



# Transforming Information Security to Information Risk Management

**Presented By:**

**John P. Pironti**

**CGEIT, CISA, CISM, CISSP, ISSAP, ISSMP**

**Chief Information Risk Strategist**

**Getronics**



John P. Pironti, CGEIT, CISA, CISM, CISSP, ISSAP, ISSMP  
Transforming Information Security to Information Risk management  
April 27, 2008



## Agenda

- Current State of Information Security
- Risk Management Versus Security
- Risk Management Program
- Final Thoughts

## Why Is Security So Difficult?

- Adversaries have extraordinary resources
- Adversaries need to master only one attack
- Defenders constrained by ethics and laws
- Defenders must serve business goals
- Defenders must win all the time



3

## Current State of Information Security

- Information security still too focused on technology
  - The widget will fix the problem
- Compliance driving most information security decisions and investments
  - Security by compliance
- Threat landscape changing to more focused and professionally oriented activities
- Too many chiefs with no real voice



4

## Risk Management Vs. Security

- Risk Management
  - Defines the areas which should be secured
    - Business Value
    - Business Impact
    - Compliance and Strategy
- Security Defines how to protect
  - Identifies Threats
  - Defines controls
  - Monitors effectiveness



5

## Evolution to Information Risk Management

- Too many chiefs, not enough Indians
- 360 Degree View of Risk
- Organization which provides realistic view of risk management
- Inputs from multiple stakeholders and business groups



6

## Risk Management Program

- Structured approach to enterprise risk management
- Provide decision makers with the best possible information to make decisions
- Consulting group within the enterprise



7

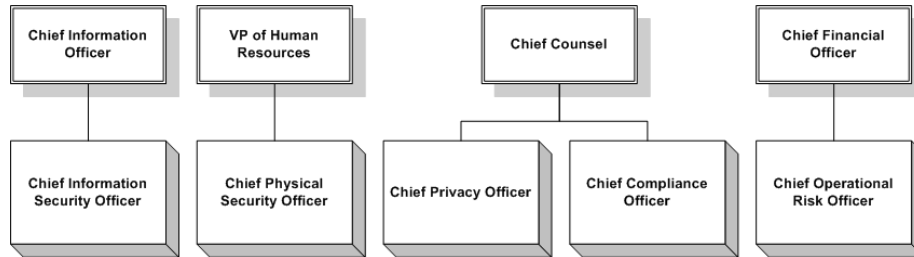
## Key Elements of a Risk Management Program

- Structured approach to risk management
  - Risk Program Framework
- Aggregation of multiple groups and departments
- Chief Risk Officer
  - Individual who has a seat at the boardroom table
- Provides information to decision makers
  - Does not make decisions for the business



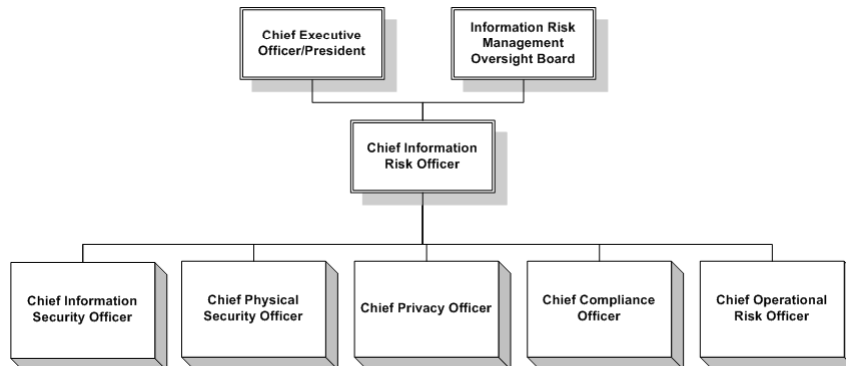
8

# Current State of Information Protection Organization Design



9

# Future State Risk Management Organization



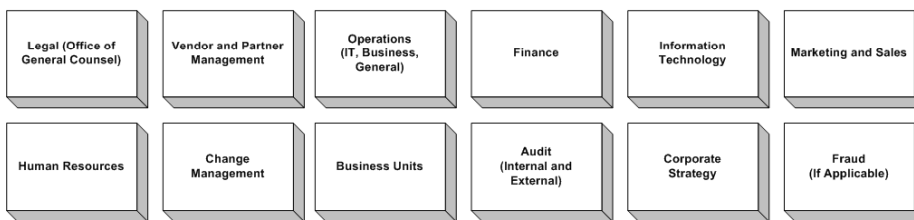
10

# Risk Program Framework

## Functional Elements



## Organizational Interactions



11

## Chief Risk Officer

- Responsible for all elements of the risk management program
- Reports meaningful data points to senior management
- Establishes risk level for organization
- Provides information to decision makers about risk of activity



12

## Information Security

- Identifies threat and vulnerability information about information infrastructure
  - Provides input for risk evaluation
- Defines and monitors controls related to identified threats and risks
- Consults with organization to educate community about threats and countermeasures



13

## Physical Security

- Identifies physical security threats
- Implements physical security controls
- Tracks physical security events and incidents
- Protects facilities and physical plant



14

## Compliance

- Identifies internal and external compliance requirements
  - Regulatory considerations
  - Audit standards
- Identifies gaps in current business processes
- Develops remediation plans to achieve compliance



15

## Privacy

- Identifies privacy requirements and considerations
  - Aligns to industry and organizational privacy requirements
- Defines privacy controls and requirements
- Provides risk officer with privacy risks associated with business processes



16

## Finance Risk

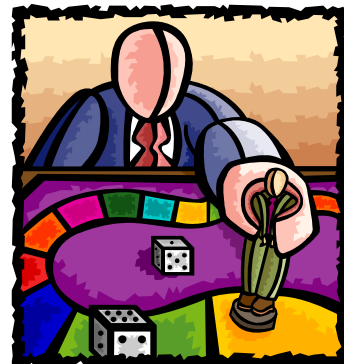
- Evaluates financial risks of business activities
  - Profit vs. Loss
- Defines financial boundaries and controls for business processes
- Identifies risk characteristics and variables



17

## Market and Strategy Risk

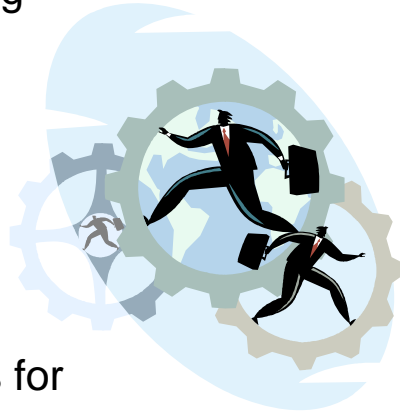
- Evaluates market and strategy risk considerations
  - How will this activity be perceived by outsiders?
- Evaluates strategy for soundness and potential positive and negative impacts
- Identifies control points for evaluation of strategy and market considerations



18

## Business Operation Risk

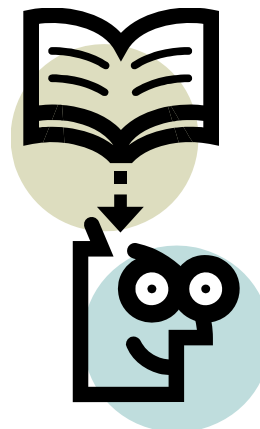
- Evaluates risk of carrying out business activities
  - Investment Strategies
  - Business process risks
  - Customer impacts
- Identifies controls for business processes
- Develops actuary tables for business impacting events
  - Business impact analysis



19

## Risk Methods, Practices, and Standards

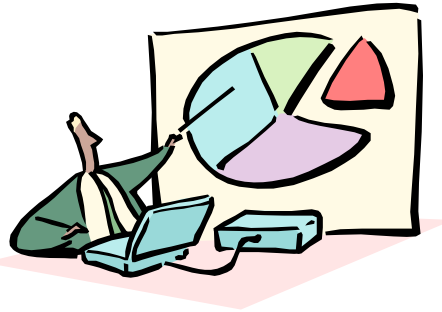
- Develops risk management methodologies, practices and standards
- Defines and implements tools and technologies to assist and automate risk evaluation
- Develops risk management policies and procedures
- Assists business process owners in establishing risk thresholds for business processes



20

## Key Performance Analysis and Effectiveness

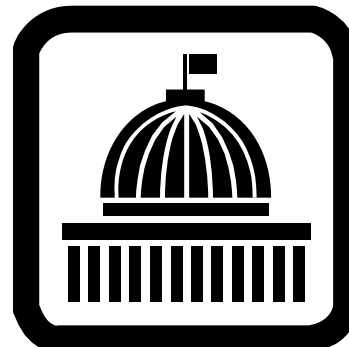
- Analyze Key Performance Indicator (KPI) results to identify trends and behaviors
- Monitor effectiveness of program and controls
  - Internal and External view
- Develop transformation plans to increase operational effectiveness
  - Technology, Process, Standards, and Procedures



21

## Strategy and Governance

- Create plan to mature program
- Ensure goals of program are aligned with the goals of the organization
- Define future requirements and assess current needs
- Establish control framework for all other program elements
- Monitor effectiveness of program
  - Internal and External Inputs
- Define future functional requirements and lifecycle of current requirements



22

## Risk Oversight Board

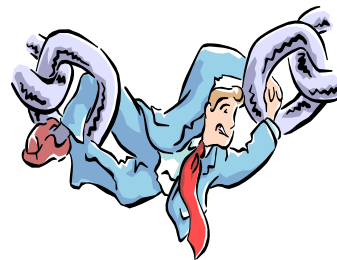
- Comprised of representatives from all aspects of organization
- Provide guidance and direction for program
- Ensure that program activities align with organizational goals
- Evaluates exception activities
  - Applications and Grants



23

## Organizational Interactions

- Provide communication channel risk organization and other elements of organization
  - Specific elements of organization which require direct interaction beyond general communication
- Provide feedback loops and check and balance capabilities
- Ensure appropriate communication and collaboration between risk program and organization
- Ensure risk management representation in key organizational activities



24

## Final Thoughts

- Current State of Information Security losing effectiveness in enterprise
- Information Security must evolve into Information Risk Management
  - Continue to provide value to organization
  - Business alignment
  - Provide information to decision makers to enable better decisions
- Structured governance approach essential to future success



## Thank You For Your Time!



**John P. Pironti**

**CGEIT, CISA, CISM, CISSP, ISSAP, ISSMP**

[John.pironti@getronics.com](mailto:John.pironti@getronics.com)

**01-978-625-6540**