When Worlds Collide

Paul Phillips, CISA, CISM, MBA
WHEN WORLDS COLLIDE

• Shake hands and smile

• “Hello, my name is ________________.”

• “Welcome to AfricaCACs 2019”
WHEN WORLDS COLLIDE

WHO AM I?

• Technical Research Manager for ISACA International

• Bachelor degree in Accounting and an MBA with concentration in both Management and MIS.

• Certified Information Systems Auditor and a Certified Information Security Manager.

• Part-time instructor for various universities and institutions of higher learning organizations for 20 years.

• Former member of the board of the ISACA Chicago Chapter

• Former IT Audit Manager and IT Director
WHEN WORLDS COLLIDE

COLLIDING and EVOLVING WORLDS

• Technology has long been integral to the success of any organization, but as the range of business applications and the pace of innovation has increased, so has the risks.

• It is vital that risk management and information technology professionals communicate with each other on a regular basis to ensure that their organizations are getting the most value out of their technological investment.

• It seems like the two groups are speaking a different language—that is, if they even speak at all.
WHEN WORLDS COLLIDE

COLLIDING and EVOLVING WORLDS

• ISACA and RIMS have set out to bridge this gap by developing a joint report to help all parties collaborate and communicate more effectively to bring more value to their organizations.

• To help enhance the abilities of risk management and information technology professionals to speak the same language as they endeavor to incorporate the benefits and uncertainties associated with data and technology into the organization’s overall strategy in order to create value and counter-balance unwanted risks and outcomes.
When Worlds Collide

PART 1:
IT AND RISK MANAGEMENT WORLDS COLLIDE

• Once limited to the realm of digital assets, such as networks and servers, the information technology (IT) function has increasingly evolved from managing hard assets as a shared service to serving as the backbone of the worldwide economy. As such, digital enterprise strategy—the IT architecture and governance of an organization—has become a strategic imperative.

• Risk management has evolved as well from protecting the balance sheet through mitigation controls and insurance purchases to informing strategic and operational decisions and enhancing the viability of organizations within their respective ecosystems.

• In the past, these worlds existed in separate environments, but a number of factors are now bringing them together...

BUT WHAT HAS KEPT THEM APART?
When Worlds Collide

PART 1:
IT AND RISK MANAGEMENT WORLDS COLLIDE

• Lack of Strategy
  • Unknown, unclear, un-supported, non-existent

• Unclear roles and responsibilities
  • Who is responsible for what?

• Others?
When Worlds Collide

Strategy

- A plan of action designed to achieve a long-term goal or goals
- Master plan
- Grand design
- Game plan
- Plan of action
- Policy, proposed action, scheme, blueprint, program, procedure, approach, schedule?

- Not really
When Worlds Collide

Strategy

Corporate Strategy

IT Strategy

Risk Management Strategy

Other Functional Units
When Worlds Collide
Strategic Links

- Strategy
- Policies
- Methodology
- Procedures
- Projects
- Processes
When Worlds Collide
Strategic Considerations

- Cost
- Regulations
- Competitors
- Current State
- Culture
- Risks
Collaboration between IT and risk management professionals can add value to an organization in a number of ways, including through processes and sub-processes:

- Coordinated procurement and contract review, resulting in more favorable terms and conditions, service level agreements, and coverage terms
- Better incident response that enhances reputational protection
- Improved information protection through records and data management training
- **Controls** assurance that provides validation from multiple sources that controls are operating as intended
• IT and risk management professionals both employ various tools and strategies to help them manage risks.

• Although the methodologies used by the two groups differ, they are generally designed to achieve similar results.

• By integrating these frameworks, roles and methods, IT and risk management professionals can better coordinate their efforts to address threats and create value.
When Worlds Collide

PART 3
INTEGRATING FRAMEWORKS, ROLES AND METHODS

Integrating Frameworks

• There are several frameworks available to facilitate the integration of Risk and IT:
  
  • ITIL
  
  • COBIT
  
  • ISO
  
  • NIST
When Worlds Collide
Three Line of Defense Model - Roles

Board of Directors

First Line of Defense
Management
Risk Ownership

Second Line of Defense
Risk Management
Risk Assessment & Response & Control

Third Line of Defense
Audit
Risk & Control Assurance
When Worlds Collide

PART 3
INTEGRATING FRAMEWORKS, ROLES AND METHODS

Integrating Roles

- Successful organizations do not create a separate “risk governance” structure for their risk management practices. Rather, they integrate risk management into existing governance arrangements based on process, framework and technical design.

- In the ISO 31000 standard on risk management, “The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making. This requires support from stakeholders, particularly top management.”
Integrating Methods of Assessment

- Collaboration and communications processes in IT security are similar to those used in enterprise risk management, but with different, though complementary, objectives and different terminology.
- IT security processes typically tend to support an asset-based, control-centric approach to risk reduction, while enterprise risk management processes generally support management of both downside and upside risk associated with uncertainty and volatility in achieving business objectives.
- Most organizations already have controls established against commonly and widely understood risk, such as business disruption, environmental and execution failure, among others.
- What tends to be missing is a set of common methods of assessment and conducting root cause analyses that tie control actions to both the risk appetite of the organization and to its strategic objectives.
Integrating Roles

• Accountability for managing risk, at times referenced as “risk ownership,” is an important aspect of the technical design of risk governance. For example, there should be clear understanding of roles, responsibilities and accountability within the governance structure.

• Cyber risk management falls naturally into both strategic and operational risks due to the ubiquitous use of technology. At times, strategic and operational risks become the oversight responsibility of the entire board, rather than delegated to a board committee.
CONCLUSION

Many organizations struggle to align risk functions in support of common interests because of communication difficulties between the different functions. Lacking a common taxonomy, professionals in information security and risk management may not realize that they are performing substantially similar activities with different areas of focus.

For instance, risk identification in an information security context typically begins with identification and valuation of information assets and proceeds from there to identifying possible threats and assessing vulnerabilities.

In contrast, risk management professionals may use business processes as a starting point for identifying risk, beginning with delineation of objectives and then seeking to reduce the uncertainty associated with attaining them.
Developing and communicating common goals and objectives by creating a strategy and creating clear roles and responsibilities can serve as a strong bridge to unite the risk management and information technology functions together, resulting in significant value creation for organizations.
When Worlds Collide

CONCLUSION

QUIZ ASSESSMENT

• What is the strategic direction of the enterprise?
• Does it exist? Is it documented?
• Has it been communicated?
• Is it clear, concise, and understandable?
• Are there clear roles and responsibilities?
• Is senior and middle management clear on how they can support the strategy?
• Does senior and middle management support the strategy?
• Does the functional strategies support the corporate strategy?
• Does the policy, processes (including performance management), and procedures support the functional strategy?
• Does actual practice align with the policies?