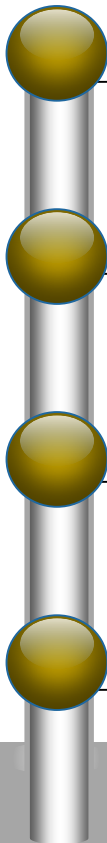


# CORE INTERNAL AUDIT ROLES FOR ERM

PREPARED FOR BAHAMAS INSTITUTE OF  
INTERNAL AUDITORS

MARCH 20, 2019



- 
- What is Risk Management?
  - ISO' Approach to Risk Managemetn
  - Internal Audits Role in Risk Management
  - Do's and Don'ts for Internal Audit

# RISK MANAGEMENT OVERVIEW

- According to the Institute of Internal Auditors (IIA), an effective Internal Audit is one of the four cornerstones of Corporate Governance (CG).
- Recently ERM has become essential in managing an array of corporate risk in an integrated, enterprise-wide fashion.
- Therefore, the study of Corporate Governance is paramount to ERM and IA.

# FOUR CORNERSTONES OF EFFECTIVE GOVERNANCE



1. IA essential to good CG
2. Along with the audit committee.
3. Management support is crucial.
4. External auditors can also assist.

- Entities financial performance is incomplete without reference to the necessary risk to achieve objectives.
- Governance monitors & assesses performance, satisfy shareholders, and adds value to maximize enterprise value.
- Recent studies also show a positive correlation between the IA's knowledge and use of Information technology plays an important role in capturing and evaluating accounting information.

## CORPORATE GOVERNANCE

---

Globally in academic literature, CG denotes a well-defined problematic area, that relates to managing large companies in the interest and under the control of shareholders who respects the rights of other interest holders in the entity.

Not always the same when we consider CG and management of entities in The Bahamas.

# CLASSICAL MODELS OF CORPORATE GOVERNANCE



In corporate governance system there are many interested factors, including:

- shareholders,
- directors,
- managers,
- employees,
- creditors,
- suppliers,
- customers,
- government and the community.

- According to research in the field, two models of corporate governance were identified : **shareholder model** and **stakeholder model**.
- While the shareholder model aims to maximize value for shareholders,
- **Stakeholder model** is interested in maximizing value for **all parties involved** in the life of the company (shareholders, managers, employees, trading partners and so on).

## 3 MAIN MODELS OF CORPORATE GOVERNANCE

- In international practice, there are three models of generally accepted corporate governance models.

### Anglo-Saxon Model

- Commonly found in The Bahamas & USA.

### Continental-European Model

- Dual Governance system.

### Japanese Model

- BOD includes representatives of stakeholders & Censors Commission.

**Table 1. Comparative analysis of corporate governance models**

	<b>Anglo-Saxon Model</b>	<b>Continental-European Model</b>	<b>Japanese Model</b>
<b>Main financier</b>	Exchange market	Banking market	Banking market
<b>Ownership right</b>	Based on the ownership of shareholders	Based on the ownership of shareholders and the relationship between employees and company	Based on the interests of the parties (stakeholders), mainly keiretsu (a type of grouping several firms)
<b>Shareholder structure</b>	Dispensed	Concentrated	Concentrated (cross-holding of shares)
<b>Council composition</b>	Unitary system of governance: <ul style="list-style-type: none"> <li>Executive managers</li> <li>Non-executive managers</li> </ul>	Dual governance system: <ul style="list-style-type: none"> <li>Execution Board - in charge for company management</li> <li>Board of Directors - in charge for supervision of the Execution Board</li> </ul>	Board of Directors includes representatives of stakeholders and Censors Commission
<b>Control mechanisms</b>	Extern	Intern	Intern
<b>Accounting system</b>	Generally Accepted Accounting Standards (GAAP)	International Financial Reporting Standards (IFRS)	GAAP and IFRS

Source: Cuc, S. & Tripa, S., 2006, p. 437.

- **The Anglo-Saxon Corporate Governance Model or the Shareholder Model** is based on **dominance of shareholders**, the only interested parties to whom managers have an obligation to respond.
- They act as administrators of money because **their predominant interest is the enrichment**.
- The management of company is provided by a unitary Board of Directors, without differentiating between non-executive and executive positions, since all board members are responsible for all legal actions of the company.
- These members have the obligation to defend the interests of shareholders.

## TWO CONTRASTING VIEW POINTS

**FOR**

### Negative side

- Profit focused
- No long-term planning.
- Dispensed shareholder structure.

**AGAINST**

### Positive side

- Seeking Efficient domains
- Reducing inefficient domains

- The IIA International Standards define risk as “**the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.**”
- Organizations of all types and sizes face **internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is “risk”.**

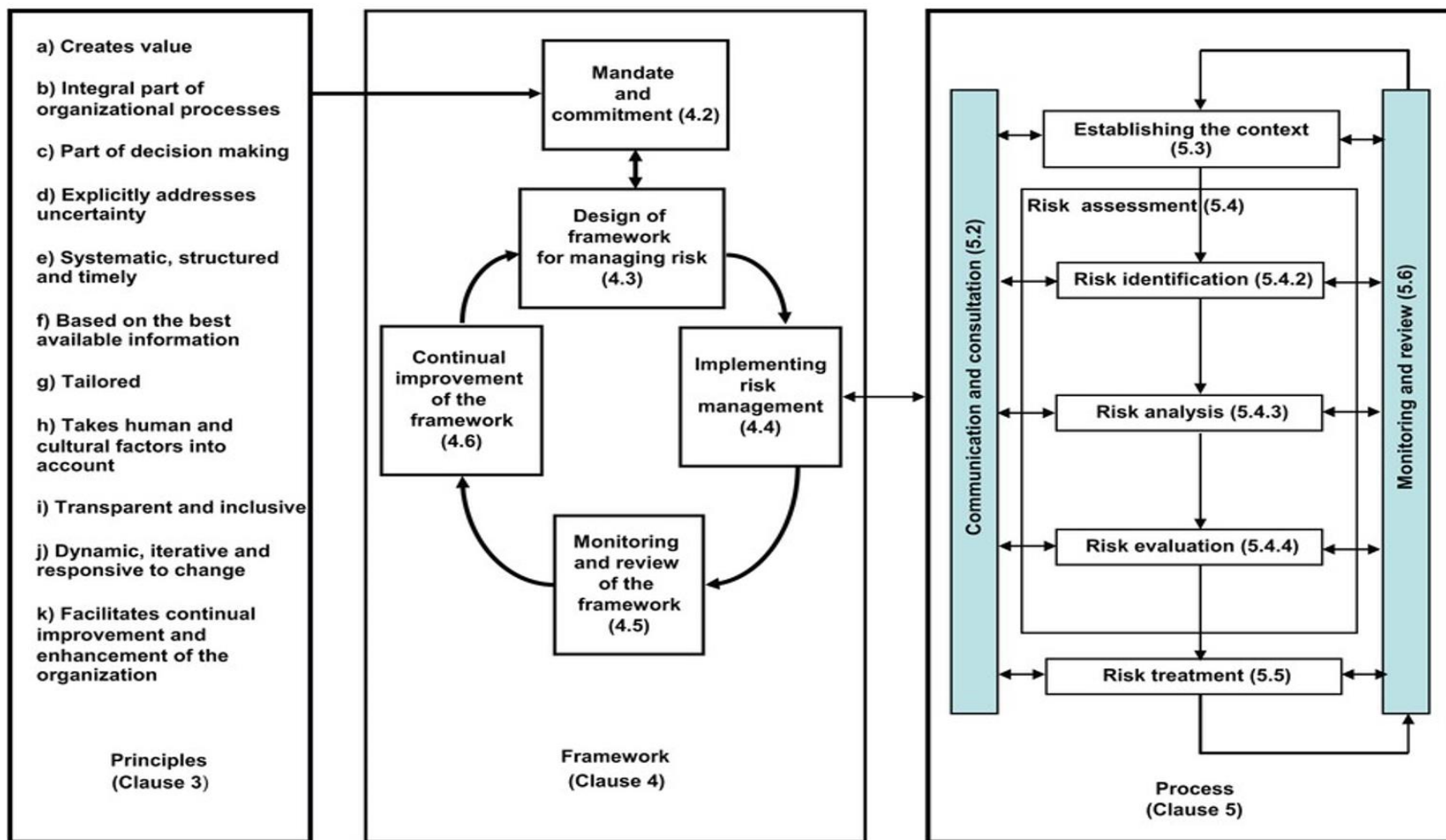
-

- ISO 31000 is an attempt by the International Organization of Standardization (ISO) to produce a generic version of risk management that could be adopted to most organizations.



- When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:
  - increase the **likelihood of achieving objectives**;
  - encourage proactive management;
  - be aware of the need to **identify and treat risk throughout the organization**;
  - improve the identification of opportunities and threats;
  - comply with relevant legal and regulatory requirements** and international norms;
  - improve mandatory and voluntary reporting;
  - improve governance;

# RISK DEFINED



**Figure no. 1 The relationship between the principles for managing risk, the framework in which it occurs and the risk management process according to ISO 31000**

# INTERNAL AUDITS ROLE IN ERM

The first question to consider is, “**What are internal auditors being asked to do?**” It is important to understand the direction that is being provided by the board of directors, typically through **the audit committee** (to whom most internal audit activities report functionally) and **management** (to whom most internal audit activities report administratively).

In August 2009, a **Global Audit Information Network (GAIN) Flash Survey** with **321** respondents identified the following when it asked about the direction provided by the audit committee:

## INTERNAL AUDITS ROLE IN RISK MANAGMENT

Has the audit committee asked internal auditing...		
	Yes	No
to provide an opinion on any individual programs or areas related to risk management?	41%	59%
to provide an opinion on the organization's overall risk management processes?	23%	77%
to perform specific audits of any components of risk management?	28%	72%
for recommendations or advice on enhancing the organization's risk management processes?	45%	55%

While it is difficult to conclude why these percentages are not higher, one answer may be found in another question from that survey. Respondents were asked “How much do you agree or disagree that there is an emerging need for the audit committee to have better insight into the organization’s risk management processes?” The answers to this question were:

Strongly Agree	37%
Agree	38%
Neutral	5%
Disagree	1%
Strongly Disagree	19%

COSO's Enterprise Risk Management Framework is a new and improved version of the Integrated Control Framework. **It is the process the board of directors and management use to set strategy, identify events that may affect the entity, assess and manage risk, and provide reasonable assurance that the company achieves its objectives.** The basic principles behind ERM are:

- Companies are formed to create value for their owners.
- **Management must decide how much uncertainty it will accept as it creates value.**
- Uncertainty results in risk and opportunity, which are the possibilities that something negatively or positively affects the company's ability to create or preserve value.
- The ERM framework can manage uncertainty as well as create and preserve value.

- The ERM framework takes a risk-based rather than a controls-based approach. As a result, controls are flexible and relevant because they are linked to current organizational objectives. The ERM model also recognizes that risk, in addition to being controlled, can be accepted, avoided, diversified, shared, or transferred.
- Because the ERM model is more comprehensive than the Internal Control framework, it will likely become the most widely adopted of the two models.

TERM adds three additional elements to COSO's IC framework:

Setting objectives

Identifying events that may affect the company

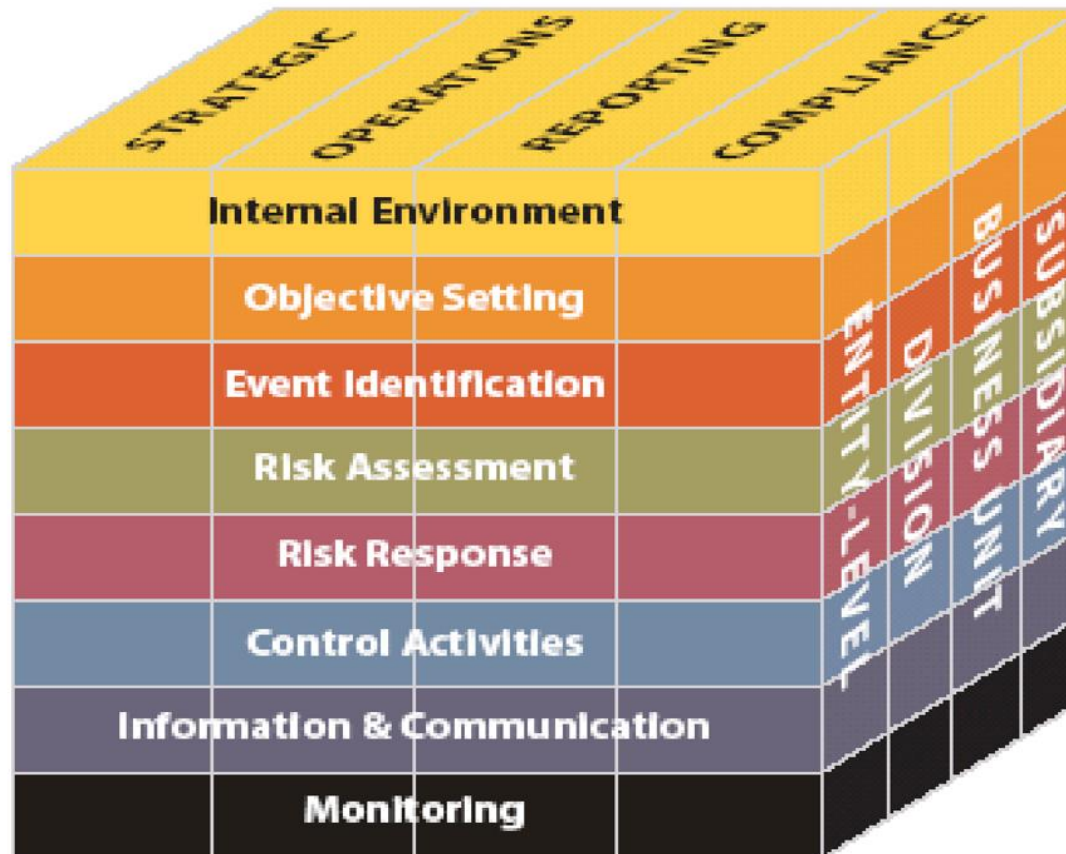
Developing a response to assessed risk.



# RISK BASED APPROACH



# COSO'S ERM FRAMEWORK



- Despite the modest level of top-down direction received from the audit committee and management, **internal audit activities have made strides in playing a role in risk management and will continue to do so.** The 2010 IIA Global Internal Audit Survey (a component of the Common Body of Knowledge [CBOK] studies) indicated that **57 percent of internal audit activities around the world perform audits of enterprise risk management processes.** Furthermore, 20 percent of respondents indicated that they believed performing such audits would become more prominent over the next five years.
- An IIA Position Paper titled *The Role of Internal Auditing in Enterprise-wide Risk Management* provides an illustration that presents a range of risk management activities and indicates which roles an effective professional internal audit activity should and, equally importantly, should **not** undertake.

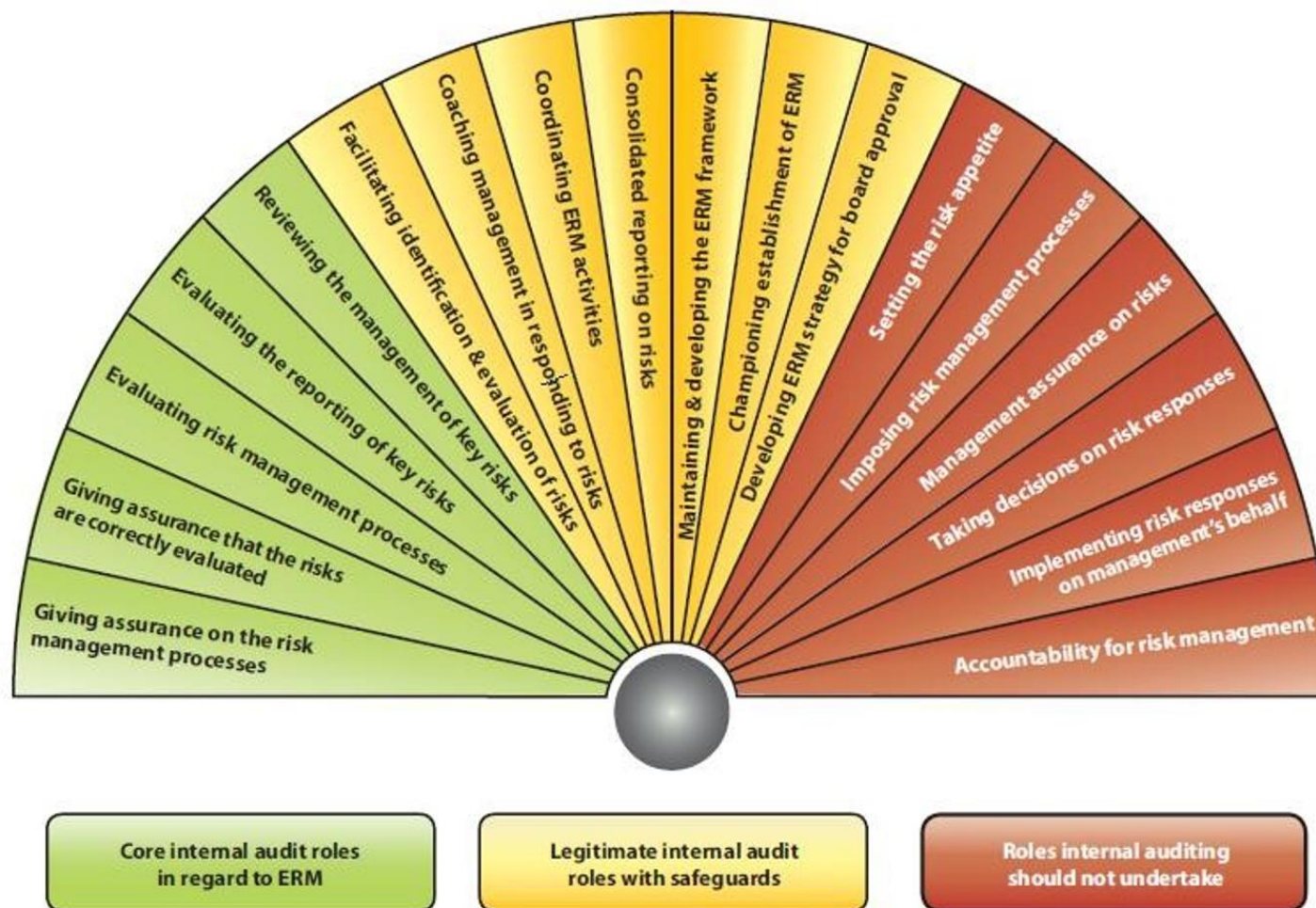
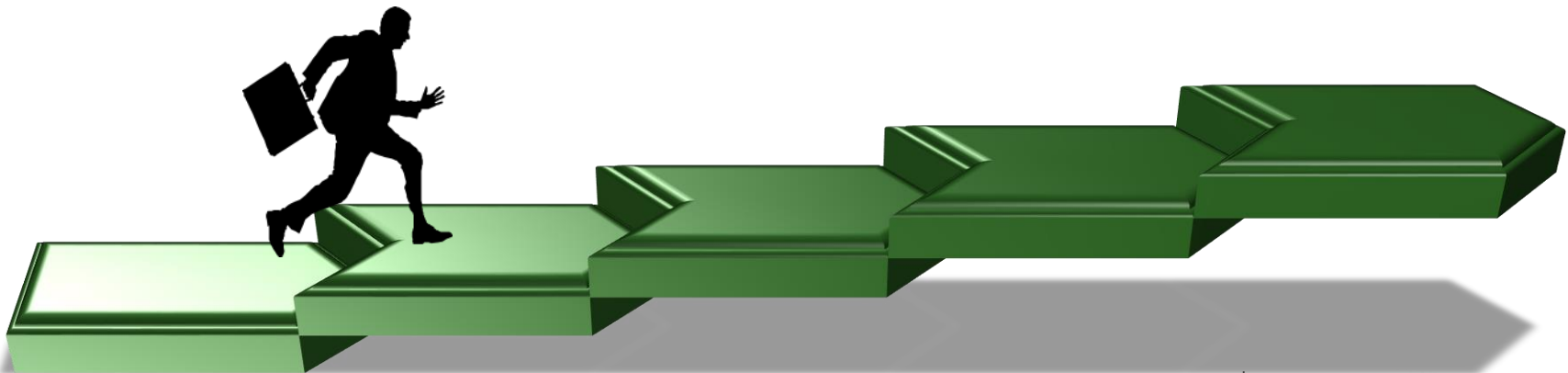


Figure no. 2 Internal auditing's role in ERM

- The five areas on the left of the fan represents **core IA roles for risk management.**
- The seven areas in the middle represent **legitimate IA roles** with **appropriate safeguards.**
- The six areas on the right are roles **that IA should not undertake** because they are management responsibilities that would impair the IA objectivity.

- The five areas on the left of the fan represents core IA roles for risk management.
- The seven areas in the middle represent legitimate IA roles with appropriate safeguards
- The six areas on the right are roles that IA should not undertake because they are management responsibilities that would impair the IA objectivity

# GROWTH AND IMPORTANCE OF IA



Internal Audit  
was only  
concerned  
with Fraud

Internal Audit  
become an  
integral part  
of checks and  
balances

Company  
failures  
increased the  
worth of IA  
Assurance  
Exercises

Risk  
Management  
were  
assessed by  
IA

ERM is now  
an integral  
part of the  
Core  
Functions of  
IA

# CONCLUSION



- RM is a fundamental element of CG.
- **Management is responsible for establishing and operating the RM framework** on behalf of the Board.
- There are **different objectives of Boards**, depending on what model is followed.
- IA core role in relation to ERM is **to provide assurance to management and to the BOD on the effectiveness of RM.**

- When IA extends beyond its core activity, **it should apply certain safeguards**, including treating the engagements as consulting services and applying applicable relevant consulting standards.
- In this way, **IA will protect its independence and the objectivity of its assurance services.**
- Within these constraints, ERM can help raise the profile and increase the effectiveness of IA.

**Should internal auditors be members of systems development teams that design and implement an Accounting Information System? Why or why not?**

Many people believe that internal auditors should be involved in systems development projects in order to ensure that newly developed systems are auditable and have effective controls. However, if the auditor's involvement is too great, then his or her independence may be impaired with respect to subsequent review and evaluation of the system. Accordingly, the auditor should not be a member of a systems development team, or be otherwise directly involved in designing or implementing new systems.

**Any Questions?**

# THANK YOU CARD



## **Contact Information**

Name: JOHN S. BAIN

Phone: 242-427-3880

Email: john@uhy-bs.com