Office of Internal Audit & Compliance's (OIAC) mission is to support the University System of Georgia management in meeting its governance, risk management and compliance and internal control (GRCC) responsibilities while helping to improve organizational and operational effectiveness and efficiency. The OIAC is a core activity that provides management with timely information, advice and guidance that is objective, accurate, balanced and useful. The OIAC promotes an organizational culture that encourages ethical conduct .

We have three strategic priorities:

1. Anticipate and help to prevent and to mitigate significant USG GRCC issues.

2. Foster enduring cultural change that results in consistent and quality management of USG operations and GRCC practices.

3. Build and develop the OIAC team.

# From the Chief Audit Officer

John M. Fuchko, III

Under the Chancellor's and the Board's leadership, the OIAC's vision is focused on the future. We recognize that relevant risk management, good governance,

KPMG identified several core attributes of organizations that ar understanding the model's concepts and a world class IA func tion requires an Audit (IA) function. According to KPMG, optimum balance between positioning, people and processes that can add value across the organization. Excellence is achieved when these key factors work in tandem to create institutional transformation.

Positioning focuses on expanding and focusing the services provided by the IA function, so that institutional business pa rtners view the IA function as providing value across the enterprise and not just evaluating financial compliance. The IA function should employ people who posse ss a diverse mix of skills, experience and capabilities to expand the ability of the team. Finally, the IA function must employ and integrate formal auditing processes that align with the organizational strategy.

# Embedding "Risk Management" into Yo ur Everyday Decision Making

by Scott Woodison

## The Black Swan

The book is concerned with randomness and uncertainty, and our chronic inability to accurately fathom and measure these phenomena.

According to Taleb, a Black Swan event is one that is unpredictable yet has wide-spread ramifications. Not only are Black Swan events difficult to

Currently one of the hottest topics in the business press is the concept of "Risk". Whether it's the collapse of the financial markets, the turmoil in the European Common Market over the Greek debt crisis, or the tsunami and subsequent nuclear reactor failure in Japan, everyone is talking about Risk.

And no, the recent book that everyone is talking about titled The Black Swan is not about a ballet dancer. The risk theory known as the Black Swan was developed by Nassim Nicholas Taleb in his book The Black Swan: The Impact of the Highly Improbable. His book develops the concept of the disproportionate role of high-impact, hard-to-predict, and rare events beyond the realm of normal expectations, and how to think about these occurrences. Since his writing in 2004, many unexpected, high impact events are now referred to as Black Swan events. But not all of our risks are Black Swan events. In fact, very few risks are Black Swan events. Most risks can be predicted or possibly prevented.

The University System of Georgia is currently implementing a system wide Enterprise Risk Management (ERM) program. The basic tenet of the program is "risk mitigation" through a specific process, which include the following:

- Identifying institutional objectives;
- Identifying and ranking risks.
- Selecting key risks and assigning a risk owner to each key risk
- Identifying a risk tolerance and mitigating controls for each key risk.

The goal of ERM is to work with each institution to develop a list of key risks, and to subsequently consolidate the key risks of all institutions into a system-wide risk profile. The consolidated list of key risks will then be evaluated to help determine which key risks impact the USG as a whole.

While this creation of a list of key risks for each institution is a major focus of the ERM program, a second focus item of the program is to have each institution embed the concept of risk management into everyday operations. Every major decision made by an institution

## Embedding "Risk Management" into Your Everyday Decision Making, cont'd

should be considered in regard to the question, "What is the risk of this decision?"

In order to properly understand risk management, we must understand a new set of terms, processes and questions.

What occurrence or activity (the risk) will stop us from being successful?

If we define risk as "something that will stop us from accomplishing our objectives", then we should focus on what environmental risks, (business, legal or otherwise) will prevent us from being successful.

When we evaluate a decision from a risk perspective, we must attempt to answer a number of questions:

What is the impact, likelihood, and the velocity of this risk? The Impact measures the negative outcome if the risk should occur. The Likelihood measures the expectation that something will happen, usually based on prior experience. The Velocity measures how fast the impact can occur. The value of the product of the impact, likelihood and velocity will provide us with a risk rating.

What is our tolerance or appetite for risk?

Risk is inherent in everything we do. In a risk/reward scenario, to earn a reward requires some level of risk. Our risk tolerance measures how much risk we are willing to accept based on the anticipated reward. Management must decide their tolerance for risk, or how much risk they are willing to accept. For example, management may have a lower tolerance for risk, if that risk could have a major effect on the reputation of an institution or success of a program.

What controls are currently in place, and what controls should be put in place?

If there are no controls in place, then we have what is referred to as inherent risk. However, if controls are put in place which will reduce risk, then we will end up with what is called residual risk. As managers, we need to ensure that before starting projects, controls are in place to reduce risk (residual risk) to a level where the risk is below the established risk tolerance.

The purpose of ERM is to evaluate and rate risk. After the risk is identified and rated, controls need to be implemented to reduce the risk to a level commensurate with the institution's risk tolerance.

Risk management is not difficult, but it does often require a new way of thinking. If you can successfully anticipate and control risks, then your project should also be successful.

---

Contact Scott Woodison to learn more about risk management and for assistance with implementing your institution ERM program.

Scott Woodison
Executive Director, Compliance and Enterprise Risk
Email: Scott.Woodison@usg.edu
Telephone: (404) 962-3027

# Governance, Risk Management, and Compliance

## by Jeanne Severns

Governance. Risk Management. Compliance. These are some of the concepts behind successful organizations. Just like financial institutions and manufacturing businesses, the USG's mission of Creating a More Educated Georgia requires a high standard of governance at all institutional levels: administration, nda.0011 Tw (2011 an3T7sTw uires.nst(eTw (2er4(RROW )]TJ q/eTJ 0 -1.30sstudce bodyf 10.02 - (2er4-2.

> "No matter if you use the term or not – GRC (Governance, Risk Management, & Compliance) is a reality. We are in 2011 and it has been ten years now since I first started using the term GRC in research and interactions with organizations.
>
> The truth of the matter is – GRC as an acronym is approximately 10 years old, but GRC as part of business is as old as business itself. "
>
> Michael Rassmussen, CCEP, CISSP
>
> Michael Rasmussen is an internationally recognized pundit on governance, risk management, and compliance (GRC) with specific expertise on the topics of corporate compliance, business ethics, policy management, and corporate culture.
> www.corp-integrity.com

## Governance, Risk Management and Compliance, cont'd

A focus on human resources that demonstrates efforts to build and improve an effective and supportive workforce environment by providing training for employees, by engaging employees in the organizational planning, and by ensuring that performance measures are in place and that employees are evaluated against them.

A focus on results that provides continual evaluation for effectiveness by looking at productivity, work cycle timelines, and accuracy. A strategy used to measure results is the use of key indicators.

When OIAC performs an internal audit, one of the aspects it considers is the overall governance of the institution. Recommendations are often made based on the assessment of the factors mentioned above. Additionally, in its support role, the OIAC staff is available to consult on what best practices might look like in any of these areas.

We look forward to answering any questions you may have on this topic, and we hope you will look forward to reading more on the topic of governance, risk management and compliance in our next issue.

Jeanne Severns
Interim Executive Director, Internal Audit and Compliance
Email: Jeanne.Severns@usg.edu

## A Model for Good Governance Incorporating Leadership, Policy, Workforce Participation and Results

# Desk Audit Results – Compliance and Ethics Reporting Hotline
## By Belinda Pedroso

The OAIC Compliance and Ethics Program launched the Compliance, Ethics and Reporting Hotline in 2008. The Hotline was introduced to reinforce USG's commitment to high standards of integrity and accountability in respect to governance and financial operations. The Hotline also reinforced the culture established through the USG Ethics Policy, and the administration's goal to increase esteem for higher education.

It's been approximately four years since the launch of the Hotline, so we decided to conduct a brief desk audit of its visibility system-wide. The desk audit entailed a very simple procedure. We identified our objectives: visibility and access. Next, our methodology entailed viewing all USG institution websites and virtual communication portals to find the Hotline link. We asked the very simple que Next,e cr Tc -1leons Tw9(:)8(-5.5(ti)-Tj 0 -1-20-.0 <04 0 TD .0006 Tc .14(e

| | |
|---|---|
| 5. | Where was the Hotline located on the Institutions' website, as in, what department or division of |