Achieving Enterprise Risk Management Maturity

Enterprise Risk Management (ERM) is a process effected by an entity’s board of Directors, management, and other personnel, applied to strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO).

Do we practice Risk Management at the Workplace?
Yes of course we practice risk management individually and in our teams at the workplace. We also inadvertently practice Risk Management (RM) in our personal lives, at home, on the road, and in almost all situations that we are confronted with. How can this be? To answer this question we need to go back to the definition of risk!

What is risk? Risk simply is anything that can prevent you from achieving your objectives. Risk Management is managing those risks to reduce the likelihood of occurrence and or the impact if it does occur, thereby facilitating achievement of objectives.

One simple example of how we manage risk in our personal lives can be seen by examining Fred’s situation below:

Fred’s objective is to safely cross the busy highway to purchase two doubles from the best doubles man in the area. However Fred identifies that there is a risk that he can get knocked down by a passing vehicle in his attempt to cross the road.

Fred internalizes and assesses this risk by observing the volume and speed of traffic on the road, considering his own speed - walking skills, and the impact of getting knocked down and he even recalls a media report a few months ago on a pedestrian accident in the area.

After taking all of these factors into consideration Fred has to decide on his risk response to mitigate this risk. He may either:

- Look both ways, then cross when it's safe or
- Use the walk over
- Or jump in his trusty car and make the rounds to the nearest intersection to get to the other side
- Or not even bother to get the doubles on the other side of the road and settle for the cold tasteless doubles next door instead.

Fred’s decision will be based on his acceptable level of risk i.e. his risk tolerance levels and the cost of each response. Using the walk over may be safer than looking both ways, however will definitely take more time and energy for Fred to climb the steps to the walkover. Whilst settling for the cold tasteless doubles next door may be just as safe but less costly in terms of time and energy, however the tradeoff will be in the quality of the product for consumption.
This subconscious ad-hoc process which Fred went through is called the **Risk Management Process** and we do it every day in everything that we do to make decisions at home as well as for simple and complex decisions in the workplace.

In our personal lives these risk management decisions will primarily impact ourselves and our families. Whilst in an organization where our objectives, risks and responses have far reaching consequences, these risk management decisions impact thousands of stakeholders daily and can relate to health, safety, efficiency, profitability and the sustainability of the organization.

Hence it makes sense for this critically important RM process to be structured, and consistently applied across the enterprise. Using one agreed framework ensures that risks are properly and thoroughly considered by Management with the best outcomes in mind.

Best practice suggests that a Committee of Experts within the entity should be constituted to review and agree on Management’s:

- **identification of risk** that may prevent the achievement of strategic and operational objectives;
- **assessment** of each of these **risks**;
- **response** to each of these risks;
- **monitoring and communication** of all of the above to ensure that objectives are met.

This will ensure that the best decisions are made to mitigate risk to the tolerance levels agreed by Management and the Board, thereby enabling objectives to be met whilst also taking advantage of available opportunities.

The good news is that there are best practice frameworks currently available that any entity can adopt and customize to formulate their own RM policy and procedures. E.g. ISO 31000 or the COSO Enterprise Risk Management Framework.
There are many areas within our organizations that are heavily regulated and have included sophisticated RM activities into their day to day processes. However the organization as a whole remains at risk if there is no consistent RM framework that continuously considers and monitors all types and levels of risks throughout and across the entire organization.

There are also many different ERM Maturity scales available that one can use to assess your organization’s current Risk Management Maturity level and to set short and medium term goals for the continued improvement of your entity’s ERM program.

Many other organizations are doing it. Why shouldn’t we?
Section 3.2.4 of the State Enterprise Performance Monitoring Manual (SEPMM) states; “the ability to manage risk is one of the core competencies of any organization and its employees. The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. This framework assists in managing risks effectively through the application of a risk management process at the varying levels and within specific contexts of the organization”.

The benefits of a defined risk management program include:

- Greater awareness about the risks facing the organization and the ability to respond effectively
- Ability to plan for and take advantage of opportunities
- Achievement of our individual, departmental and organizational objectives
- Reduced losses / Increased profitability and higher incentives for employees
- Return on Investment (ROI) for shareholders

“Risk management is a more realistic term than safety. It implies that hazards are ever-present, that they must be identified, analyzed, evaluated and controlled or rationally accepted”.


“Some risks that are thought to be unknown, are not unknown. With some foresight and critical thought, some risks that at first glance may seem unforeseen, can in fact be foreseen. Armed with the right set of tools, procedures, knowledge and insight, light can be shed on variables that lead to risk, allowing us to manage them.”

— Daniel Wagner

“The essence of risk management lies in maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome.”

— Peter L. Bernstein

SUBMITTED BY:
Kevin Padmore
Executive Manager, Internal Audit
Caribbean Airlines Limited
**Humour to keep your stress level down**

*WHEN YOU’VE HAD A ROUGH DAY BUT YOU’RE TRYING TO STAY POSITIVE.*

“It’s great. I’m great. Everything’s just great.”

---

**Joke of the Day**

My boss asked me to start my presentation with a joke...

So I attached my paycheck to the first slide!

---

Dad, when is Fathers Day?

Nine months before Mothers Day

Dude! I have a ton of online followers and they all want to have me over for dinner!
The Institute of Internal Auditors celebrated its thirty-year anniversary by hosting a week of training from September 17th to 20th, 2018 at the Arthur Lok Jack Global School of Business. The theme for this week of celebration was “Taking The Lead – Embracing Change & Inspiring Innovation for 30 Years”.

The first seminar was held on September 17th and was entitled ‘Cyber security for non-IT Auditors’. This seminar was facilitated by Mr. John Sapp of GoldSRD. He provided an overview of the types of cyber attacks on organisations, the importance of developing a Cyber security strategy, the components of this strategy, the role of the Internal Auditor, the three lines of defense, the cyber security risk assessment framework and cyber security controls. This was a very informative session which provided vital insights into the assessment of strategies and frameworks to assist an organisation with instituting and strengthening internal controls to mitigate against cyber security risks.

‘IT Auditing for non-IT Auditors’ was presented by Mr. John Sapp on September 18th. This course provided Internal Auditors with a basic knowledge of IT Auditing and an understanding of the general concepts and best practices that encompass a more robust audit of IT systems. Information technology consists of people, networks, software, hardware and data. These must be effectively managed to ensure that risks are mitigated and that the organisation receives value.

On September 19th, ‘Value for money auditing’ was facilitated by Mr. Kenny Jalsa. He provided an overview of the internal audit process and the definition and mission of internal audit. In addition, the Internal audit planning and execution processes were outlined. Mr. Jalsa also delivered a synopsis of the purpose of exit meetings, the importance of receiving management’s responses and effective communication during and after the audit engagement.

The session on emotional intelligence was an interactive one whereby the Presenter, Shane Ram, engaged the attendees throughout the session. He provided real life examples that helped him along his career path and this was well received by the attendees. Overall, the feedback was very positive and Mr. Ram encouraged members to look at life’s situations/challenges from an optimistic perspective. He also offered better approaches to dealing with negative life experiences and provided tips on self-motivation, job satisfaction, effective communication, conflict management and relationship management.

The Institute of Internal Auditors expresses its sincerest gratitude to the membership for supporting this week of activities and we look forward to creating future opportunities for knowledge sharing and professional growth.

SUBMITTED BY: Martha Prince V.P.—Professional Services
Auditing in Cloud Computing Technology

While cloud computing has been around for the past ten years, it’s only recently become a growing topic for businesses and governments across the Caribbean. So much so, that the subject has led to a few round table discussions, such as those hosted by both Cable and Wireless (C&W) and the Trinidad and Tobago Coalition of Services Industries (TTCSI). It was at these forums that presenters Marcelo Oliveira, Director at C&W and Enrique Camacho, Managing Partner of eSource Capital Technologies, delved into the varying benefits of Cloud Computing Technology and the importance of having that strategic conversation. However, to begin this conversation, one must first understand; what exactly is cloud technology and whether the regulatory policies are in place to facilitate and monitor a smooth transition while protecting all parties and data involved.

**Cloud Computing Technology** – Microsoft, one of the leading global providers of cloud computing services, defines it simply as “the delivery of computing services—servers, storage, databases, networking, software, analytics, intelligence and more—over the Internet” (“the cloud”). Additionally, considering that each client may not have the same needs, cloud computing is deployed in four general types; public cloud, private cloud, hybrid cloud and community cloud.


**The Importance of Policies and Audit** – Understanding the significance of both areas is critical in this new and growing industry. As with all investments, one should note that, the greater the rewards, the higher the risks. It was due to this fact that on the 25th May 2018, the European Union decided to enforce its General Data Protection Regulation (GDPR) with the sole aim of protecting or issuing fines to individuals involved in transitioning to cloud computing technology. It is therefore of utmost importance that governments and businesses across the Caribbean chart the same course by enforcing proper regulated policies that not only aim to protect and govern the users of cloud technology, but also to allow auditors and compliance officers to assume their key roles in assessing risks and vulnerabilities as cloud services evolve.

Auditors should appreciate the huge significance of data security since it serves as a guide to designing the various aspects of the auditing framework for the cloud computing environment and the three types of service delivery are as follows: Infrastructure as a Service (IAAS), Software as a Service (SAAS) or Platform as a Service (PAAS). Auditors should be aware that data governance and compliance issues faced by organizations are the same whether operating in the cloud environment or not, based on the company’s expanding data volumes due to growth. Therefore, when an organization considers moving business data and systems into the cloud, a sound data governance platform must be in place to avoid costly data protection errors. It is at this point, internal audit is ideally positioned to review how well the organisation has established sound IT governance and IT security foundations, including defined organisational structures, documented policies, clarity of roles and responsibilities, performance and monitoring arrangements.
Furthermore, because risk management is considered the basis of good governance, internal audit should examine how well management has identified and assessed risks, particularly those related to cloud computing, and express a view on whether or not this has been done effectively. This should then enhance how emerging risks are regularly reviewed and reported through to senior executives and the audit committee. The cloud provider should also have a mature risk management process in place which is an important part of choosing a suitable partner. This therefore means the organisation needs clear visibility of the provider’s risk appetite and risk limits to gauge how much risk the provider is prepared to tolerate. To do this effectively, internal audit is to ensure that the organisation performs due diligence in selecting the most appropriate service provider by asking some basic questions as these below.

1. Do they have a good track record? (Any history of security problems and fines)
2. Do they serve similar clients? (Can they offer testimonials and references?)
3. Are they financially stable? (Availability of financial statements and bank references)
4. How will they provide support? (Where, when and how with service level agreements)
5. Do they have adequate resilience and contingency arrangements?
6. Have they performed their own risk assessment? (Can we see the risk register?)
7. What is the migration process? (How much effort is required on our part?)
8. What is the default data storage/usage volume? (Will this work for us?)
9. Do they have quality and IT certifications? (Such as COBIT, ISO9001 and ISO27001)
10. Will you do audits and provide reports? (Or can we audit with penetration tests?)

Having addressed all these concerns, internal audit now has the opportunity to work with the management within the organisation to establish continuous monitoring arrangements in relation to cloud operations.

https://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/10-14-16-cloud-computing/cloudcomputing.pdf
https://gdpr-info.eu/
https://www.iia.org.uk/resources/it-auditing-and-cyber.../cloud-computing/

SUBMITTED BY:
Simone Rowley-Burgess
Internal Auditor
The Anniversary Dinner was the culmination of our Week of training activities which took place over a four (4) day period. It was held on September 21st, 2018. The night began at 6.30 p.m. with cocktails, and followed by the formal session. This event was hosted by Mr. Khyam Abdulah, V.P. Professional Development. The national anthem was done by Mr. Anselm Walters, violinist.

The President then took to the podium with the opening address (excerpt of which is included). She welcomed the feature speaker, Mr. Mariano Browne, our Board of Governors, Executive team, and other specially invited guests. Her speech tied into the theme for the Anniversary Week “Taking the Lead – Embracing Change & Inspiring Innovation for 30 years”, and addressed some of the ways in which the IIATT has taken the lead while embracing innovation.

Dinner was served from 7:20 p.m. with exquisite musical accompaniment by the accomplished Mr. Walters who provided a wonderful blend of classical, Asian, middle eastern, and of course local music.

The feature Speaker then took to the podium and spoke on the topic “Cryptocurrency and the Auditors’ role”. He urged Auditors to be proactive in obtaining extensive information on cryptocurrency as it is anticipated to revolutionize the financial sector and become a mainstream form of exchange.

The night belonged to our membership and the Chapter sought to recognize the members who had successfully completed IIA Certifications during the period 2016 to 2018. Twenty-seven (27) persons were identified, and tokens were presented in celebration of their achievements. Our past Presidents were also recognized.

Door prizes in the form of hampers were given to our members and this writer thinks that we should audit the success of the NGC table which claimed at least three in quick succession.

Then it was time to once more be entertained, and we had the beautiful Tricia Lee Kelshall who gave a very vibrant performance, which even saw our Chapter Treasurer taking to the floor for a spin with her (much to the delight of the audience).

The evening closed with a vote of thanks which was carried by our Senior Vice President, Sunil Babooram. Special mention must be made of our corporate sponsor, Atlantic LNG, who very generously supported our anniversary event.

IIATT is looking forward to our next event as we continue to celebrate our achievements with you, our members.
Excerpt of the opening address by the President of the Institute of Internal Auditors, Trinidad and Tobago Chapter:

“In 1988 a visionary group of practitioners who believed in auditing and the positive impact that it would have on our twin island republic took the lead and partnered with the IIA Inc. we were accepted as a member of the Institute of Internal Auditors on 30th September, 1988 at a Conference held in Albuquerque, New Mexico.

In 1991 we were incorporated by Act of Parliament with the objectives to:
• Increase knowledge and skills of its members as regards internal auditing and the practice and methods thereof.
• Establish and maintain high standards of integrity, honour and character of its members.
• Promote and protect the welfare and interest of the Institute and the internal auditing profession in Trinidad and Tobago.

Over the past 30 years we have seen the Chapter steadily grow in numbers while building on those stated objectives. We have continued to take the lead, we have embraced change and inspired persons from all walks of life to come on board and join the profession of internal auditing.

Some of the changes which have been made was dispelling the myth that auditors were policemen running down 10 cents, we are now seen as change agents who assist management in strengthening business systems. We are sought out rather than hidden from and it is now understood to a large extent that we are here to help to improve systems and not to find fault or ascribe blame.”
1. Thursday, November 8th       Half Day  
   3rd Chapter Meeting for 2018  Venue: Arthur Lok Jack Global School of Business  
   “Applying the Procurement Legislation—Ensuring Good Governance and Achieving Compliance”

2. Thursday, December 6th    6:00 pm to 8:00 pm  
   Annual Christmas Cocktail  Venue to be advised