KPMG

cutting through complexity

Institute of Internal Auditors (IIA) Tallahassee Chapter

Information Security, why should you care?

August 23, 2012

Dan Manley

Managing Director

KPMG LLP

Is Security Important?

Please raise your hand if….

- You locked a door this morning?
  - House
  - Car
  - Office

- You use a fire proof safe or lock box to protect important documents?

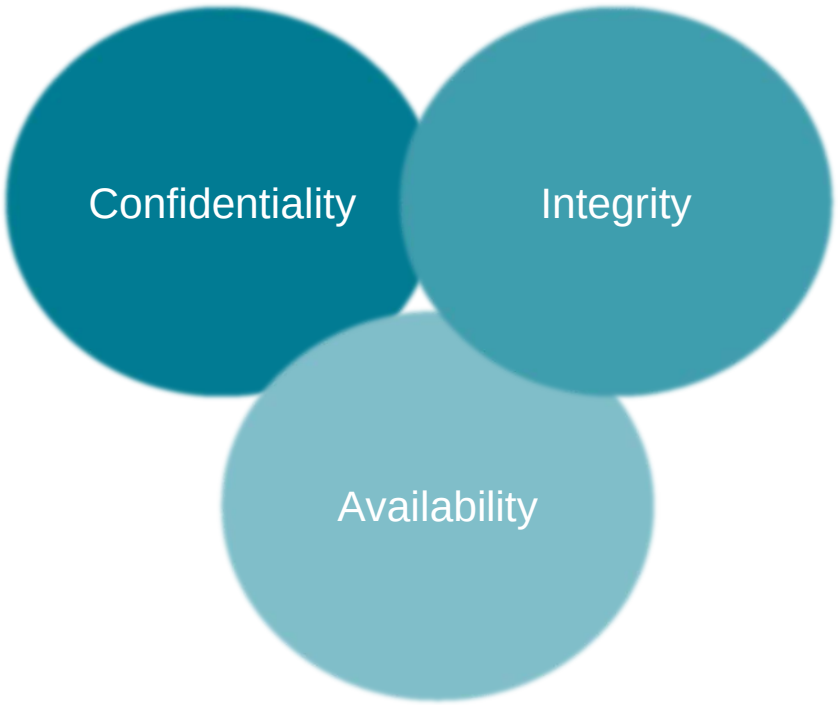
- You have a password or PIN that you keep to yourself?

If you raised your hand, you already have an appreciation for why Information Security is important!

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. 53490CHI

Information Security in simple terms

Information Security is about the **protection of information assets (systems and data)** in order to provide **trust and confidence.**



- **Confidentiality:** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"
- **Integrity:** "Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity…"
- **Availability:** "Ensuring timely and reliable access to and use of information…"

Source: FISMA

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 53490CHI

Business Drivers

Legal and Regulatory Obligations

- HIPAA and HITECH
- GLBA and FFIEC
- PCI-DSS
- Sarbanes-Oxley
- FISMA
- FTC Enforcements
- FIPS
- Others

Market and Operational Considerations

- Dynamic business models
  - M&A , divestiture and consolidation
  - Distributed Operations
  - Remote / Mobile Workforce
- Increasing Consumer Expectations
  - Services
  - Availability
  - Privacy
- Evolving threats (e.g., cybercrime)

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. 53490CHI

What is the “problem statement” to solve?

Assets

- Increasing volume and value
- Dynamic definition of assets (Intellectual Property)

Threats

- Rapidly evolving
- Many are clearly malicious
- Some are associated with innovation or transformation

Resources

- Human Capital
- Discretionary spend
- Drives need for efficiency

Gross Risk

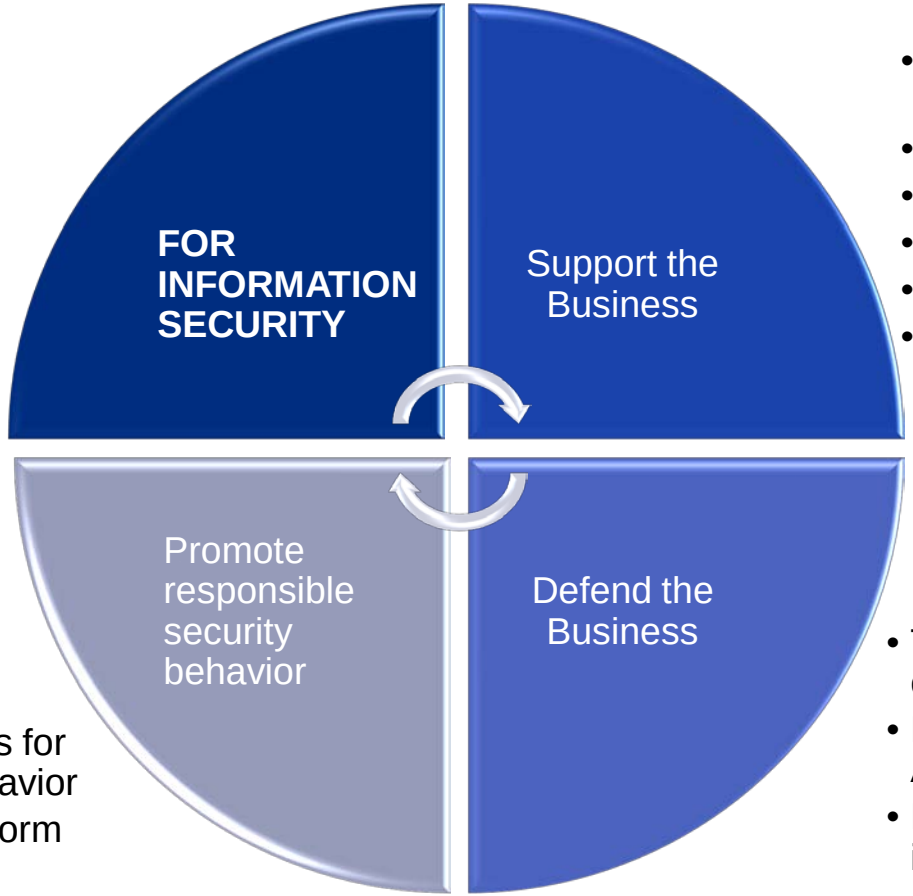
- Across multiple dimensions
- Interdependent

Residual Risk

Obviously depends on the design and operation of key controls

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. 53490CHI

Security Principles



- Integrate security into business processes
- Work to drive value
- Meet statutory obligation
- Manage information risks
- Assess and analyze threats
- Build reliable and robust systems

- Set expectations for appropriate behavior
- Educate and Inform
- Trust but Verify

- Treat risk in consistent and effective manner
- Leverage Risk Based Approach
- Protect sensitive data and information
- Improve security effectiveness

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. 53490CHI

Security Environment

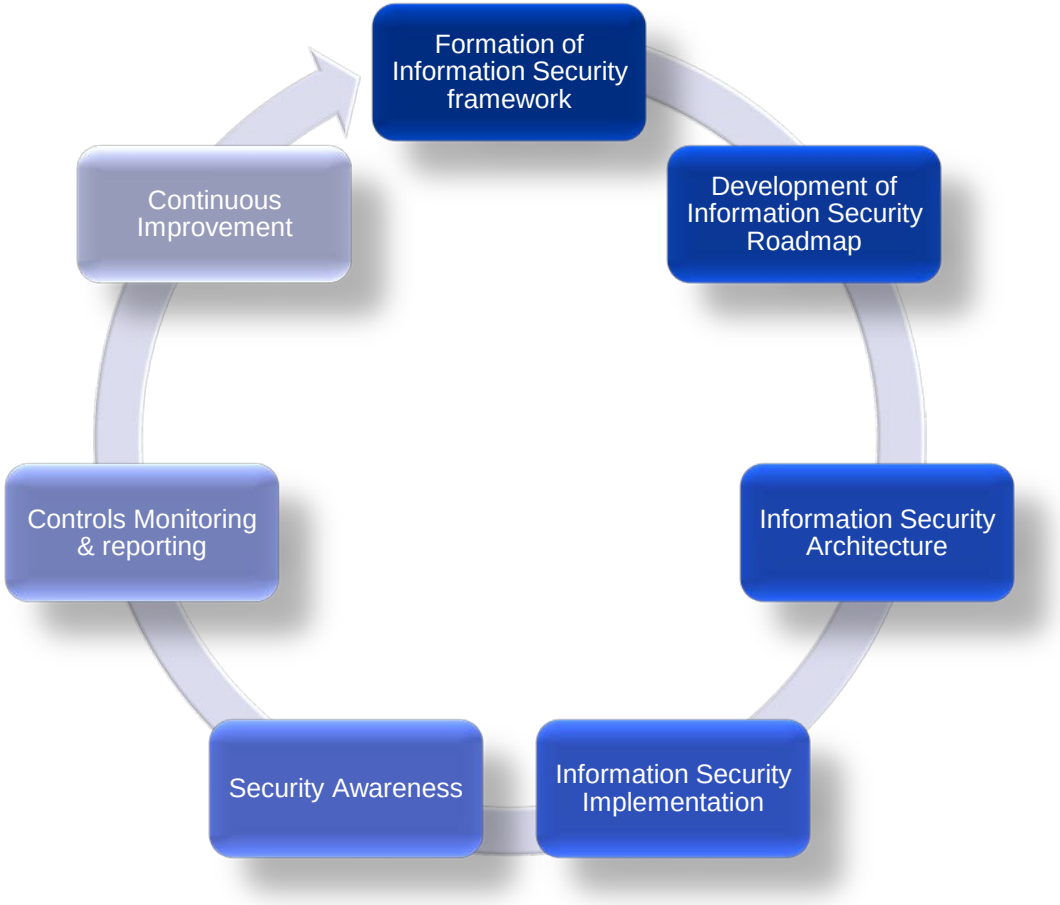
© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 53490CHI

Transforming Information Security

In building a robust Information Security Program, it is important to leverage a structured and disciplined approach, which aligns to the business and addresses a holistic set of controls across the dimensions of people, process and technology

Industry Frameworks:

- ISO
- CobIT
- NIST
- ITIL
- Cloud (still developing)
- Others…



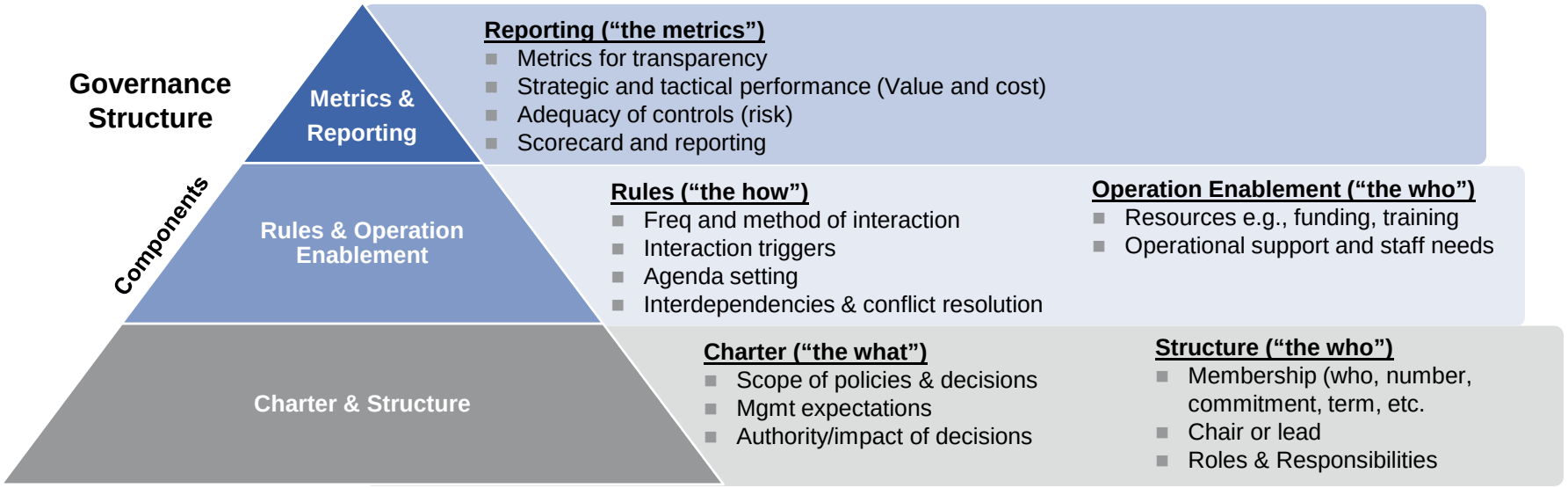
© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 53490CHI

Importance of Information Security Governance

Effective Governance structures establish structure and discipline that help an organization recognize their desired value.

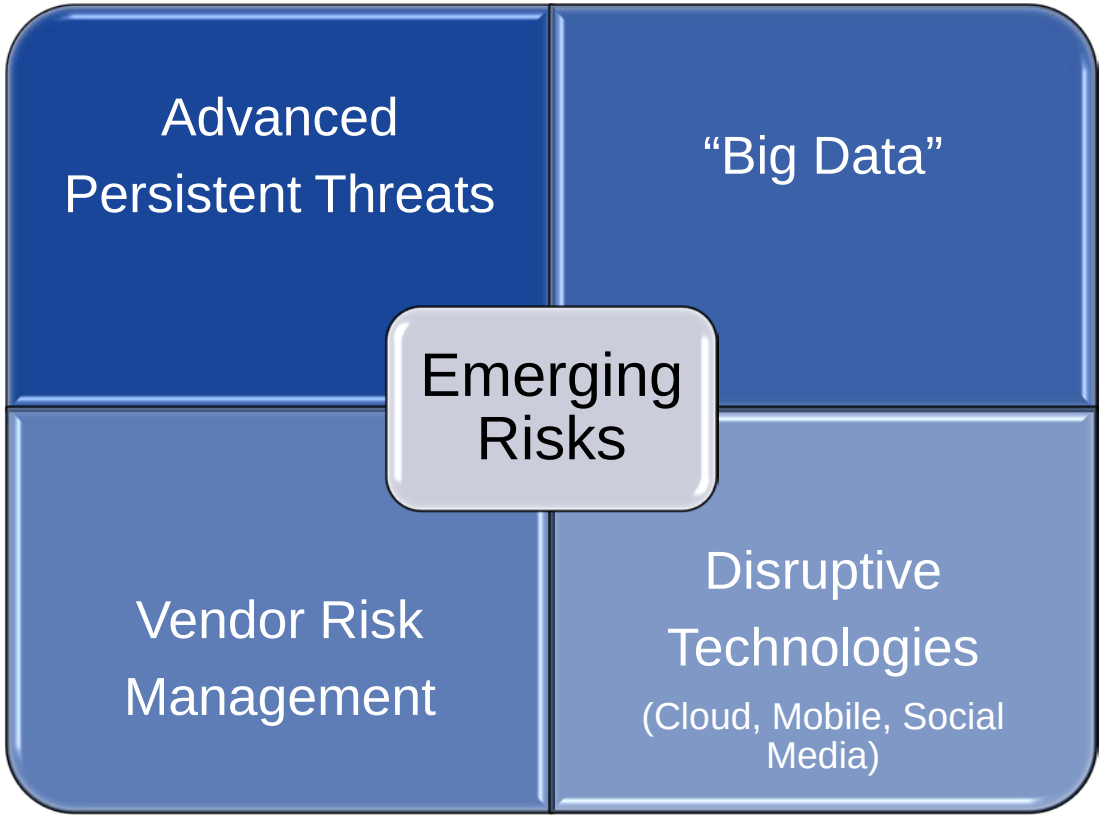
The purpose of an Enterprise Information Security Governance Structure is to:

- Enable leadership to better understand its Information Security risks and manage them in a manner consistent with the organization's risk appetite
- Promote a sound control environment, complying with applicable laws and regulations and in line with the organization's risk management framework.



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 53490CHI

Emerging Risks



© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 53490CHI

Conclusion

- **Key Takeaways**
  - Acknowledge the importance of Information Security, but look for the value it can provide to the Business and Organization (i.e., Trust and Confidence)
  - Look for a disciplined structure in how Information Security is Managed
    - Risk Based
    - Balanced
    - Well governed
  - Use Industry Standards as an accelerator to build, operate and audit Information Security

- **Questions?**

- **Thank you!**

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 53490CHI

Contact Information

Dan Manley
Advisory Managing Director
Information Protection & Business Resiliency

KPMG LLP
550 South Tryon Street
Duke Energy Center
Charlotte, NC 28202-4214

Tel 704.371-8217
Fax 704.973.0631
Cell 704.560.6127

dmanley@kpmg.com

KPMG LLP is a U.S. limited liability partnership.

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. 53490CHI