SOFTWARE SECURITY ASSURANCE SUMMIT

September 12, 2011 | HP Protect at Gaylord National | Washington D.C.

A Business Process Approach to Managing Operational Risk and Information Security

Dennis Dickstein

presented by HP Enterprise Security

Flying Should Be Safe

Controls:

1. *Pilot (& Co-Pilot most of the time)* in airplane
2. *Lights & Signs* on runways
3. *Ground crew* providing direction before runway
4. *Controllers* talking to/watching aircraft from control tower

What happened to Comair flight 5191 in Lexington KY on Aug 27, 2006:

- Two runways: one short and one long (98% of operations) close to each other
- Construction forced passing over the short runway to get to the long runway
- Early morning, dark; lights not on the short runway
- One controller in tower; looked away to perform administrative tasks

The result:

- Flight took off short (wrong) runway
- 49 people killed (all but the co-pilot)

Surgery in Hospitals Should be Straightforward

Controls:

1. *Administrators* admit the patient and document the treatment
2. *Technicians* provide exact location for surgery
3. *Nurses* confirm technician notes; report patient issues
4. *Doctors* confirm all documentation and perform the surgery

What happened at Rhode Island Hospital in 2007:

- January patient: mark in wrong place; doctor operated on wrong side
- July patient: location not written on form; doctor operated on wrong side
- November patient: nurse-doctor disagreement; doctor operated on wrong side

The Result:

- Expense; serious injury; death

  This happened with other surgeries and with wrong doses of medicine

Electricity Should be Available

Controls:

1. *People* monitor and prune trees and manage the systems
2. *Local systems* detect short-circuits; re-route power to other lines
3. *Regional systems* provide backup alerts and service

What happened on August 14, 2003:

- Some trees in Ohio were not pruned; they hit some lines — short circuit
- Local systems did not detect the short circuits and shut down wrong lines
- Regional systems did not collect real-time data and shut down more wrong lines
- People did not understand the problem until it was too late

Result:

- 50 million people in US & Canada without power; losses of about $4-6 Billion
- The US blamed Canada; Canada blamed Niagara Falls, then NY, then PA

A similar event occurred a month later, affecting 56 million people in Italy

Definition of Risk

Risk is the potential that an action or inaction will lead to an undesirable outcome

Risks you wish to incur and perhaps profit from *(expected risk)*:

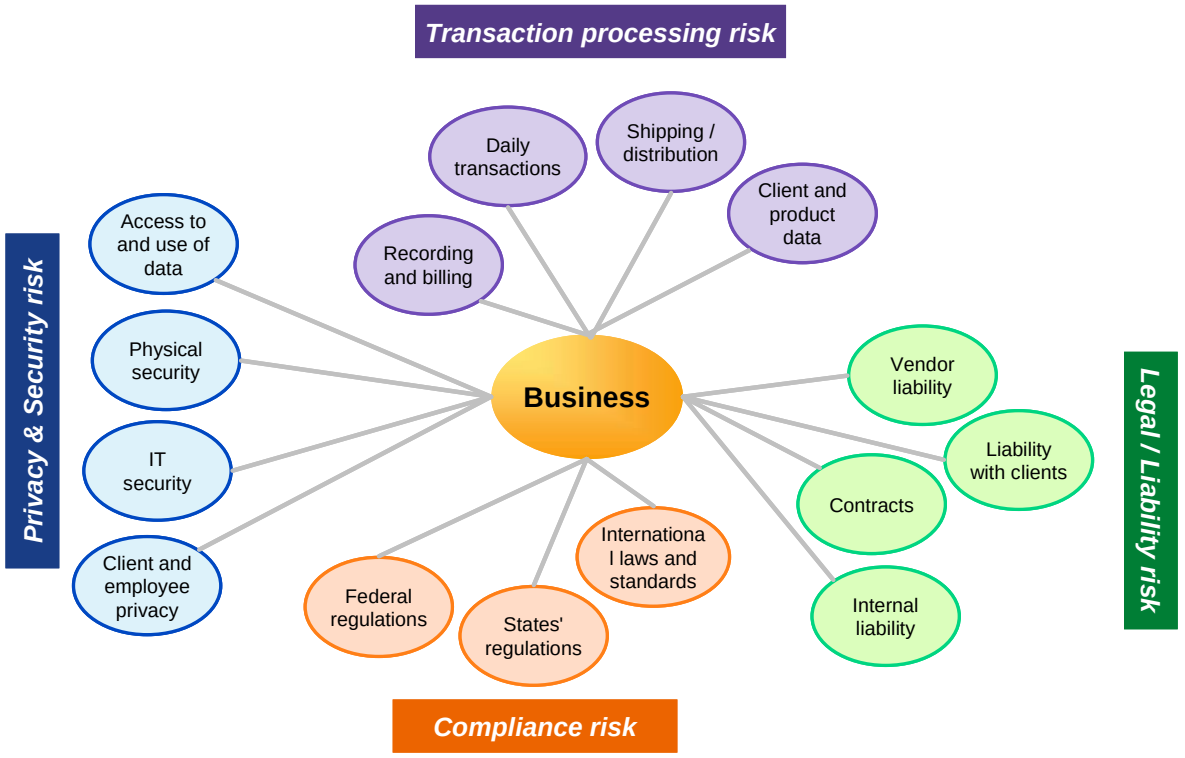
- Market risk
- Credit risk

Risks you generally do not choose to have *(unexpected risk)*:

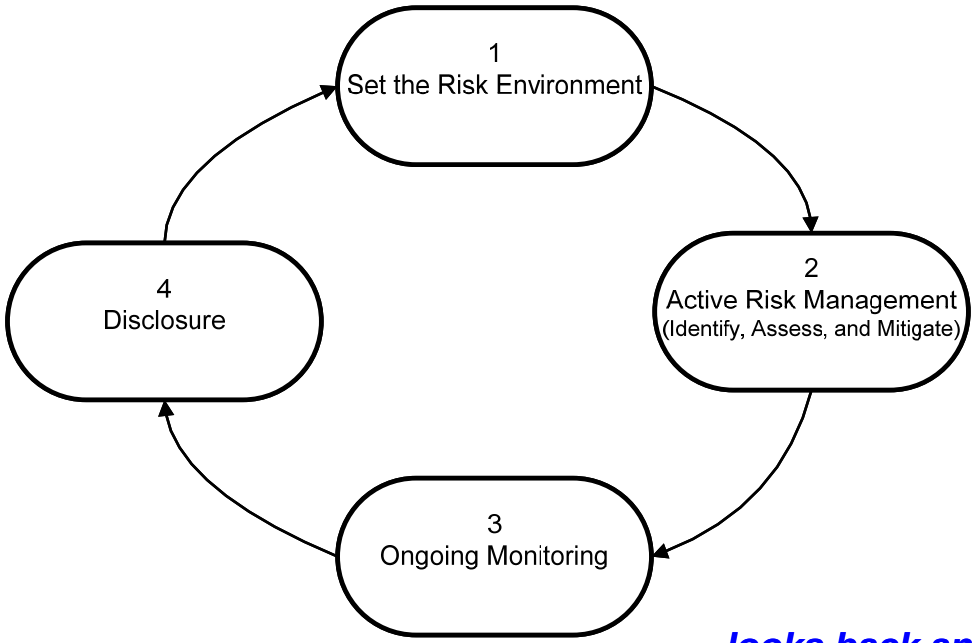
- Reputation risk
- Operational risk

Operational Risk is the risk of loss resulting from inadequate or failed people, processes or technology

Types of Operational Risk



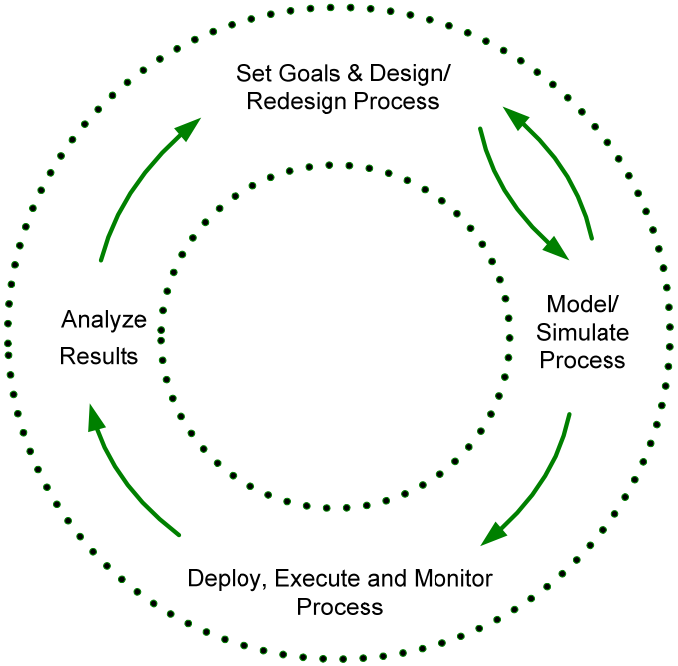
Typical Approach to Managing Operational Risk



...looks back and reacts

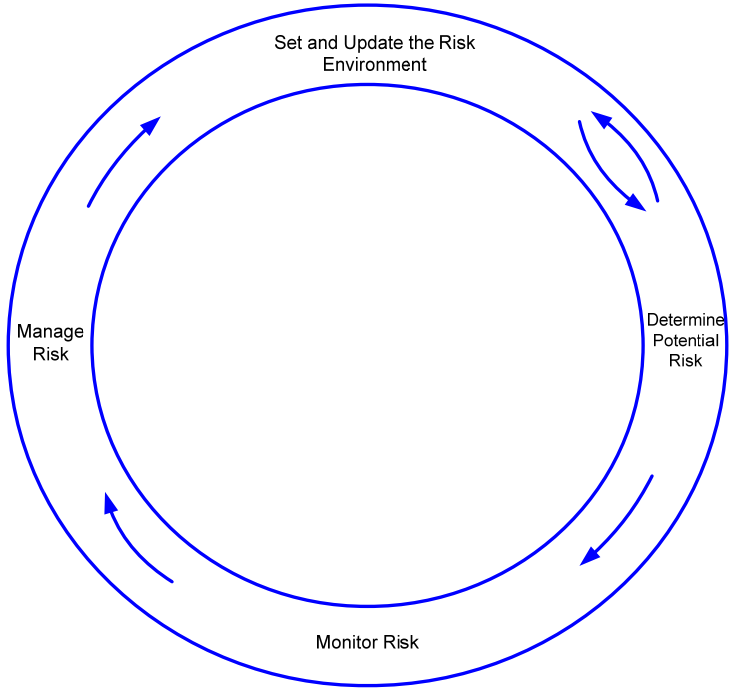
Source: Dennis I. Dickstein and Robert H. Flast. No Excuses: A Business Process Approach to Managing Operational Risk. Hoboken: John Wiley & Sons, 2009.

Consider the Business Process Framework



Source: Dennis I. Dickstein and Robert H. Flast. No Excuses: A Business Process Approach to Managing Operational Risk. Hoboken: John Wiley & Sons, 2009.

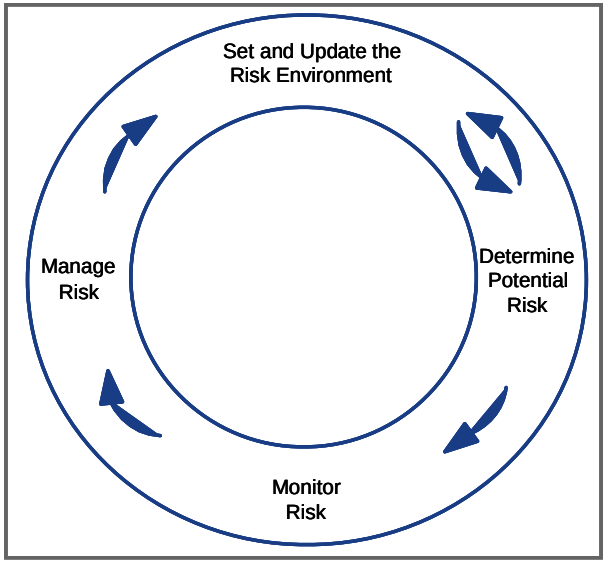
Consider a Proactive Risk Management Framework



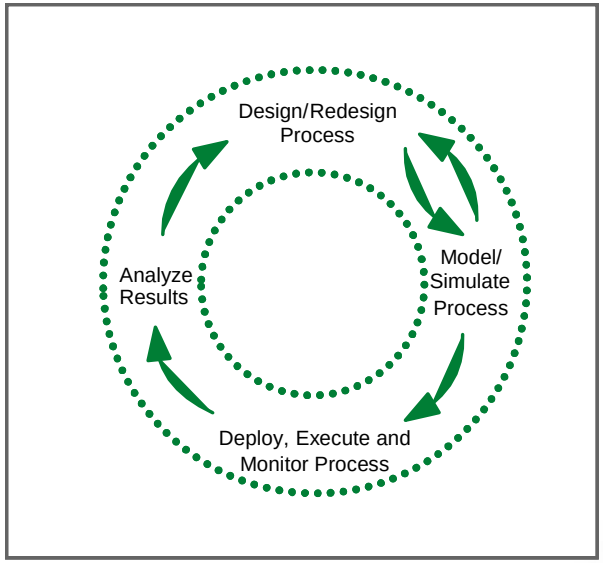
Source: Dennis I. Dickstein and Robert H. Flast. No Excuses: A Business Process Approach to Managing Operational Risk. Hoboken: John Wiley & Sons, 2009.

An Opportunity to Approach This Holistically

A Proactive Operational Risk Management Framework

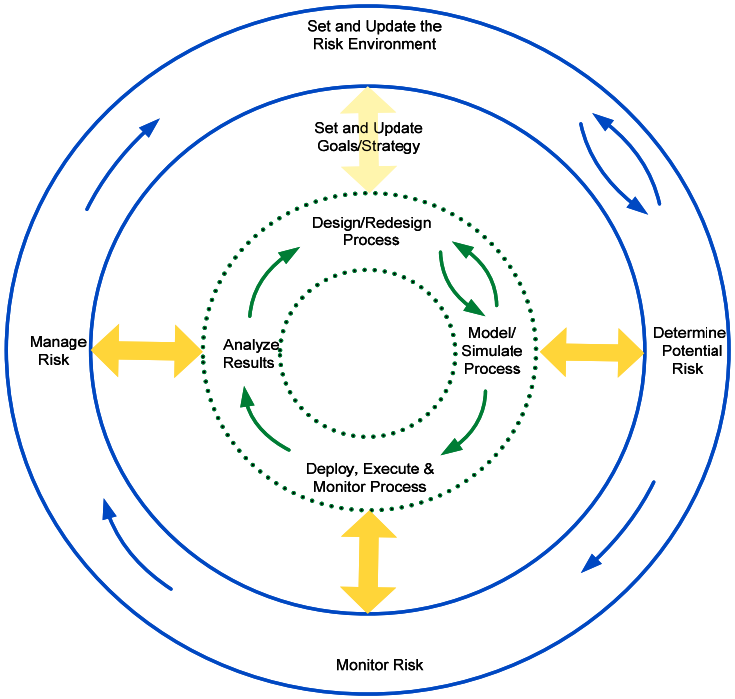


Process Management Framework



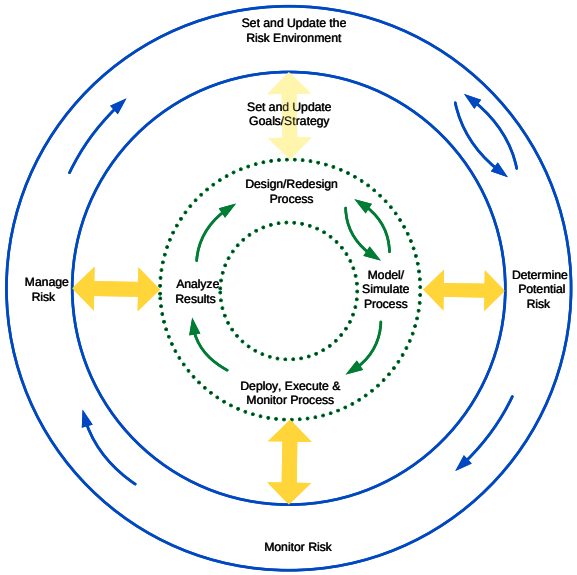
Source: Dennis I. Dickstein and Robert H. Flast. No Excuses: A Business Process Approach to Managing Operational Risk. Hoboken: John Wiley & Sons, 2009.

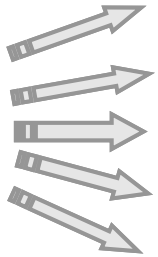
Result: An Integrated Framework



Source: Dennis I. Dickstein and Robert H. Flast. No Excuses: A Business Process Approach to Managing Operational Risk. Hoboken: John Wiley & Sons, 2009.

The Framework is Only One Part of the Puzzle





Sales and Marketing
Product Development / Manufacturing
Distribution and Operations
Billing and Finance
Control functions: Audit, Legal, etc.

Designing a framework is fairly straightforward. Obtaining buy-in is key…

Source: Dennis I. Dickstein and Robert H. Flast. No Excuses: A Business Process Approach to Managing Operational Risk. Hoboken: John Wiley & Sons, 2009.

Information Security Checklist – Not Only Technology

- Policies and Procedures
- Data Breach (Incident) Review and Response
- Internal Controls
- Training
- Security of Third Party Service Providers
- "Programs"
- Organization and Governance

Policies and Procedures

- Scope; what is covered
- Protocols to follow; processes to monitor
- Roles and Responsibilities
- Recognizing risk – mitigating risk
- Follow up with training

Data Breaches

- **What to do when an incident is identified –**
  - Is it a "reportable" breach?
  - Protection services or other security measures?
  - *One-time event or indicative of a systemic control deficiency?*

- **Roles and responsibilities**
  - Contact point
  - Analysis and determination
  - Responding, reporting and logging

Follow up with training

Internal Controls

People

Processes

Systems

And if you provide services, do not forget the new SOC 2 and SOC 3 reports…

Training

- **What**
  - General awareness
  - Test employee ability to follow policies and/or procedures
  - Employee self-certification of policy / procedure adherence
  - Specialized training for specific areas or functions

- **How**

In-person – "town halls"

Conference calls

On-line

Third Party Service Providers

Even outsourced, the risk remains with you

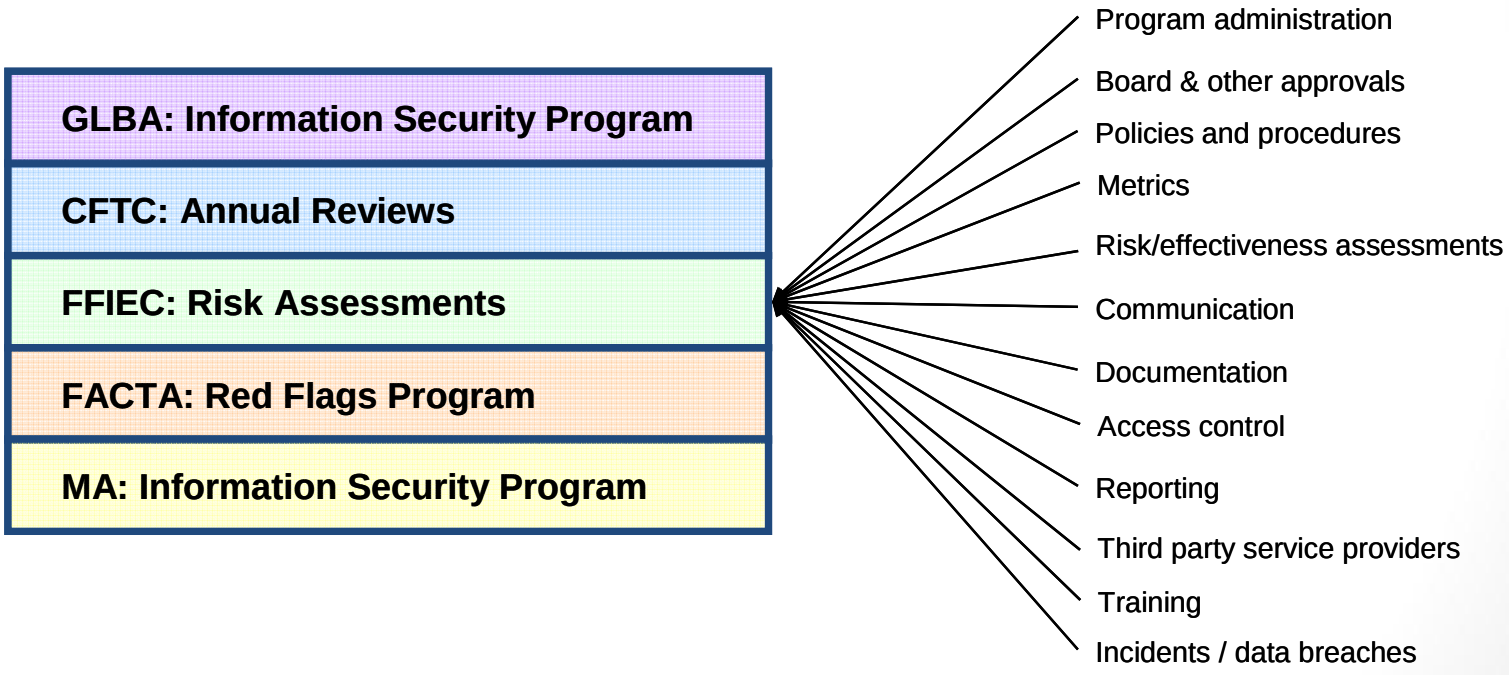
- Determine management of the relationships
  - Roles and responsibilities
  - Guidelines or checklists for internal relationship managers
- Maintain an inventory, identifying for each:
  - Purpose and service; contractual obligations; internal relationship manager
  - Sensitive data involved; its access, acquisition, use, storage and disposal
  - Relative risk – allowing a risk-based approach to periodic reviews or assessments
- Review processes and privacy/security controls
  - Initial review prior to or as part of contract negotiation
  - Periodic monitoring or auditing
  - Use of new AICPA SOC 2 and SOC 3 reports

Do You Need Written Information Security Programs?

- Written document
  - Roles and responsibilities
  - Coverage
- Management accountability
  - Tools to help
  - Tools to enforce
- How do you know?
  - Policies, procedures and training
  - Employee self-certification
  - Metrics
  - Testing
  - Combination of above

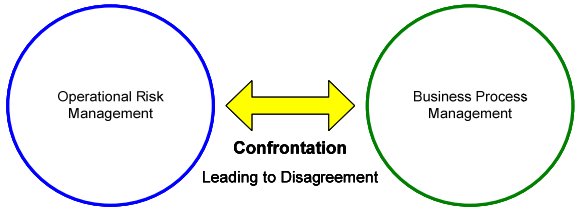
Build and Integrate; Do Not Duplicate

Comprehensiveness: targeted or broad; risk-based or compliance-based

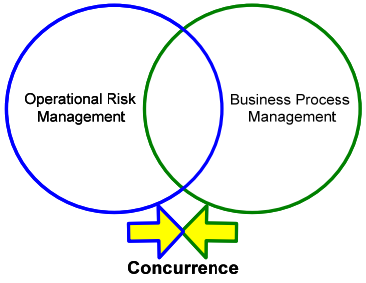


Aligning Risk Management to Business

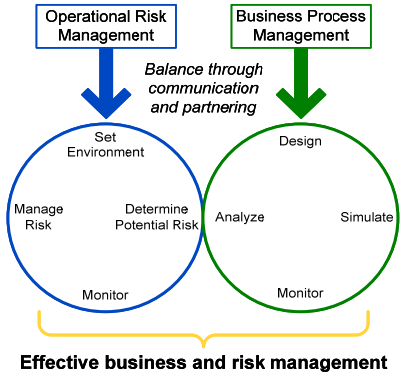
Option 1: Separate from business...



Option 2: Within the business...



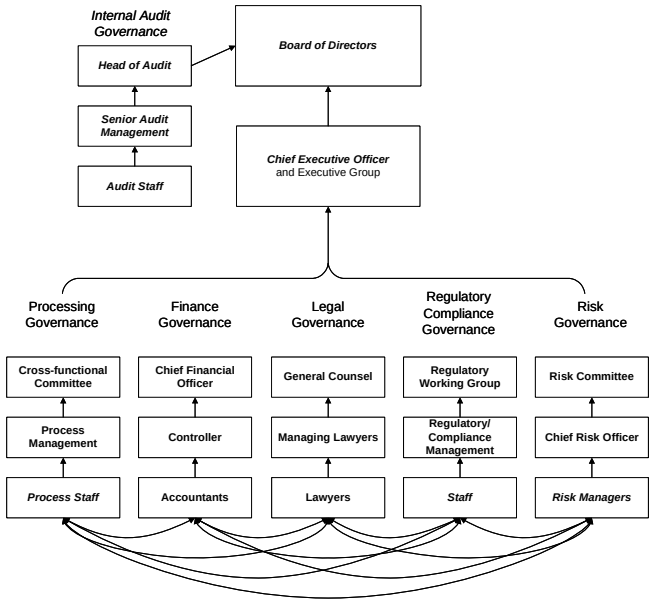
Option 3: Partner with business...



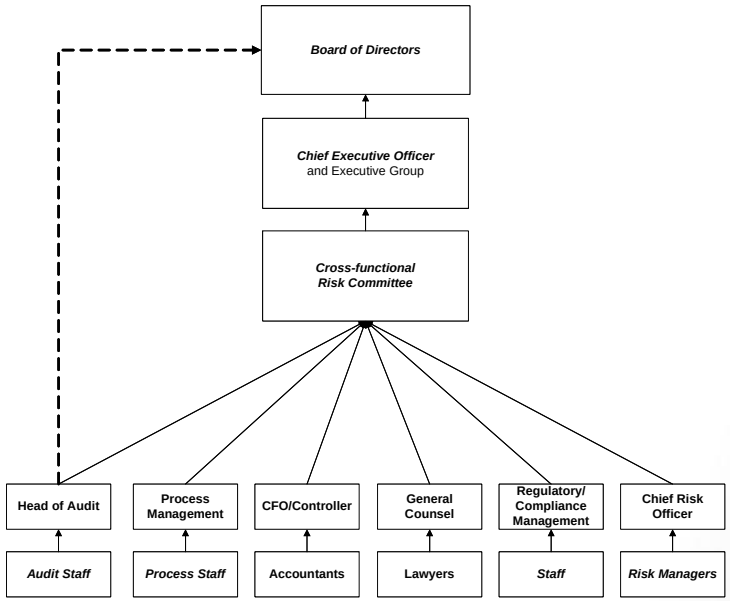
Source: Dennis I. Dickstein and Robert H. Flast. No Excuses: A Business Process Approach to Managing Operational Risk. Hoboken: John Wiley & Sons, 2009.

Create Risk Governance

Multi-Control Model

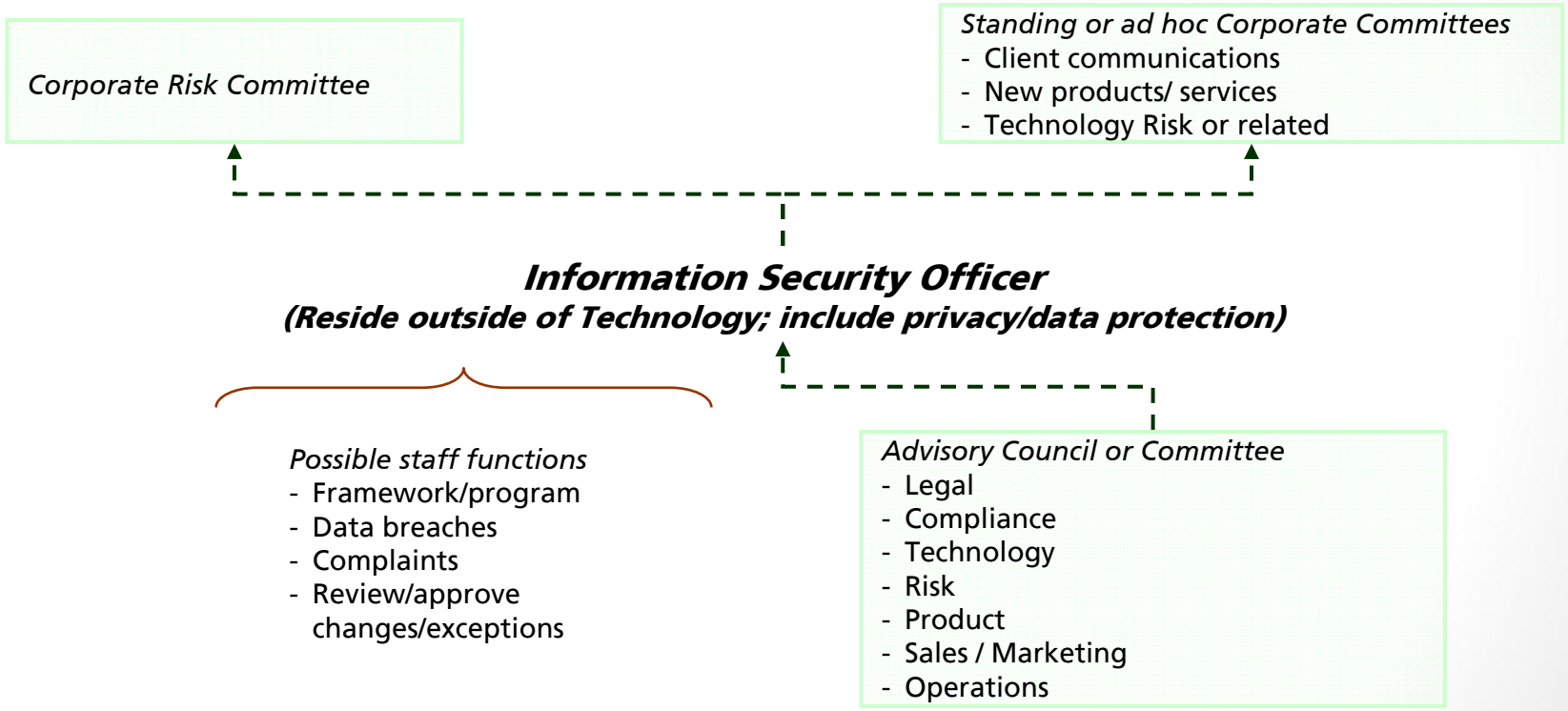


Single Thread Model



Source: Dennis I. Dickstein and Robert H. Flast. No Excuses: A Business Process Approach to Managing Operational Risk. Hoboken: John Wiley & Sons, 2009.

Sample Governance Structure

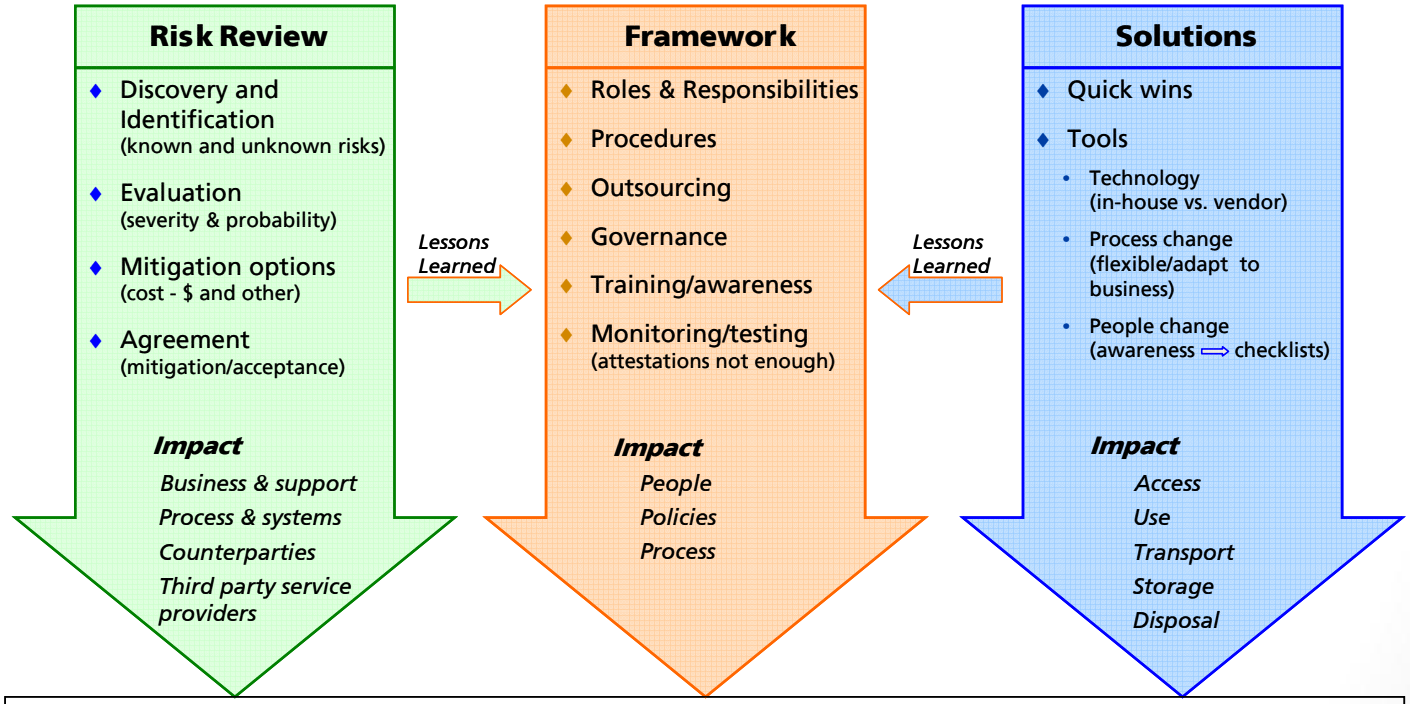


Utilize Corporate Lines of Defense

- ***Line managers*** manage the risks of their areas
- ***Risk management*** identifies, assesses and helps manage the risks
- ***Compliance*** sets and communicates policy
- ***Executive committees*** approve control design and review effectiveness
- ***Internal audit*** independently confirms design and effectiveness
- The ***Board of Directors*** reviews the results

DOES IT WORK?

A Possible Approach



Obtain buy-in: the risks are real; the solutions can vary; and accept a level of risk when mitigation costs outweigh expected risk

Now You Have No Excuses!