

# “An Ongoing Compliance Function Is Part Of The Corporate Culture Of Any Successful Enterprise”

The Editor interviews **Ronald A. Joma**, Senior Manager, Amper, Politziner & Mattia, LLP.

**Editor: Mr. Joma, would you tell our readers something about your professional experience?**

**Joma:** My background is in electrical engineering and computers, where much of my career has been focused on the design and implementation of business computer systems. Over the past dozen years, this has led me into Information Technology (IT) audit, where I have specifically addressed the areas of governance and the oversight of these systems. My experience in deploying systems operationally has greatly helped in the performance of the audit and in providing recommendations for improvement.

The IT, security and governance field has undergone considerable evolution since my undergraduate days at the University of Toronto some 25 years ago. The fledgling research network used for collaboration among academics, government and the military has grown into what today is a major force – perhaps the major force – in the global economy and constitutes an online culture in its own right. This has meant that, increasingly, the safeguarding of information, both financial and personal within the public and private sectors, and the regulation of its use, is at the center of the Internet’s continued development and evolution.

**Editor: Tell me a little about Amper, Politziner & Mattia.**

**Joma:** Amper, Politziner & Mattia is one of the largest regional accounting and consulting firms in the Northeast U.S. and is listed nationally as a Top 25 accounting firm. Amper has offices throughout the New Jersey/New York/Pennsylvania area. Amper is also one of the fastest growing accounting firms in the region.

Our firm’s leadership has taken a very proactive stance in recruiting a powerful team to address the needs of a growing client base in the risk-advisory services area and we are in the process of expanding our security and risk-advisory services offerings.

**Editor: Please tell us about the firm’s Risk-Advisory Services practice.**

**Joma:** Our services portfolio represents the evolution of services surrounding IT audit towards one of helping our clients to address issues that present a risk to their operations, information and infrastructure. Our suite of services includes Security, Continuity, Governance and Compliance. Whereas much of this was traditionally centered around the financial statement audit, we are now taking a much more proactive stance with our clients towards the protection of their facilities, their information and the continuity of their business operations.

Our audit clients look to the Amper team for expertise to help them set up systems of controls that enable them to meet their financial reporting requirements while at the same time helping them realize efficiencies and economies of scale. Put very simply, our clients are in business to sell their goods or provide their services to market; we help them effectively achieve their governance and compliance requirements.

**Editor: Who are your clients?**

**Joma:** We have a large presence in telecommunications, insurance, financial services, and support many mid-sized enterprises across a wide spectrum of industries.

**Editor: What types of issues does your practice address?**

**Joma:** Our clients look to us for our expertise to ensure that their financial controls are operative, that the system reports are accurate and reliable. We help the client’s IT function to deploy controls over their online financial records, assess the security of the systems that manage their business and improve their IT operations practices.

We have also seen a great deal of activity in the Sarbanes-Oxley compliance arena. Clients demand IT systems in compliance with the rules and regulations along with the benefits of an efficient reporting process while encompassing economies of scale. As auditors we understand the controls; as IT professionals we understand the technology, and this combined experience provides value to our clients.

Particularly important in today’s business climate is the ability to do things better, at lower cost and to manage their systems efficiently while promoting ease of use and maintaining security. These are powerful business differentiators, and is the area in which our practice operates.

**Editor: With respect to the implementation of IT governance and the management of IT risk, what are the major challenges facing general counsel and the members of corporate legal departments today?**

**Joma:** Regulatory requirements are being issued from all levels of government and from a myriad of oversight boards. The compliance requirements today can be staggering, and organizations are faced with some very direct challenges such as: How do we keep up with what is expected of us? How do we know what is required? How do we manage this situation? And how do we effectively address what is necessary without compromising our business operations?

Our practice can help the client’s IT department identify their compliance requirements. We are not acting as legal counsel here but rather helping to establish governance practices that promote a partnership between in-house and external counsel and the stakeholders within the IT department to properly identify the organization’s response to this set of potentially complicated regulatory requirements.

Too often, IT administrators are forced into a situation where they must address the technological requirements of information management without any guidance on how compliance with a large spectrum of rules and regulations is to be achieved. As the global economy advances, the international aspects of multi-jurisdictional compliance will begin to add to an already complex situation. We can help by establishing risk management practices at the project, organizational and enterprise levels so that issues and potential errors may be identified



**Ronald A. Joma**

and addressed early in the design cycle.

As compliance requirements are identified, we work with our clients on the design and implementation of business and technical controls that will enable them to move IT initiatives forward operationally. Another imperative, increasingly important since the enactment of Sarbanes-Oxley, is to assist our clients in developing an ongoing compliance function to verify the correct and proper operation of these controls.

Finally, it is simply not cost-efficient to madly scramble to meet a regulatory requirement and then coast along until the next time, or to manage controls by addressing audit exception. Ongoing compliance monitoring is becoming a part of the corporate culture and setting up systems to support this function is another example of the services Amper provides to its clients.

**Editor: Does it make sense for a corporation to have a full-time staff concerned with the management of IT risk?**

**Joma:** The critical distinction is continuous management vs. full-time management of IT risk. Certainly the size and the market dynamics of the organization play a role, but we are seeing an increasing number of organizations choose to establish the post of a Chief Risk Officer, to address this area. For some organizations this has become a full-time position, for others, having the role identified and individual on-call has been sufficient. I might also add that the Risk Officer is frequently associated with the legal department.

In our experience, companies that have successfully addressed enterprise risk, whether with in-house staff or in conjunction with outside consultants, tend to have a competitive edge.

**Editor: Privacy concerns vary from jurisdiction to jurisdiction. The differences between the U.S. and the EU in this area come to mind. How do you factor these differences into your advice to a global enterprise concerning data governance?**

**Joma:** This is an extremely challenging area both in terms of the cause and the effect of these regulations. Some countries traditionally rely on a strong central government to establish all regulations. In North America we tend to place our focus on the market for a more self-regulatory approach. For operations spanning various jurisdictions, the result is a sometimes bewildering set of requirements, at times even being self-contradictory.

Compliance while maintaining a competitive edge entails knowing the applicable rules in each jurisdiction where the organization carries on its activities and the combinations in which those rules will be applied. That entails a considerable effort in systems design and controls analysis. Process data flows can, for example, result in inadvertent export of personal or identifying information along with exposure to various penalties. Consider the implications of having EU citizen data, stored in a reservation system housed in the U.S., but viewed by an out-sourced help-desk function located in Asia.

We help our clients to establish a data governance framework through which they can map and understand the data regulatory requirements they are subject to across all

of the jurisdictions in which they operate. As regulations usually have some ramp-up period before full mandatory conformance is called for, data governance is not a simple mapping exercise either but also involves an understanding of the IT strategy and controls architecture implications going forward. In this area alone, the value of a solid framework managed by a compliance organization should be quite clear.

**Editor: You mentioned tradeoffs concerning the various risks that a company faces. Can you be more specific?**

**Joma:** Let me use a scenario to make my point. Assume that one needs to travel from one location to another. For an emergency vehicle the priority is to get from location A to location B as quickly as possible, regardless of the increased risks of exceeding the speed limit, going through red lights, and so on. Other travellers will choose to take a lower risk and get to point B at a later time but with considerably less stress. This is your risk posture – what is the level of risk you will tolerate to achieve a goal?

Organizations think along similar lines, understanding that where there is risk, there is also reward. How an organization approaches risk and what level of risk it will assume in its operation has become a key differentiator. Not understanding an aspect of the risk facing the enterprise can be the prelude to disaster.

There are many ways in which a company may address risk. One can simply choose to get out of risky operations. Or one can transfer the risk onto someone else through insurance policies or similar arrangements. Most organizations will assume a level of risk but mitigate it to an acceptable level by deploying controls into the operating environment.

The important thing, I think, is to *consciously* approach the tradeoffs between risk and reward. A company that is going to maximize its upside is the one that can make an informed decision of the risks/exposures vs. the opportunities/rewards, and the potential controls that are available to balance these factors.

**Editor: As you know, most of our readers are general counsel and the members of corporate legal departments. What role do they play in this area?**

**Joma:** The corporate legal department has an extremely important role in this area. As mentioned, there is the well-established role of being the “legal” risk advisors. Working in a collaborative manner with IT, corporate legal departments can consult with IT about the regulatory requirements, the deployment of controls and alert IT to changes as these occur.

As stakeholders in the management of risk, when corporate legal departments provide their input *in advance*, i.e., during the design phase of an IT project, the resulting controls can be most cost-effectively designed and deployed. This is far preferable to having no legal review of systems compliance and far less expensive than re-developing systems with add-on controls after the fact. Legal departments must establish themselves as active members of the development life cycle. I see the corporate counsel-IT partnership as absolutely crucial to success in the risk management arena.

Please email the interviewee at [joma@amper.com](mailto:joma@amper.com) with questions about this interview.