceeds the cost – avoid, manage or mitigate, or transfer that risk elsewhere.

To a large degree we have worked through the report provided by the DSSA Working Group and our view is that that would apply very, very heavily in this particular area.

The danger we see is that if one tries to take this – and this is very much the risk or the danger, I should say, the hazard with taking existing risk methodologies –, is that you can apply it wrongly in areas where you might imply you have control, where you imply you can make rules, when in fact you can't. You can get caught in a process of groupthink if you have the single process for all of it.

Many of you will be aware of the Challenger, the groupthink that led to the launch of the Challenger. And what was worse still, the groupthink that led to the person who identified and said, "We shouldn't launch," not only being discounted, not only being ignored, but actually, effectively ending his career by suggesting that perhaps it wasn't a good idea to launch tomorrow.

So part of what we have talked about in the rules and the protocols is to ensure that we do have a culture that encourages the challenges. Encourages the identification of risk and then puts in place processes for escalating, for triggers, for action and for decisions, and that's work that we'll be moving to in our next phase.

The second one is the external events, which is somehow trying to identify, whether it's scenario planning, whether it's through war-

gaming, the external events that could arise; the external events that could prevent us from achieving our goals.

For example, again, we can't control the likelihood… We have a volcano in New Zealand, in the middle of the North Island called Mount Tongariro. It erupted 1886 with significant loss of life. I have seen some geo-technical reports based around some planning, some town planning in the region of that volcano. The main period between eruptions is 3,000 years. The error around that is 2,900 years. [laughter]

We are already within the window of a new eruption, which is why I say we have no means of controlling the probability. All we can do is try to identify and address the impact. Again, this is one where it's very easy to say that somebody's dreaming, somebody's thinking outside the square, somebody's speaking irrelevantly.

The challenge I would put to you, the challenge somebody put to me once very early in my days was, in terms of news that I didn't like to hear, if you think back, when did you actually learn something new from somebody who agreed with you? Risk management is about being prepared to listen to people who have messages that we don't want to hear.

Then the third component to this model, and these will fit together and we'll show you how, are those strategic risks. Now, it's a slightly different approach here because first up, we are about to make a decision, we are about to do something, we're about to take a decision in analyzing and before we make the decision to go we look at the

options and we look at the potential impact if those risks were to crystalize – the threat, the risk and the acceptability of them.

The Board will then typically make a go or no-go decision. Now, for example, you might take a strategic decision based on no market research at all, that the market might actually appreciate something like that; a tablet computer, five years ago. Now, why would we do that?

If you actually did your market research you'd go back about ten years and find that when they were launched about ten or twelve years ago, they fell flat on their face. Therefore, that would prove that the market didn't need them. So it's a brave decision to go and launch a tablet computer, because we know that people don't want them.

So what you might chose to do in you go, no-go decision is pilot that. You might to and launch this new strategy in a market where nobody is going to notice. For example you might launch tablets in a country like New Zealand. If it falls flat on its fact, 99.5% of the world's population won't know.

You test it, go or no-go. You pilot it and then you assess the results of that pilot. You come back to go or no-go for the main rollout. In reality, you can't always go that. If you want to launch IDNs, if you want to launch new top-level Domains, you probably don't have the ability, you have to make a strategic decision, what are we going to do? Have we looked at the options? Have we looked at the potential risks, the impact, the probability and the impacts of those risks? Do we have mitigations?

Close your eyes, take a deep breath and make a decision to go. You implement and you then monitor what happens as a result and then what you see when we put the entire model together, the residual risks that come from there flow back into one of the other two categories above, of controllable or external risk.

So what you see is that this model that we've put together shows the differences in how one manages the three brands of risk; the controllable, the external or the strategic. However, it's still quite – as someone will suggest, as someone will say – it's still quite a generic model.

For those who've read Kaplan, for those that have seen current risk thinking, it builds on the models proposed there. It's taken it quite an extent further but it is still at a generic level in that it doesn't reflect either the uniqueness of either the DNS or of ICANN itself.

What I'd like to do now is to pause for a moment for any questions, for anybody to take a breath, for anybody to stand up and stretch their legs should they choose to – and then I will hand over to my colleague Colin to take us on the next part of that journey.

CHAIR: Questions or comments please?

JULIE HAMMER: Julie Hammer for the transcript. Just a question, and I recognize that this might be something that's covered in more detail later – but sometimes the category of whether a risk might be controllable or the

uncontrollable risk as an external event, is not really as black and white as we would hope.

Is there a series of questions or characteristics that we can look to, to try and get a better grip on that categorization?

COLIN JACKSON: Julie, thank you. That's actually a very, very important point. It goes back to my point that process is not a substitute for though, that even within this framework, as we get further into it you will see that the boundaries that we draw, in not just this dimension but the other dimension, are actually quite fuzzy boundaries and which category something fits in is less important than the fact that we've identified it. Thank you.

WARREN KUMARI: Warren Kumari, Google. Maybe this is also covered later, but one of the things you can do with risk is transfer it. How do we make sure that the people that we're transferring the risk to are actually willing to accept it? For example, I can decide that it's perfectly acceptable to transfer my risk by dumping pollution in another country. It's not necessarily my place to make that decision; it's them who have to accept it.

COLIN JACKSON: Thank you Warren, that's what my dear economist friends would call an externality, which is effectively shifting your costs onto somebody else under another name. I would… I think in the context we have here, that is what the Multi-Stakeholder environment is all about.

And using a process such as we're proposing here would at least surface those assumptions, those transfers potentially that are taking place, so that people in this community can look at it and say, "Actually, is that what we intended? Is this reasonable?" so there's no amount of accountability in the whole model here I think.

WARREN KUMARI: So… Sorry, one quick follow-up. That only works if the stakeholders are actually represented fully. If the stakeholders are actually involved and are properly represented.

COLIN JACKSON: While I agree, there are however quite a lot of people who come to these things and that's really perhaps a matter for the Board of ICANN to consider, on how it reaches out to the broader corpus of Internet users.

CHAIR: Dennis, please?

DENNIS JENNINGS: Will you be following up later with some analysis of strategic decisions that the ICANN Board has taken in the past, to see whether there are…? Whether the risks were adequately identified and transferred? I ask with a certain bias because of my interest in IDNs.

COLIN JACKSON: I think I might duck this one and hand it to the Chair of the Working Group. [laughter] I can tell you that it's not within our Terms of Reference at the moment Dennis. All right. I'll continue now. Hopefully you can see that there are actually circles on this diagram; it's fairly faint.

But what I want to introduce here is that Richard has shown you… Described a framework involving, effectively one dimension of types of risk. He's categorized them into three types. But we also believe there's another dimension here in terms of categorizing risk. And this is something that relates much more to ICANN's particular role in the world, and on the Internet.

We have shown ICANN in the center here – by the way, I want to add, this is not an earth-centric universe as such, I don't particularly wish to be anatomized for having moved the sun to the center, this is simply that that is a matter of convenience for showing it from ICANN's perspective – but if we take the central circle here, these are things that are directly under ICANN's control.

A good example would be L-Root operations. There's little doubt that ICANN has a very strong measure of control over that and if for instance Joe were to go to the Board with a proposal to apply vast amounts of funding to a new platform than the Board would, at its sole discretion, effectively make a decision on what to do about that. That's fine.

Then you get a wider ring that I've described as ICANN community – thank you, thank you Richard –, and that is largely the sort of people that are represented at these meetings; the people who operate key

pieces of DNS infrastructure, the people who really care about this stuff and do have some measure of understanding about what's going on in it.

And ICANN largely operates to seek consensus among such people as part of the bottom-up model, and that's entirely appropriate and that's going on in this room right now and has been going on in this meeting and has been going on in all the 46 meetings before it.

And then there is a wider ring still, which I've described as wider Internet community, of people who maybe have never even heard of ICANN but nevertheless have stakes in the Internet. Maybe they run large corporate systems, their own name servers, they certainly expert the Internet to work, maybe their ISPs.

And to them the best ICANN can do in terms of influence is to communicate, whether it's through this community or directly. So I can seek to influence them if necessary, but it's fairly diffuse. There is certainly no element of direct control.

So the purpose of this further division, really, is to divide the risk space we are looking at into things that ICANN has direct influence over, things where it needs to seek consensus through a meeting like this, or where the best it can do is communicate, run adverts if necessary, persuade people around this table to talk to all their stakeholders and to try to affect change in that way.

Okay. Now, back to the diagram that Richard showed you earlier… Excuse me… These three horizontal slices represent the risk types that

Richard introduced; as we know, the controllable ones, the external ones and the strategic ones.

But we want to reflect the… We need to modify these to reflect the extent of concern and influence in each of the other rings in the diagram I just showed you. Thank you. So I'm going to show you three diagrams that look a bit like this.

The legend up in the top-left does not change, and what that does is show you that the blue boxes with the pointy corners are things that it is proposed that ICANN can manage internally from its own resources and the orange boxes with the rounded corners are things where we consider that the community needs to be involved and quite possibly drive.

However, the identity of the boxes is pretty much the same in all cases, and I'm going to work through them because they're actually fairly difficult to read up on the screen and I have the advantage of having a copy on the laptop right in front of me so I can read it here.

The first layer of this, the first slice on this diagram is showing you how we would do risk management on something that is a controllable risk; that is wholly within ICANN's domain. And this is absolutely classic risk management, that… To use a buzz=phrase it's risk management 101, it's quite simple, we're proposing an ISO model on this but honestly, and of them would work, and you've got the classic thing:

Where once you have assessed risks you go to a set of options, you design a mitigation, which is what that second box says, and that mitigation may be technical, in which case you implement it and monitor

its effect. It may be operational, in which case you set up a set of rules and you monitor compliance on that, and remember for this example we're saying this is wholly within ICANN's purview.

And then you reassess – you're monitoring this – you reassess and you look back around and consider, do I have a residual risk that I'm still unhappy with? And if so, you feed it back in and add more mitigations. As I said, this is classic, there's nothing unusual here.

The second slice on this one shows how it might operate within something that affects it, that was within the ICANN community's control as opposed to ICANN's control – so we've suggested that and the community itself, probably a Working Group from the community, would be involved in developing options for managing this controllable risk that I'm just hypothesizing.

And the community would be involved in designing mitigations and if it's a technical mitigation then implementing that, and we would see ICANN monitoring that effect, and it would be an ICANN Staff job in our view, they're to monitor the impact of that mitigation and check whether it was adequate or not.

And then a community body again would reassess that and whether the risk needed further mitigation. Also, if it was an operational mitigation rather than a technical one, then ICANN can't require compliance of course but it can set up a set of protocols and warmly encourage the community to adopt those.

And the community itself would, we imagine, assess compliance against protocols and again, ICANN can monitor the adherence from that so that

the community can asses whether or not the mitigation is working and whether or not the risk is adequately controlled.

When I look at the third slice, the lowest slice in this diagram, this is for once things that affect the wider Internet community. Now, this one, again, is much the same as the ICANN community one above, with the exception that if it is an operational matter, where you need to get a lot of people to do a lot of things, you cant really set a protocol.

The best you can do is communicate – that's what I discussed earlier when I was describing the rings of the diagram. ICANN and the ICANN community would in this case do their best to make people in the wider Internet community aware of the issues of what needed to be done.

An example of this might be, who remembers the open relay? Wasn't it a great idea that mail servers all just openly moved stuff around? Isn't that cool? Unfortunately we discovered it wasn't and it became quite a massive exercise to persuade people who operated mail servers to switch off open relay.

Can we move onto the next slide please? Now, this is the second risk category. The external events – the San Andreas letting go, etc. Again, I'm going to address these in the three different slices. For the ICANN only ones, remember this is not something you can affect the probability of. You can't mitigate the likelihood, you can't reduce the likelihood of these events. All you can do is defend.

So you're building a wall in a sense. You're defending probably in depth against something that may happen and you can't prevent it. And if it's within ICANN's purview again, as Joe will tell you, he's distributed our

root across… How many countries? A lot? Yeah, it's not all sitting in California anyway. Exactly.

You have a lot of options and you develop options within ICANN of what you're going to do about it. You prioritize those. You defend, effectively, you execute some or all of those options and you monitor and you consider, have I sufficiently mitigated my risk against these events? And you reassess and it gets fed back around to the assessment box to say, is this sufficient or do we need to do more?

And again, that is relatively straightforward because it's always under control of the one organization and the Board can just require this to be done and is perfectly capable of having Staff check that that has been done, as indeed it should.

Within the ICANN community – again, this is a wider issue and it's certainly not something that ICANN can attempt to do entirely under it's own bat, but ICANN would convene a Working Group composed of community people to assess the potential for external events to disrupt the DNS. Again, that group would prioritize options for defense and come up with and implement those defenses.

ICANN can monitor that itself but again it is up to the group to reassess whether sufficient defense has been done and whether more needs to be done. If it is an issue affecting the wider Internet community or controlled by the wider Internet community, we have the same as last time really, in that that whole [leaders? 00:46:25] forgetting action in the wider community are less than in the ICANN community or within

ICANN as a whole, and we have to communicate – again, it's not quite fair to recycle my example of open relay, but it's a bit like that.

We would have to go back and start persuading people around the world in some way or another to change what they were doing, maybe to upgrade some software – and you see that happening quite often when vulnerabilities are discovered – to defend against some particular attack or some problem that we don't know about when it's going to occur.

Let's move on please. This final one is about the strategic risks. And remember, these are what some people might call a calculated risk – although I often question how calculated they really are. We have decided we are going to go and do something. We know it's risky but we believe there's a potentially good outcome so we're going to do it anyway.

And again, once it's within ICANN's purview, if that's the top slice, that is effectively a Board decision and the Board can decide whether to do something. The Board may well try to pilot or cause ICANN to pilot what it wants to do, if that's at all possible, and assess the outcome of that, and also then we'll move to implementation and monitoring.

That's fairly straightforward. Within the ICANN… If this is something that is within the control of the ICANN community, as opposed to ICANN itself, maybe it's something in an innovation in the root say, which clearly isn't wholly under ICANN's control, then the Board may decide that it wishes to go ahead but of course it doesn't have the power to do that wholly by itself.

The community would need to consider how this would best be piloted, or even if piloting was possible, on how to assess that pilot, and again the Board would get another slice out of the decision if that had happened – and implementation again would be a community matter, but it's very reasonable to expect that ICANN would monitor the progress of that risk.

And the arrows leading on from this one, on this slide, lead back up to… Because once you've taken your strategic decision, these risks then become a controllable or an external event type risk and become assessed in that fashion. And I also want to just discuss briefly the final slice, which is the wider Internet community.

To be honest there's not a lot of difference between this one in this case and the ICANN community. The Board may decide to do something, people around the wider Internet will potentially pilot things and they'll potentially implement things if it's given to them.

But ICANN will need to monitor that and feed back into, was this what we expected? Are we in a risky situation here? Do we have to feed back into one of the classic risk management methodology, such as the one we started with? Thank you.

So going back to the circular slide now; it's called, "Grandiosely – the taxonomy of risk." I'll just walk briefly across the different parts of this, just to give you and idea of the sort of things we're talking about here. Again, within the controllable risk segment, things that might affect the wider Internet community, technical attacks, hacking in the vernacular – although I dislike the use of the term in a pejorative fashion.

These are things that do happen out there, the defense against them is usually under the control of the wider community – although of course if can affect ICANN, it can affect the community members, but it can also affect just about everybody on the Internet.

Another risk that is perhaps within the ICANN community is say a weakness in DNS software, and of course we try to mitigate that by running multiple platforms and so forth, but the possibilities exist out there that protocol vulnerabilities are found and so forth.

And then there's DDoS, which I've drawn as actually between the two rings of ICANN control, because all of it could clearly be affected and other aspects of the zone distribution mechanisms, and the roots in general. I should also note here that the aligns on this diagram, these circles, are deliberately fairly faint.

There was a comment earlier, from Julie, I think saying that sometimes it's a little fuzzy, which categories things live in. That's always going to be the case. I'll go back to saying processes is not a substitute for thought. [coughs] In the external events section, there are quite a number of risks – and again, I've just thrown out examples here.

We've seen, in the history we've seen various attempts to split the root, attempts to start alternative roots, there's always a risk that say… Within a [policy? 00:51:57] for instance, somebody might try to set up their own alternative root. I think most of us think that that might be damaging to the Internet. However, that's an external event and it's fairly difficult to actually manage the probability of it.

Another one would be very much something that affects the community is if some new, disruptive technology were to occur that meant we actually don't need the DNS anymore. I can't think what that might be, but I suspect there are people right now who are plotting.

Oh, Warren, Warren, yes. [laughter] I don't need to know about Google's business plans, thank you. But also… And then I've drawn governance change or potentially something like that for something that would be directly under ICANN's control as an external event.

Then in the strategic region section I wasn't able, off the top of my head, to come up with something in the central ring in the ICANN box. Some strategic risk where the Board has direct influence but it's all under the Board's control.

I suppose if the Board decided to go and try and run [Al rugon? 00:53:09] and Amiga or something, that would be perhaps a very brave decision, but moving away from a slightly fanciful one like that, we would have IDNs for instance as very much an ICANN community issue, where that is under the control of the community, where ICANN is playing a strong part in leading consensus on it, or trying to develop consensus on it.

There were huge technical issues, no doubt, and ICANN is bringing those people together and trying to assess the extent to which those surveys are being risk managed. Again, the framework we're proposing here could be used for that, and would hope it will be. And then gTLDs I've put into the wider Internet community ring because they do have…

The control of them does to some extend flow right out into the wide community and people were expected to apply for these things, people were expected to use these things and, as various discussions in this meeting have described, various people out on the Internet may need to modify their behavior in an environment of New gTLDs.

Again, I have to say, these are just examples. There are designed to make it easier to think about how we categorize risk and therefore which arms of those decision trees that I've shown you earlier, get used.

RICHARD WESTLAKE: So ladies and gentlemen, that brings you up-to-date with where we are in terms of developing the framework itself. We now have a process of work to go from here. Today is about seeking your feedback on this framework… Patrick?

PATRICK FÄLSTROM/JONES[?]: We have a question in the chat from [Rick Weller? 00:55:00]. It says: "Does the framework consider risk as strictly threats or negative events versus opportunities, which, if they occur, would be positive?

RICHARD WESTLAKE: We've always taken that risk can be positive or negative. The hardest bit is to look at the negatives because we typically try to resist those so our focus is on the negatives, but very much the same principle, the same process applies to identifying opportunity as well. The reason we tend to go for the negative is that it is so much harder, and if you can do that, people will welcome the same process to think for the positives.

COLIN JACKSON: And if I can just add as a comment to that, we're strange creatures we humans. The same person who goes out and ensures their house will also buy lottery tickets, because we're looking for upside risk.

RICHARD WESTLAKE: Patrick, any more questions you wanted to… Or any other questions you wanted to ask?

PATRICK FÄLSTROM/JONES[?]: Just a note – the slides that we have online are not the slides that you've presented.

RICHARD WESTLAKE: That's correct. What we have done is a slight update to those slides. The ones you had online came in about two to three weeks ago. Before we arrived we got an initial round of some feedback comments, which did lead to a slight updating – so I apologize, I didn't make that clear at the start.

So we brought a slightly substituted version because we certainly did get a few comments through and thought it was quite important to incorporate those rather than to go through that process again. And I assume that ICANN will update the copy online. Thank you Patrick.

So now, as I say, we are seeking your feedback from the proposed risk management framework, and I'm hoping also that we'll be able to use much of the next hour or so in the DSSA Working Groups workshop, for exactly that part of it. And then from here we then go back and start

working in, how does this apply in practice? How do we set processes for developing risk triggers?

The escalation processes, to make sure that you never get to the point of a major risk happening. Someone said, "I never knew it was going to happen," and someone further down the organization says, "Oh, we knew all along." And how often do you hear that happening?

PATRICK JONES: There was an earlier comment in the chat that the third sphere cannot be reduced to ICANN communicates that there are a lot of uncontrollable, potentially lethal risks out there from the most technical and the most political.

ICANN does not only communicate, ICANN must attack, manage, and react. It all goes into contingency planning instead of the more normal cycle with lots of proactive action. So that was a comment from the chat.

RICHARD WESTLAKE: Yes, and I don't think we would dispute that at all. We absolutely say that you have to do more than communicate because from ICANN's perspective it actually has to say what is the risk to ICANN, to the stable operation of the DNS, what can we do about it? Within ICANN's control, ICANN can decide to do something.

Within the community it can seek community cooperation, collaboration, consensus, but there is still probably, when you have that

type of risk eventuate the need to get out and communicate. You may well be operating in all three… Dare I say orbits, simultaneously?

Then, having had the feedback, having worked through this, we will be revising any aspects necessary. We will be testing, as we have to a degree already, some of the example risks identified by the DSSA Working Group, and part of the job, before we can in fact put in a proper full set of recommendations, is to in fact gain an initial understanding of what is the current status, what is the current readiness state, within ICANN itself, of Staff preparedness.

Because to convert this from theory to policy and practice within ICANN, what Staff structures, what lines do you need, and again, one of my major backgrounds has been risk within the banking background. As you know, they have been exposed to some quite significant risks over the last four or five years in particular, many of which we've had people down the organization say, "We knew all along."

It hasn't saved chairmen of chief executives or people at that level, who said, "We didn't know it." And one of the major issues there has been not only the setting up or the requirement for a separate risk committees, which I'm delighted that ICANN has already done; a separate risk committee – so that risk isn't just seen as a compliance function but is seen as a strategic, forward-looking outwardly focused topic, which as I say, it is absolutely.

It is part of… I'm quite happy to see a strategy and risk committee, which does tend to bring the two together quite neatly. And the other thing that the banking world is requiring now is a C-Level Risk Officer. A

Chief Risk Officer within the organization, who isn't liable to be captured by the line.

The danger, if you have risk embedded anywhere through the line process in an organization, is that you almost end up inevitably with contrary motivations where you in fact have an incentive to go with the line, to go with the strategy, rather than to say what could go wrong – hold on a minute, we need to assess a risk.

So one of the recommendations within the banking world – whether it's applicable here, we still reserve judgment – but one of the recommendations in the banking world is that every major bank should have a Chief Risk Officer who has an independent line straight to the Chief Executive and straight to the Board's Risk Committee.

Ladies and gentlemen, from that we will then be presenting our final report and framework for the Durban meeting, and of course it will be in draft form and ready in approximately, we hope, one month ahead of the Durban meeting. Thank you. I'm happy to take any further questions before we take a break and then move into further feedback. Thank you.

CHAIR: Good, thank you Richard. So the DSSA Group have agreed to donate about an hour of their time to continue this discussion, if any of you are able to stay with us, which I hope will happen. We can do a few questions now, then I do think we need to take a brief break to reset and… Hmm? Yeah, just some logistical matters that need to be taken care of. So let's have a couple of questions and then we can reset.

WARREN KUMARI: Warren Kumari, Google. So I think this is really, really useful work. But something that concerns me slightly is looking around the room I see many of the usual suspects. I think it would be very useful, especially the discussion of the risk framework and how you evaluate some of this, if it could be somehow gotten in front of a larger audience.

This self-selects for people who have an interest in risk and managing it. How do we get this message to the wider community?

RICHARD WESTLAKE: So do I. How? I guess all I can say really is that this is a matter for ICANN and the ICANN Board to push this out wider. We can demonstrate the model, we can show you how to execute it and we can assist Staff with that. But there will have to be buy-in at a fairly significant level in ICANN and the ICANN community – it's not solely ICANN the corporate problem. That's my comment.

CHAIR: Thanks. Yes please?

CHRIS CHAPLOW: Chris Chaplow from the Business Constituency. I'm not a usual suspect but was just happily sitting next to Richard on the bus to the gala yesterday and I'm glad I did. Thank you.

CHAIR: Julie please?

JULIE HAMMER: Julie Hammer. I have a few thoughts myself on how I see the work that the DSSA Working Group has been doing. Actually, meshing with this, but I'd be interested in Richard and Colin's view on where you see the focus of that group sitting within this context.

RICHARD WESTLAKE: Julie, thank you. As I say, one of the absolutely key parts of the process from here, to make sure that we are on something like the right track, is actually to take the work that the DSSA Working Group has done – right now. It has identified some risks, it's developed a very thorough process for assessing, monitoring, mitigating, managing those risks.

We want to test those against our framework. Cheryl? So that's very much the next part of the work. And as I said, our aim is to adopt and adapt, not to reinvent. So thank you.

CHAIR: Thank you. Jacques for the last question before we break.

JACQUES LATOUR: So this is about developing a framework, right? And developing a framework is different than implementing a framework. So does this cover implementation of the framework within ICANN, or…?

RICHARD WESTLAKE: Let's say that this project takes us to the point where the framework can be built. We will provide the architect… We've done the framework, developed the framework, now it's making it into a design for the structure and a design for the model and how it will be implemented, and then there is a phase, which is actually working with ICANN to implement; to make sure it goes in.

And as with all these good processes, not only make sure it goes in, but then to monitor and test it.

CHAIR: Thank you, yes. This is foreseen as being a multi-faceted project. We wanted to get the framework in place and then assess where to go from there. Dennis, I missed you as well. We'll get you in just before the break.

DENNIS JENNINGS: Thank you very much indeed. Dennis Jennings for the record. Observing the banking crisis, it seems to me that conflicting strategic priorities is one of the endemic causes of major risk. In Ireland a particular bank decided it had to compete in the mortgage lending market and it went in three years to be the leading lender and therefore completely destroyed its business.

But that was because it took the strategic priority that it needed to compete in this high value, high return business. And that trumped the risks. Does this framework adequately address the groupthink that will arise from competing strategic priorities…? That may arise?

RICHARD WESTLAKE: We believe that it can. I won't go further than that Dennis, [laughs] because so much of it depends on exactly what I was telling you at the start: can we get a firm, well-ingrained risk culture through the organization? Do we have a Chief Executive who doesn't sit there and… I mean, it won't happen in ICANN, but certainly one of the major Australian banks had for years and years and years of:

"I want 5% quarter on quarter growth on earnings. I don't care how you get there, guess what? When we don't get there we fudge the numbers. Once we've started to fudge the numbers once we have to compound the fudging of the numbers and we all end up in jail."

So, no. It does come down to the culture, the acceptance of the fact that we have to have that culture imbued. And it doesn't happen overnight either.

CHAIR: Good, thank you. And with that we'll take a five-minute break so the room can be reset for the DSSA group. Thank you all very much for your interest. It's great to see so many people here. I hope many of you can stay.

UF: Bravo. [applause]

[END OF TRANSCRIPT]