Navigating Governance, Risk and Compliance Challenges to Drive Business Excellence

Top row (from left to right): Gautam Bhasin, Sales Director, Financial Services, **HCL Technologies**; Joe Cunningham, Global Head of Technology, Strategy & Innovation, **Visa**; Winston Chew, Global Head of Application Security, **Barclays**; Frankie Phua, Executive Director & Head Credit & Country Risk Management Division, **UOB**; Thomas Kok, Head of Technology Risk Management, **DBS Bank**; Sam O'Brien, Senior Archer eGRC Specialist, **RSA**; Solomon Tay, Head Information Technology, **CIMB**. Bottom row (from left to right): Alex Yan, Executive, Group Audit, **CLSA**; Chong Seow Peng, Regional Head of Risk & Control, **DBS Bank**; Sandeep Malhotra, Head of Emerging Payments Platforms, Asia Pacific, Middle East & Africa, **MasterCard**; Rimin Dutt, Senior Editor – Asia Pacific, **FST Media**; Luke Rankin, Head of IT, Singapore, **ANZ Bank**; Kevin Austin, Head of Assurance APAC and India, **RBS**; Gopal Rao Ippili, Senior Manager, Governance, Risk & Compliance Practice, Financial Services, **HCL Technologies**.

FST Media, HCL Technologies and RSA hosted an exclusive roundtable with a select group of senior financial services representatives to discuss governance, risk and compliance issues currently affecting the industry in Singapore. Attendees discussed the technologies, frameworks and processes they use to seize opportunities and mitigate challenges in achieving compliance.

SAM O'BRIEN, RSA: I focus on RSA's governance, risk and compliance technology. As an organisation, we help customers deal with different GRC challenges. We gave a presentation this morning that was focused around Technology Risk Management (TRM), which is obviously something that is very topical for customers in Singapore at the moment. There is a lot of change, a lot of upheaval that has been driven out of that. The companies present, around the table, are not just operating in Singapore. We are operating across the broader Asia Pacific region and even across the globe. So it is not just TRM that we are dealing with on a day-to-day basis, there are a lot of other regulations that really come in to play.

There are also the privacy changes that are occurring everywhere. We have the privacy priorities and principles in Australia at the moment and there is obviously the Personal Data Protection

FST Media
Financial Services Technology Media
where the market meets

RSA®

HCL

"The four hours maximum unscheduled downtime is something that many of us have debated. If you split four hours by 12 months, we are talking about 20 minutes downtime per month."
– Thomas Kok, DBS Bank

"I recruit a lot of IT people. I want to have a lot of people with IT skills in credit risk management because we have to leverage technology to comply with a lot of these regulations."
– Frankie Phua, UOB

Act (PDPA) in Singapore as well. So there are a lot of buzzwords to throw around.

When it comes to dealing with some of these changes, there are essentially two schools of thought. There are the people who just want to get the minimum amount done to comply and that is completely fine, but then the question is how do you do things more efficiently? There are others who are using some of these changes as a way to drive initiative, to drive innovation and to drive extensions of the technology capabilities in organisations, off the back of some of the mandates that are coming through. Easier said than done, but it is happening.

One of the challenges that I have spoken about a lot is the concept of dealing with multiple regulations at once. When we are working in a cross-border fashion, a concept of control harmonisation becomes very important. GRC can be really broad, but it can be broken down into a number of different challenges that people have to address. That is really where the first steps come into play, and as a result it is very important to have a strategy to drive that through.

What we are seeing at RSA around the region are things like business continuity and disaster recovery, regulatory change management and security operations and security risk management. They are probably the high-priority topics that we speak to customers about every day of the week.

RIMIN DUTT, FST MEDIA: Thank you, Sam. Thomas, what is the greatest challenge that the evolving Singapore regulatory landscape poses to your organisation?

THOMAS KOK, DBS BANK: I see complying with the Monetary Authority of Singapore (MAS) TRM notice as a challenge for the industry, as it is legally binding. In particular, the four hours maximum unscheduled downtime is something that many of us have debated. If you split four hours by 12 months, we are talking about 20 minutes downtime per month.

Sometimes your critical applications can go down for as long as two hours, so you effectively have lost 50 per cent of your quota for these applications. If you have an issue that impacts multiple applications, do you measure that as a breach on each critical application? How much do you have to pay for those breaches?

SAM O'BRIEN, RSA: Has there been any guidance from the regulator, or has there been any advice provided on how that actually gets calculated?

THOMAS KOK, DBS BANK: I will be discussing these regulations with MAS shortly. They are keen to understand how we, as an industry, are moving forward in complying with these notices.

FRANKIE PHUA, UOB: I am from credit risk management at UOB. To address the challenges, I recruit a lot of IT people. I want to have a lot of people with IT skills in credit risk management because we have to leverage technology to comply with a lot of these regulations. UOB is a very IT-orientated team. We have people who know programming, who are able to understand system audits very well because when we build capability to cope with the regulatory changes, we need people who are IT-savvy. You will see more IT people working in risk management, simply because we need IT to help.

WINSTON CHEW, BARCLAYS: The four hours that Thomas touched upon is a challenge. The fact that we will only have one hour to notify MAS is the other challenge we need to be concerned about, because technology risk traditionally has not been a 24 hours a day, seven days a week function. Having to inform MAS in the middle of the night on a Sunday, while you are home with your family, is going to be challenging. But it is not just the TRM, it is also the rest of the regulatory requirements.

There is a lot of talk around about GRC changes in technology. Traditionally we have been isolated from many of these issues because technology risk is an IT problem, not a regulatory one. It is nothing to do with financial risk, credit risk, market risk, which have very mature models for costing and the like integrated together to qualify their risk position. We are seeing a trend where we are going to have to integrate risk, and technology risk is going to become part of that whole organisation risk. I have not seen that yet in the seven banks I have worked in.

SAM O'BRIEN, RSA: We are seeing that concept of bottom-up risk aggregation enabling the ability to take very technical issues and roll them up either through a business hierarchy or even a risk hierarchy. A missing patch on a server means absolutely nothing to a business manager, but if it has an availability risk for a key system of some kind, then that may be something that needs to be flagged with them as a red light on a dashboard. If it gets serious enough, or if there are enough of them, senior business stakeholders are going to become engaged in that risk management process and that links in with what the TRM guidelines look to achieve.

RIMIN DUTT, FST MEDIA: Luke, what are your views on the changing regulatory landscape and how are you responding to them?

LUKE RANKIN, ANZ BANK: A significant share of investment over the past three years has been on delivery of compliance related projects. There is a cascading effect now, as our regulators adopt similar principles. Overall, a strategic approach

to addressing these challenges is required, as it is likely that these standards will become a reality in many of the markets we operate in. The challenge of sustaining compliance also requires that relevant practices are embedded in our operational processes.

RIMIN DUTT, FST MEDIA: Let us move from the topic of challenges and talk about opportunities. What practices have you implemented within your organisations in order to see regulatory change as a business opportunity, and not necessarily as a challenge?

JOE CUNNINGHAM, VISA: I am tangentially engaged on the risk side in terms of what Visa's technology is capable of enabling and the types of capabilities we need to have today in order to support our business, in order to support our clients as they respond to these types of changes in the environment. However, from what I am hearing around the table, I would be concerned about the lack of precision. For the lines of business we are in, which demand incredible precision from an execution point of view, there seems to be a lot of ambiguity around some of the rules and around the interpretation of some of those rules, around the adequateness of how those rules are implemented and accounted for. It is a little concerning. We should be having conversations as an industry around those things.

Visa has a different perspective than many of the retail banks represented around this table, but from a pure technology risk point of view, which is probably the element of the holistic risk spectrum that I see more closely, it is something that has been and will continue to be at the forefront of our technology strategy.

It is a differentiator. It is something our clients absolutely demand and it is something that sits at the core of our brand. Security, reliability and trust are absolutely core to the Visa brand, and we feel staying on the front foot of security and working with our partners in the ecosystem is critically important. How we manage the reliability of the network is critically important, because you will not be able to meet your responsibilities if we do not meet ours.

KEVIN AUSTIN, ROYAL BANK OF SCOTLAND: I would like to pick up that point and echo the concern that it seems a little bit loose, especially as far as Singapore guidelines on things like Threat and Vulnerability Risk Assessment (TVRA). I have struggled with it and I have seen my team struggle with it for the past six months. In regard to data centres, what kind of threat is adequate to incorporate in the TVRA? Is it a grenade attack? Someone burning down the building? Is it a bomb? Is it earthquakes? If I ask three different people this question I get four different answers. No one is quite clear on what the proper approach is.

I have tried to get the asset registry correct, getting the business process aligned to the asset register. If I have that, I have a framework within my group policy set, or within the International Organisation for Standardisation (ISO) standards, or within the Payment Card Industry Data Security Standard (PCIDSS), that I can apply to that part of the registry. Then I can do my control checking. The first risk assessment you do is tough, because you do not have any pre-existing data sets. You have various bits of information from all the lines of defence doing operational processes, but to gather it and give it one concise overview, particularly for integral outsourced relationships as well as third-party relationships, is a problem. We have to remember however, that it is an annual requirement and the more times you do it, the easier it will become.

The idea is to build your asset register, get that correct in the first instance, and then you can apply security controls and deal with shifts. There will always be change, but if you can get your asset register correct, get the business to buy into updating it, and have an easy way to update it, then from a governance standpoint it will make your job much easier.

LUKE RANKIN, ANZ BANK: The framework ANZ has developed in response to the MAS requirement for identification of critical systems has focused on systems supporting channels servicing customers across the business. This includes identification of systems that underpin servicing via those channels and their criticality taking into consideration business continuity.

RIMIN DUTT, FST MEDIA: Would anyone else from an international bank like to highlight how their organisation handles regulatory change in Singapore?

SOLOMON TAY, CIMB: CIMB Bank is headquartered in Malaysia, and Singapore is a branch setup. We are regulated by both MAS and Bank Negara. A number of our major systems are insourced to headquarters in Malaysia today and they still have to come under the purview of the MAS TRM guidelines. There is no excuse, we actually have to tackle these requirements sooner or later.

RIMIN DUTT, FST MEDIA: Siow Peng, do you agree with the challenges we have discussed so far? Are you seeing anything different?

CHONG SIOW PENG, DBS BANK: I am neither from technology nor from business continuity management, but I am responsible for the operational risk aspect for my functional unit.

"A strategic approach to addressing these challenges is required, as it is likely that these standards will become a reality in many of the markets we operate in."
– Luke Rankin, ANZ Bank

"There will always be change, but if you can get your asset register correct, get the business to buy into updating it, and have an easy way to update it, then from a governance standpoint it will make your job much easier."
– Kevin Austin, Royal Bank of Scotland

"We are always watching the news, when we see a bank was fined we question what they were missing to ensure we are compliant. This is more of a reactive process, rather than proactive."
– Alex Yan, CLSA

"By not considering the consumer experience while issuing mandates, you are not reaching the masses."
– Sandeep Malhotra, MasterCard

Realising and understanding all the group functions and regulators' requirements is the biggest challenge because we need to operationalise our procedures to meet everybody's requirements at the same time. As such, the operational procedures and controls are always evolving.

RIMIN DUTT, FST MEDIA: What policies or actions have you implemented to deal with the data and the privacy aspect of the regulation?

CHONG SIOW PENG, DBS BANK: The forthcoming challenge for DBS is the Personal Data Protection Act (PDPA) that is coming live for the Do Not Call in January followed by full implementation in July. At the same time we also have the new US tax regulation, Foreign Account Tax Compliance Act (FATCA). These two new regulations require all technology and operations teams in the business units to have regular discussions on how to be compliant. As these are new regulations are quite unclear, the interpretation is often subjected to advice from professional consultants. Based on the interpretation, you have to enhance the technology and change the underlying processes to make sure it works. That is the biggest challenge because every time we run a workshop, we discover new things.

ALEX YAN, CLSA: I am from audit, so thankfully I am not responsible for implementing the changes. The problem is that we keep having all these new guidelines that are refreshed every two, three years and then people have to read them, understand them, interpret them and then implement the changes and try to decide how much is sufficient. Do you need an automated system, or are manual controls sufficient?

Obviously you have to take into consideration the complexity and the size of the business but, again, that is very subjective. There are the large banks like DBS, and smaller outfits such as brokerages like CLSA; so to what extent are the controls flexible to different organisations' requirements? A larger organisation will have more resources, but we are all competing for resources. The problem is that regulators are not very explicit. If you ask them, they cannot answer what your organisation needs to do. They tell you the guidelines, but the guidelines are not explicit.

Take, for example, AML transaction monitoring. They say that you need to do AML transaction monitoring, but they never say you need to have an automated system to do so. If there is a manual way of monitoring, is that sufficient? How many reports do you need to monitor it? It is very subjective, and sometimes management just wants to do enough, given the costs involved. Then there is the question of do you wait until something happens, like you are fined, then you do more? We are always watching the news, when we see a bank was fined we question what they were missing to ensure we are compliant. This is more of a reactive process, rather than proactive.

RIMIN DUTT, FST MEDIA: Gopal, what are the top challenges that your clients have faced in the last few months and what challenges do they foresee in the next few months?

GOPAL RAO IPPILI, HCL TECHNOLOGIES: One of the issues that my clients are frustrated with is the duplication of data. We are hearing that the different regulations require a lot of reporting to be churned out, and many of the reports are the same with slight cosmetic changes. Our GRC tool will give us an option that you can map which documents are required, because the back-end database has all the regulatory requirements. You can see if you are generating a particular report for a particular regulator that can be used for the other regulator, and you can save your resource and time and submit the same thing. So this is one feature that can help you to avoid having to duplicate reports.

RIMIN DUTT, FST MEDIA: Sandeep, when technology risk and security departments work together on compliance, how do you determine who leads the venture?

SANDEEP MALHOTRA, MASTERCARD: It will be whoever has the money. We have been talking about a mandate and speculating as to what comes next. We have also been talking about how you interpret the regulations to meet the requirements of the mandate in the timeframe provided. My perspective is slightly different. I ask what this mandate means to the consumer and assess whether it is good for the consumer?

If I implement two-factor authentication on card present transactions, card not present transactions, Internet banking, mobile banking or mobile payments, I ask "is this a secure transaction?" The answer may be "Yes," but then I ask "is the consumer going to use that? Is an average Joe going to do this transaction?" If you make the process too complex for the consumer, the consumer may not use it. As an example, the Reserve Bank of India mandated a two-factor authentication for e-commerce.

Did e-commerce in India grow at the high rates seen in other markets in the region right after the mandate? No. Because an average consumer did not know what a card-based transaction was, and they had to do two-factor authentication and not many people remembered their password, not many people remembered the PIN, not many people knew how to utilise a one-time password (OTP) from an SMS. By not considering the consumer experience while issuing mandates, you are not reaching the masses.

When the regulator comes with a mandate, I assess whether this is just a mandate by itself and if it is going to be good for the economy and good for society. Maybe that is where we have to use our judgment and be a part of that mandate prior to its implementation by saying "we will work together, so before you lead the mandate, let us see if that is going to help everybody, every stakeholder."

Interpretation obviously is complex and everybody interprets differently. So maybe a mandate should come with a supplement or an appendix or an annexure, which basically outlines some basic standards or a framework around how to implement the mandate. Then it is not open to interpretation and maybe that is a standard that will work domestically and regionally. You could do a mandate that works in Singapore, but everybody is becoming international now and doing international payments, international transactions. How would you do that and maintain a consistent payment experience? If I go to a Singapore website, I get a one-time token. If I go to an India website, I enter my password, but if I go to Amazon.com, I do not do anything. Maintaining consistency and a common user experience is going to be the key.

RIMIN DUTT, FST MEDIA: Solomon, who leads compliance in your team?

SOLOMON TAY, CIMB: We actually have a team called Group Governance and Risk Analytics. They liaise with the regulators, so they function as an independent party that examines the internal implementations. This crew of people are champions of the TRM program, to make sure that it meets the regulatory deadlines. Most of the time, if you let IT lead the implementation, the danger is IT will do to the nth degree, and they might miss the deadline. Or they may misinterpret certain parts of the guidelines and thus not comply with the regulations. On the other hand, if you let the business drive the TRM programme, the business will be very cost conscious and go on a minimalist implementation approach.

RIMIN DUTT, FST MEDIA: Within your organisations, how do you get the buy-in from different staff to implement the various technology and frameworks you are trying to put together for GRC? What kind of cultural changes, such as staff inclusion policies, have you implemented in order to get the buy-in on reporting, risk assessment, and so on?

WINSTON CHEW, BARCLAYS: It is not about technology, it is about the people that you need to convince to buy-in, and getting the right process in place. A lot of times, as technology people, we focus too much on technology. We are bringing in these tools for GRC issues, but they have not solved the problems because you did not get the buy-in from the right people to participate and share their information. Different people have different business objectives, trying to achieve different things, and obviously see the situation from different perspectives. If we want to be successful, we cannot think "IT per se" to solve an IT problem. It is about getting the influential people on board.

GAUTAM BHASIN, HCL TECHNOLOGIES: Getting buy-in is probably one of the most difficult components of getting a project started. As we started the GRC implementation process with an investment holding company and a member of the world federation of exchanges about three years back, for us it was about implementing the tool into the organisation. But as we went in we encountered stakeholders who were not brought on board, and we had to do a series of workshops to get a lot of buy-in from stakeholders who had not really sponsored a project. That is one of the learnings we had, and it is one of the things we tend to do now, especially on governance projects.

RIMIN DUTT, FST MEDIA: What security features, or what kind of HR policies, are you putting in place within your organisations to get the technology take off from a GRC perspective?

SAM O'BRIEN, RSA: Buying a piece of technology is not going to solve the problem. Making sure that that technology is going to work with your people and your processes, that is going to solve the problem. Without a process, a tool can only achieve so much. The process has to be there and then the tool will help support that within the organisation; you have to get the cultural aspect right as a first priority.

RIMIN DUTT, FST MEDIA: Assuming compliance is your first priority, what is your second?

SANDEEP MALHOTRA, MASTERCARD: Growing the business. Make more money, because that is the expensive part, right? So now you have to compensate for that.

CHONG SIOW PENG, DBS BANK: After regulatory risk, I think about fraud risk because it is an ongoing challenge and you must remain vigilant to minimise internal and external fraud events. We deal with customers in many ways, whether it is face to face or whether it is through e-channels. So there is a need to have different effective controls in place for different channels. I also need to look into how to prevent and detect fraud for each of these channels.

WINSTON CHEW, BARCLAYS: I am heading up the application security global team for Barclays, so

"We actually have a team called Group Governance and Risk Analytics. They liaise with the regulators, so they function as an independent party that examines the internal implementations."
– Solomon Tay, CIMB

"It is not about technology, it is about the people that you need to convince to buy-in, and getting the right process in place."
– Winston Chew, Barclays

"Organisations operating in isolation are the ones that are exposing themselves to most risk ... together is the only true way you can be best equipped to identify risks and to respond appropriately." *– Joe Cunningham, Visa*

regulatory compliance is actually the second risk to me because the first priority is all the hacking that has been going around. Like the Eurograbber, like the mobile attacks that actually have material financial impact to the bank.

A lot of these are malicious attacks against the bank's website. All the fraudulent fund transfers and the like will be the key because those have immediate material impact. There is a lot of new technology that has been going around and information security is catching up. There are not enough professionals that specialise in that space, and really we are playing a catch up game.

JOE CUNNINGHAM, VISA: We tend not to have separate conversations. We tend to have an enterprise risk function that looks across the board. Whether that is fraud risk, whether it is the ability of our clients to meet their obligations in credit settlement risk, whether it is our own operational risk, whether it is business continuity, whether it is IT disaster recovery, and so on. We have an enterprise risk function that looks at it holistically. We may have more maturity there than some organisations.

From an information security point of view of course that is something that we tend to think slightly differently about, mainly because of the rate in which it is evolving, the types, the scale and the vectors of attacks. Winston made a point about the skill set that organisations need to have. It is certainly evolving, and it is something that is very challenging to stay on top of. The one thing I would add is that organisations operating in isolation are the ones that are exposing themselves to most risk from an information security point of view. Together is the only true way you can be best equipped to identify risks and to respond appropriately. That is something that we have been doing for quite a long time, whether it is with partners in the industry, law enforcement, regulators or the intelligence community. Because of the rate in which the space is changing, assuming that you can operate in isolation is very risky.

RIMIN DUTT, FST MEDIA: The main issues we have discussed today include defining risk, encouraging further collaboration, achieving an enterprise-wide view of risk and complying to multiple sets of regulations within both a region and a global marketplace. Thank you all for joining us. *




FST Media
Financial Services Technology Media
where the market meets

RSA®

HCL

About FST Media

FST Media produces the most successful technology conferences, roundtables and publications for the banking, insurance and wealth management sectors across the Asia Pacific region. FST Media prides its reputation on unparalleled access to senior executives, and the delivery of high-quality information on trends and disruptions in the financial services sector.

The RSA and HCL Business Alliance

HCL tackles security and risk management needs at both the organisation and industry level. Their partnership with RSA allows HCL to offer their clients solutions that are targeted to their specific needs, while leveraging industry expertise. The company produces end-to-end solutions that range from access control and user authentication to security information and event monitoring and data loss prevention to governance, risk and compliance.