

# Information Security is a Business Issue

IRENE CORPUZ

MSC IT, ISO27001 LEAD AUDITOR & LEAD IMPLEMENTER, ITIL, PMP, EFQM, CKM

# Disclaimer

- ▶ I do not speak for or on behalf of the organization that I work with, nor for any non-profit organization to which I serve as Adviser, Officer, or member.



Let me ask you a few questions...

# What do organization secure in the first place?

- ▶ Assets
- ▶ Data
- ▶ Customers and stakeholders' information
- ▶ Integrity
- ▶ Systems (the key to delivering your service)

Not securing them puts your organization's  
REPUTATION at RISK



Is your organization  
making **Risk-Aware**  
decisions?

# Do you do a risk-based approach to information security?

- ▶ IS should be a key element for any organization's Risk management strategy
- ▶ Hacktivists increase monetization of organized crime
- ▶ Information Security is far more important than just technology
- ▶ Public sector – CIS
- ▶ Private organizations – business requirement

# How do you prioritize?

- ▶ Put solutions that are right, the solutions that address the problems of the business
- ▶ Understand what the business wants, instead of imposing solutions.
- ▶ Address the business risk which are people and process
- ▶ A governance, risk and compliance (GRC) benchmark research report found that **68%** of organizations defined and documented their IT security authorization procedures based on processes agreed with the business function.
- ▶ BUT only **just over a third** of IT security experts believed that the business understands security - and this highlights a potentially serious issue.

# How about the key resource to IS?

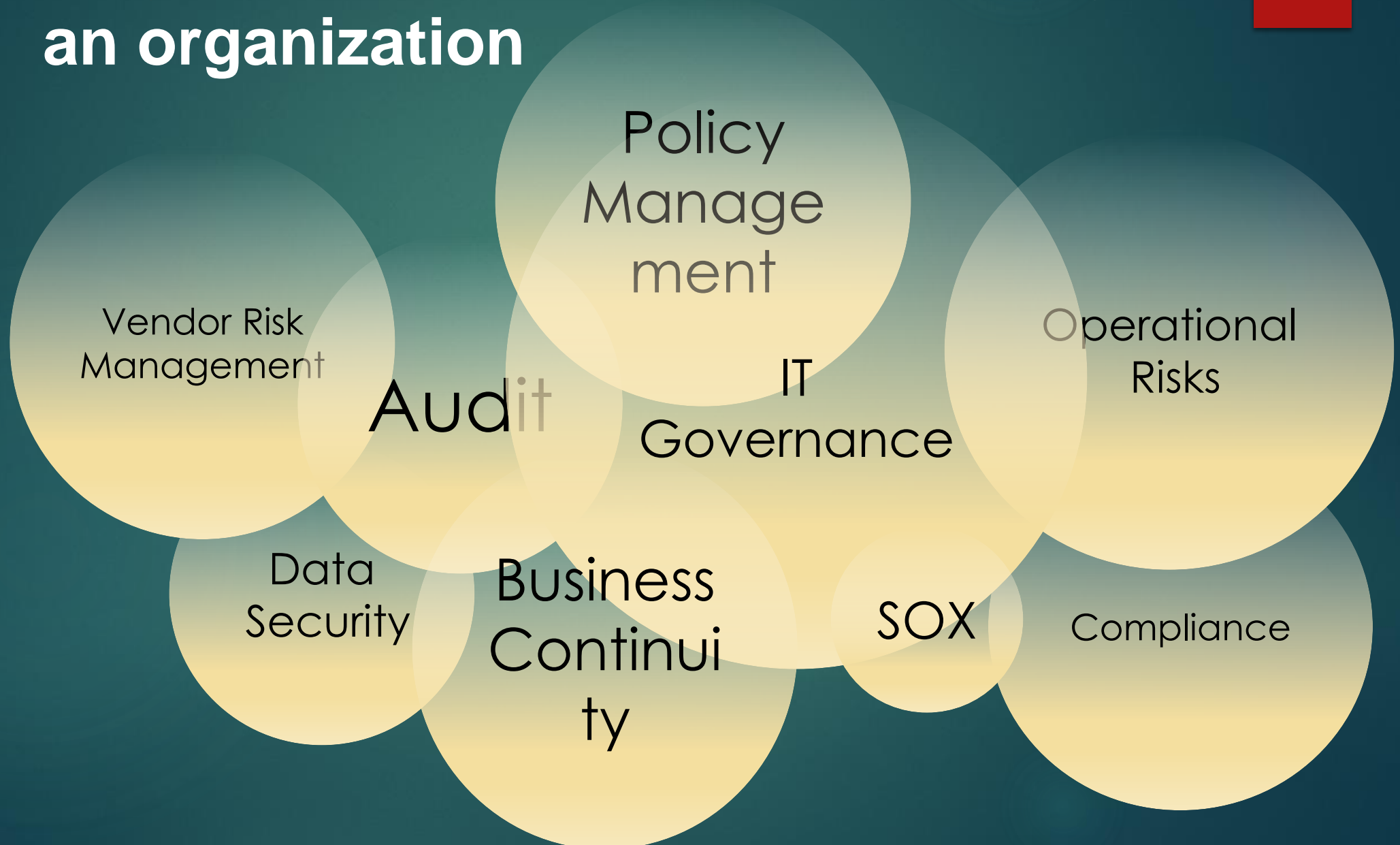
- ▶ Risk Management should come from the business – not to understand the technology, but to understand the business
- ▶ CISO should have a technical background





**Governance, Risk &  
Compliance (GRC) as  
embedded in every  
organization allows business  
managers and leader to make  
a risk-aware decision**

# Why? Because GRC Impacts every aspect of an organization



# What do you report to the Board?

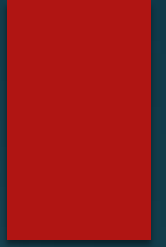
## Regulation:

Do you comply with regulatory requirements?

Are we acting appropriately with regard to cybersecurity for our customers and shareholders?

Company liability: If the organization performs poorly in cybersecurity, how does it affect the overall business performance?

# Can you protect the organization from any security threats?



The CISO needs to be able to communicate that bad things can happen to your network or your data—but the damage can be minimized to acceptable level by taking the right steps.

# My last question...

- ▶ Did I even talk about technology at all?
- ▶ But after doing a risk-based approach, then technology will follow.

# THANK YOU



IRENE CORPUZ



@IRECORPUZ

# Reference:

- ▶ IBM Analytics (only on GRC)