1

Agenda

- Presenter Bio and Objectives
- Compliance, Audit, and ERM Collaboration
- Successful Strategies for Implementing Integrated Risk management
- Technology Trends in Compliance
- 2020 PwC Global Risk Study
- Q&A

2

Introduction – Bio

- John is a Director in PwC's Internal Audit, Compliance, and Risk Management Solutions practice, overseeing the delivery of full scale internal audit outsource arrangements, technical co-source arrangements, and project specific services in the higher education and nonprofit sector. John also serves as the firm's national higher education knowledge manager, connecting teams across the country to share leading practices, developing risk trends, and benchmarking data.
- John has a B.B.S. from the University of Wisconsin-Madison in Risk Management and Insurance, and Accounting Information Systems. He is a Certified Public Accountant in the states of Illinois and Wisconsin.

3

Objectives

Develop an understanding of opportunities for Compliance, ERM, and Audit function collaboration.

Discuss opportunities for implementing technology throughout compliance functions based on the level of compliance program maturity and technical capabilities

Explore the latest trends in risk and compliance with the results of the 2020 PwC Global Risk Study

4

Compliance
Audit and ERM Collaboration

5

5

“

49%

Organizations whose, risk, internal audit, compliance, and cybersecurity, teams are not working together to develop a common view of risks and threats across the organization.

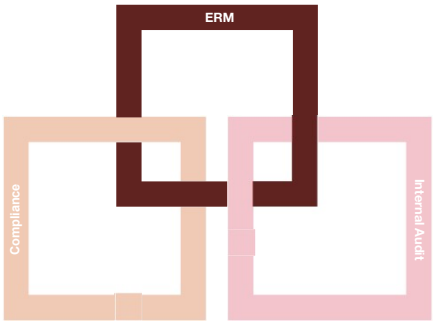
Source: PwC 2020 Global Risk Study

PwC

6

Defining Roles and Giving Autonomy

Under an integrated risk management model, each risk function still maintains its autonomy and unique responsibilities. However, functions work together to define a common set of key risks, use similar metrics and definitions when assessing and evaluating these risks, and develop coordinated project plans to maximize risk coverage.



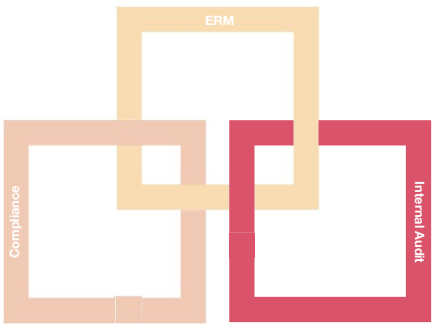
Characteristics

ERM takes a broad, strategic approach to managing risk at all levels of an organization and is generally responsible for providing risk management structure and oversight to the business. ERM programs often function as standard setters for risk management activities and leave much of the process implementation to business functions.

Objectives

- Provide timely and comprehensive risk reports to business decision-makers.
- Leverage existing processes and personnel to monitor and report risks.
- Provide uniform and sustainable risk management processes and a common risk language.
- Keep risk profiles and risk plans up-to-date.
- Encourage open and cross-functional discussions of top risks and business issues.
- Integrate risk information with planning, compliance and other business activities.
- Reinforce accountability for risk management by risk owners.

Defining Roles and Giving Autonomy



Characteristics

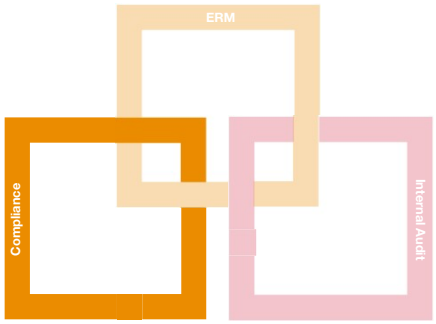
Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.[1]

Objectives

- Using a risk based approach, identify business units or processes to include in scope for the projects on the annual audit plan.
- Assess the design and operating effectiveness of the in-scope process and controls, through inquiry, documentation review, and sample testing.
- Identify gaps and make recommendations where weaknesses or inefficiencies are observed.
- Internal audit projects can be a mix of traditional audits, business process reviews, and maturity assessments.
- After a review is complete, Internal Audit will follow-up on the remediation status of identified observations.

[1] Definition of Internal Audit, *Institute of Internal Auditors*

Defining Roles and Giving Autonomy



Characteristics

Compliance programs help institutions and their employees conduct operations and activities ethically and in line with internal policies as well as laws and other external regulations. Effective compliance programs must be tailored to the organization and its goals, and must be dynamic enough to adapt to a changing environment.

Objectives

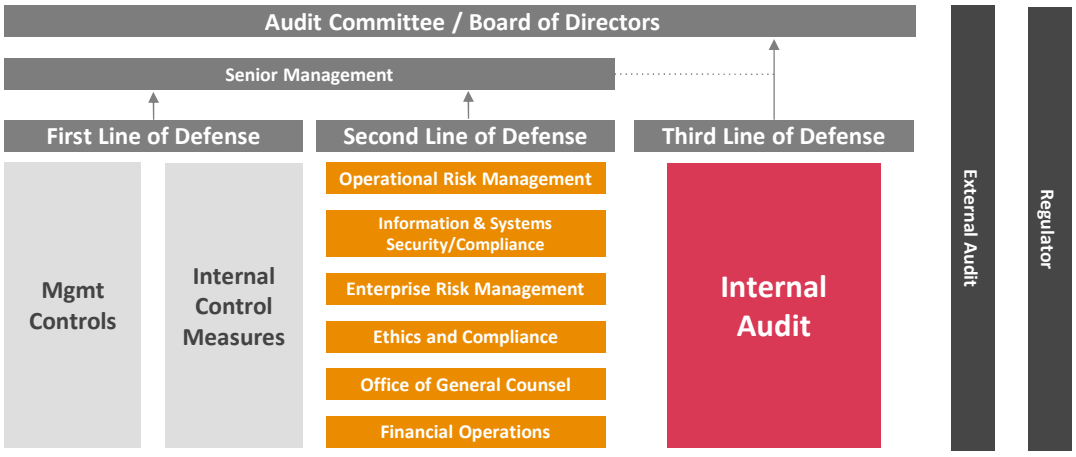
- An effective compliance program strives to reduce the likelihood of regulatory non-compliance and criminal conduct in an organization and helps lessen the negative organizational impact should these activities occur.
- Programs should maintain autonomy with direct reporting lines to the Board and senior management.
- Compliance programs help protect organizations in a complex and dynamic ethical and regulatory environment. Failures can pose significant reputational and financial risks.
- A strong program can enable an organization to confidently identify risks and seize new opportunities.

SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

9

The Three Lines of Defense



SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

10

Collaborative Risk Assessment

A collaborative approach to the risk assessment can help promote integrated risk management by creating a consistent understanding of the current state, a shared risk universe and ranking, and can also help lay the groundwork for coordinated audit, ERM, and compliance plans.

1

Create a unified understanding of the current state, including key initiatives and areas of stakeholder concern. Combining interviews can increase stakeholder satisfaction and reduce interview fatigue.

2

Work together between functions to identify risks and build a common risk universe. Audit, Compliance, and ERM can also collaborate on assessing the likelihood and impact of the identified risks and developing a common set of risk themes.

3

Map projects to the identified risk themes, selecting projects strategically to provide the broadest and most effective risk coverage. When identifying projects, consider the role of each function and which approach would best address the scope of the project.

11

Coordinating risk management efforts

As annual plans are developed, risk and control focused functions should work together to identify projects. This helps maximize coverage of the identified risk areas while minimizing duplicative efforts.

	Second Line of Defense		Third Line of Defense
Risk Theme	**Compliance**	**ERM**	**Internal Audit**
Academics	**No Planned Activities**	**No Planned Activities**	• Admissions Assessment • Academic Unit General Controls Review
External Forces / Regulatory Environment	• Title IX Changes • Higher Education Act • Accreditation	• Foreign Influence	**No Planned Activities**
Research	• Foreign Influence and Restricted Entities	• Research Misconduct	• Office of Sponsored Research Audit

12

Post Risk Assessment

The risk assessment should be a living document, with audit, ERM, and compliance functions regularly working together to make updates as University initiatives and the overall risk environment change.

Information Sharing

Internal Audit, Compliance, and ERM should continue to engage in **information sharing** after the risk assessment is complete. This can be done through **periodic cross-functional meetings** or the use of a **GRC system.** The three functions should also **meet periodically** with key **management** stakeholders (e.g., IT, HR leadership) to **stay abreast to management concerns** and changes in the risk environment.

Dynamic Plan

Changes in the risk environment mean changes to the risk universe, reflecting current and emerging risks facing the organization. This includes capturing changes in the external environment and business model that may impede an organization's ability to achieve its objectives. As such, the audit, ERM, and compliance plans were also designed to be dynamic, **incorporating ad hoc projects** to address changing risks and management requests.

Other Tactics to Encourage Collaboration

Focus on the basics

Develop a Timeline

Develop a timeline for rolling out integrated ERM efforts, including taking a phased approach. If appropriate, take a strategic break from regular meetings with ERM stakeholders in order to internally review the program and define strategic objectives.

Communication

Internal Audit, Compliance, and ERM should communicate the vision of of integrated ERM to University stakeholders in a meaningful and accessible way, particularly during periods of change.

Work across a decentralized environment

Working cross functionally to embed the Internal Audit, Compliance, and ERM functions vision, strategy, and principles into the organization's culture and day to day operations.

Know the Institution

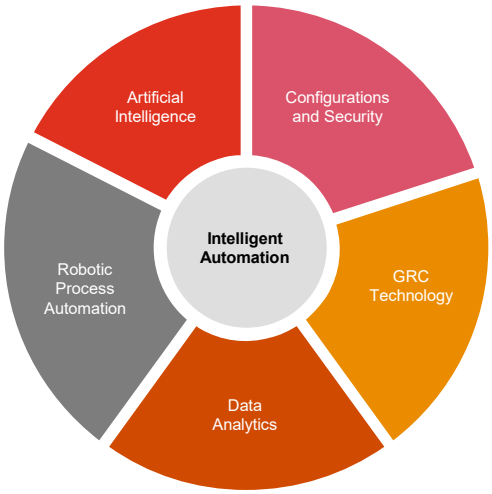
Have a deep understanding of the Institution and its strategic objectives, in order to provide practical, achievable guidance, foster meaningful relationships, and build and sustain trust.

Technology Trends in Compliance

15

The Promise of Intelligent Automation

- Organizations must control and monitor a complex technology environment comprised of powerful applications, interfaces and processes that are increasingly being automated.
- Key business processes and strategic decisions are being made in these new technology environments. Knowing when, and how, to best use automation to protect and enhance the business can deliver undiscovered opportunities.
- As companies move to become digitally integrated, end-to-end enterprises, more risks are emerging from a broader set of ever-changing rules.
- These moves are creating digitally efficient operations and closer customer and stakeholder relationships but they are also driving up the complexity of the technology landscape.

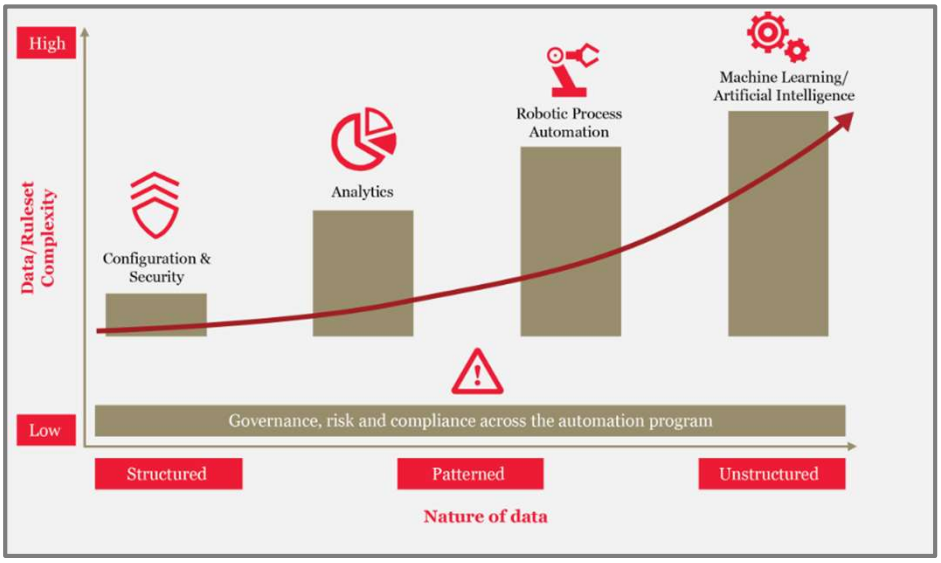


SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

16

The Automation Journey



SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

17

Configurations and Security

These two are considered together because security is technically a form of configuration within business applications. There are often a number of opportunities for companies to automate controls using system configurations and security available in the applications themselves.

Controls automation is a key aspect of managing internal controls, and can bring down the overall cost of compliance. Some examples of this include:

- System workflow to create user accounts based on defined delegation of authority matrices.
- Identity access management system can automate the access revocation based on the last working day.
- Changes to any system can be routed through a system workflow which will ensure that appropriate approvals and testing is done prior to implementing the change.

SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

18

GRC Technology Tools

Disparate Technologies
When each of the risk functions still uses several different tools and technologies, it can be time-consuming and inefficient to consolidate risk insight and reporting, as all of the information from each of the risk functions does not connect into a single platform. Technology investments can be difficult for any one risk function to swallow, but when functions consolidate their business case for investment, the value proposition gets much stronger.

GRC Tool
A governance, risk, and compliance (GRC) technology tool(s) is a key enabler of this foundation and supports the creation of a robust and sustainable risk management model. GRC technology can help support a three lines of defense and integrated ERM strategy by helping to break down individual risk function silos, facilitating the sharing of information, confirming appropriate risk coverage across the organization and supporting overall GRC and operational efficiency.

Goals for GRC:
- GRC technology can be the stimulus for creating a common framework for risk management, including establishing common processes, control descriptions and risk ratings
- While each line of defense has specific roles and responsibilities with regard to the management of risks and controls, GRC technology helps to eliminate duplication of effort and increase efficiency in testing, monitoring and oversight.
- Through the technology enabled mapping of roles and responsibilities to the various components of a company's risk universe, management has an effective process to ensure that there is appropriate coverage of the risks

Risk and Compliance Analytics

Given the potential disparity of systems and transactions flowing across the digital environment, the use of advanced data analytics to gain insights for compliance has been a fast growing trend. Data analytics effectively enables compliance, risk, and audit professionals to proactively detect and continuously monitor potential issues in real time.

According to the PwC State of Compliance study, approximately two-thirds of compliance industry leaders use technology to monitor employees compliance with ethics and compliance related policies and procedures.

Executing on technology-enabled compliance monitoring requires a cross-functional approach. Compliance executives have to better understand the available data and data sources within their organizations, partnering with other teams like IT, HR, finance, and procurement. Analytics can be used to actively monitor and report on compliance across many areas, including:
- System configurations
- Security and security activity
- Business transactions
- Master data activities

Benefits of risk and compliance analytics include the ability to identify outliers and respond to issues in real time, the minimization of internal compliance risk, and the ability for closer collaboration with the business.

Robotic Process Automation (RPA)

RPA allows for automation of manual activities. A bot is programmed to do a series of repetitive steps, make comparisons and provide output in the form of pass/fail for compliance. RPA has made leaps and bounds from when it first came into existence. By automating tasks that are mundane and need little or no human involvement, businesses can allow workers to focus on critical functions, increase productivity, and minimize errors. As RPA momentum increases, compliance and audit functions can keep pace by helping the company understand and control RPA risks and by embracing RPA within their own organization.

Overseeing Risks and Controls

Compliance functions need to understand how the organization is using RPA and how that impacts its risk profile by thinking broadly about exposure across multiple categories of risk.

Establishing governance of RPA and relevant controls up front should help effectively mitigate risks. By embedding governance, risk management, and controls into the enterprise's mobilization and deployment of RPA, organizations can catch issues before they arise.

Deploying RPA in Compliance

Audit and compliance functions are well suited to identify and recommend controls that are well suited for automation. Additionally, automating controls testing may be another opportunity.

RPA can also be used for administrative tasks such as open issue follow-up, automating reporting and dashboard activities, and evaluating data quality in any system.

SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

21

Robotic Process Automation (RPA)

Higher Education Examples

RPA is being utilized in a variety of ways including accounts payable processing, posting journal entries, assembling reports and dashboards, inventory management, and the financial closing process.

Supporting Financial Close
The financial close and reporting process encompasses many tasks and processes—from closing out subledgers to creating and delivering financial filings to regulatory bodies. The process can require posting data from sources such as spreadsheets to subledgers, a tedious undertaking that RPA can facilitate.

Data Extraction
Departments and divisions record transactions, which need to be consolidated and reconciled. A robot can gather and consolidate transactions and reconcile them in an ERP system.

Data Management
Aggregating and analyzing financial and operational performance is a business-critical function. A robot can take this job on and not only lighten the time-sensitive burden for employees gathering data, but also benefit executives who need information to gain insight into the business.

Blockchain
Blockchain may change the way higher education interacts with third-parties. Blockchain is a distributed ledger, in which a change automatically gets registered across the entire chain. In the future, the Federal Government may use blockchain to manage grants, student aid and federal research funding. All the requirements of the 'contract' would be built into the blockchain and monitored for compliance.

SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

22

Artificial Intelligence / Machine Learning

Companies or industries which implement AI will be powered with the ability to analyze data across multiple functionalities, fraud detection and high-class customer relationship management. AI are built around a learning model to make decisions that are not explicitly programmed and bring an additional level of analysis of complex data.

Machine learning is a subset of AI that utilizes algorithms and computer power to sharpen the judgments organizations make about voluminous and disparate data. Machine learning helps optimize the mix between humans and machines in a process that "learns" as it goes along. As the predictive model gets continuously "tuned," its effectiveness increases.

- **Supervised Learning**: Takes real world examples provided by humans and detects patterns similar to those examples.
- **Unsupervised Learning:** Infers patterns directly from data without the reliance on any examples.

Machine learning holds tremendous promise in addressing bribery and corruption risk as well— offering compliance and risk teams a significant boost by processing, identifying and tiering potential anomalies that may be hiding in their data. It can scour transactional data and communications for traditional corruption markers— duplicate payments, improper relationships, offshore bank accounts —and prioritize accordingly.

23

PwC 2020 Global Risk Study Results

24

Global Risk Study

PwC's 2020 Global Risk Study surfaced a growing imperative for better collaboration between risk functions (risk management, compliance, internal audit and other risk functions). As organizations embrace the fourth industrial revolution (4IR), risk functions need to be active participants, helping to achieve and protect the value envisioned.

1. Set a Collaborative Tone

Set a collaborative tone by starting with the board, senior executives and risk function executives and have a risk management program governance in place to make sure they all have a clear understanding and collaboration of business risks. Compliance functions can do this by:

- Providing a consolidated view of the organization's risk profile, including a common risk assessment, issue management, and key risk indicator framework, in order to aggregate and report on risk in a comprehensive and coordinated manner.
- The board, senior executives and risk executives must see eye to eye on risk priorities across the entire organization and risk landscape. Consolidated reporting facilitates that process because a holistic view of risk enables company leaders to have robust discussions and make informed decisions on where the company should focus its efforts.
- An organization should ensure that an enterprise-wide risk appetite is well-defined, understood across the leadership team, and relied on throughout the organization to make collaborative, intentional, and unified trade-off decisions.
- Risk functions should help monitor risk to the agreed-upon appetite and communicate whatever actions have to be taken when events occur that could increase risk beyond the organization's risk appetite.

27%

Risk functions that set an integrated tone for risk management through well defined governance.

2. Lay a Common Foundation

Executives need to collaborate and build a common risk language, and share data, analytics and technologies so that risk functions are looking at a single source of data and are measuring risk indicators in the same way as one another and are producing more-powerful risk insight.

- A common risk taxonomy is the dictionary that helps everyone think about, prioritize, and communicate risks in the same way as one another.
- Risk functions many use many different tools and technologies, and it can be time consuming and inefficient when these technologies do not integrate. Developing insights and reporting can be made easier by sharing a single platform across risk functions (e.g., a GRC tool).
- There exists an abundance of data both inside and outside organizations from which to draw more-intelligent risk insight. Risk functions should embed themselves in their organization's enterprise-wide data strategies and data asset development efforts to make their collective data and functional requirements known.

33%

Organizations that say they have the right technology and tools to anticipate, monitor, and manage risk.

SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

27

3. Optimize the Parts

Risk functions have to be able to confidently take advantage of one another's work so as to eliminate gaps in risk coverage and increase efficiency. A focus on the optimization of each function builds the levels of confidence in one another—and on the parts of stakeholders—that will move all risk functions toward more-integrated approaches and maximize risk coverage and minimize blindspots.

- As data becomes more available and quality increases, risk functions can more easily rely on that data, which sets the stage for automation. Several risk functions in the study (but not the majority) are using robotic process automation to automate data retrieval, freeing up time for more strategic and complex thinking.
- Once a common foundation is in place, team members will be able to look at risk data differently and thereby make more-complex judgments and quick adjustments. Compliance functions will need to invest in digital upskilling and building critical analysis skills.
- Risk functions should work together to provide leadership with a combined, holistic perspective of risks and opportunities. This can help better demonstrate the magnitude of an issue and build a more compelling case for action from leadership..

51%

Risk functions that are consistently following one operating model for the division of responsibilities among them.

SCCE: Harmonizing Compliance IA, and ERM
PwC

June 2020

28

Thank You.

www.pwc.com

29