



# PMI Central Mass Chapter

## “The Role of Project Management in Compliance”

Presenter:  
Jack Bergen  
Director NIS Management Services  
NSTAR Gas & Electric

*January 12, 2010*

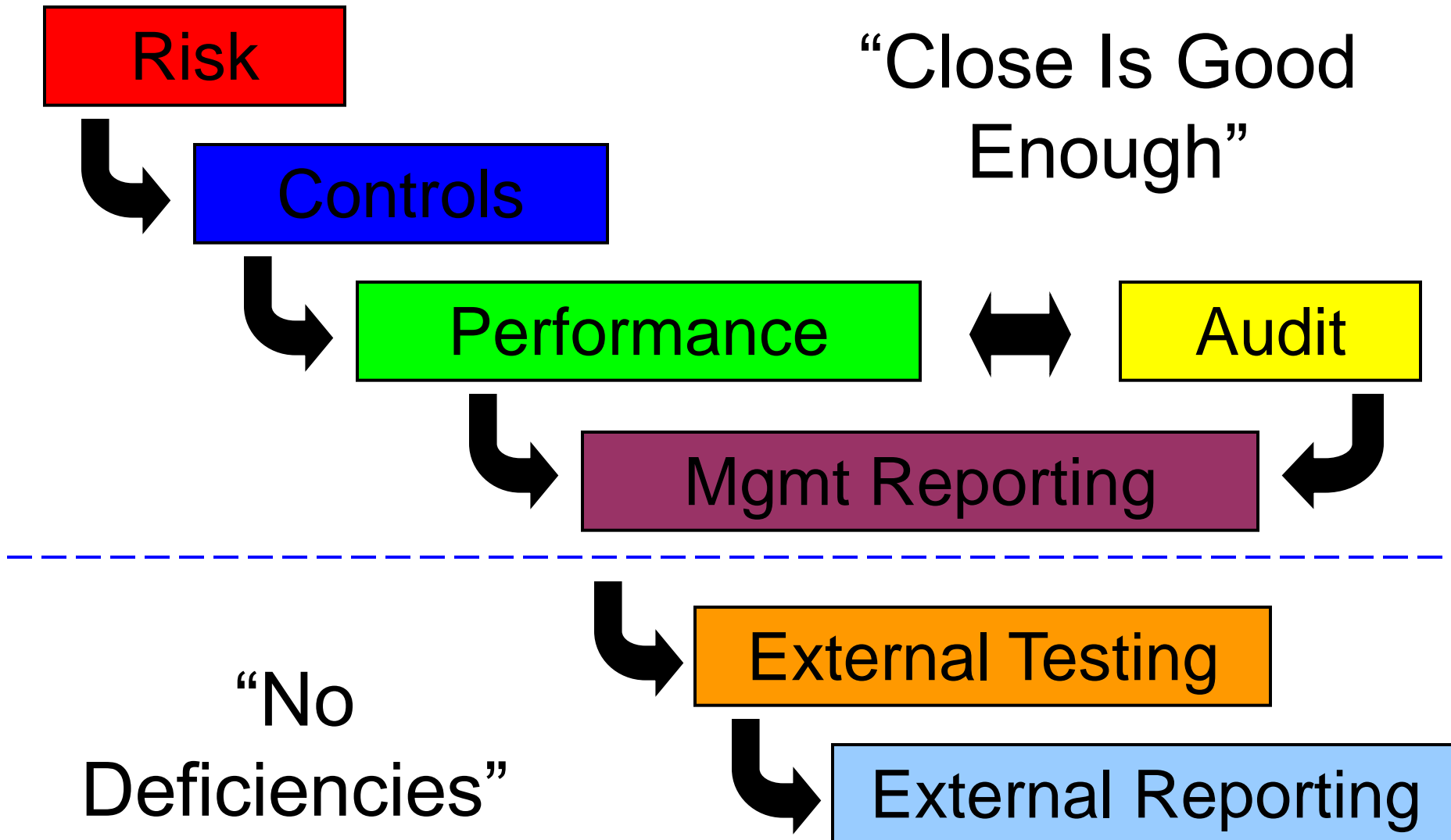
# Agenda

- Current State of Common Business Risk
- Participant Roundtable
  - What are the compliance issues facing your company?
- Approach to Compliance at NSTAR
- What Does This Mean to You as a PM?
- Questions

# What Do We Mean By Compliance?

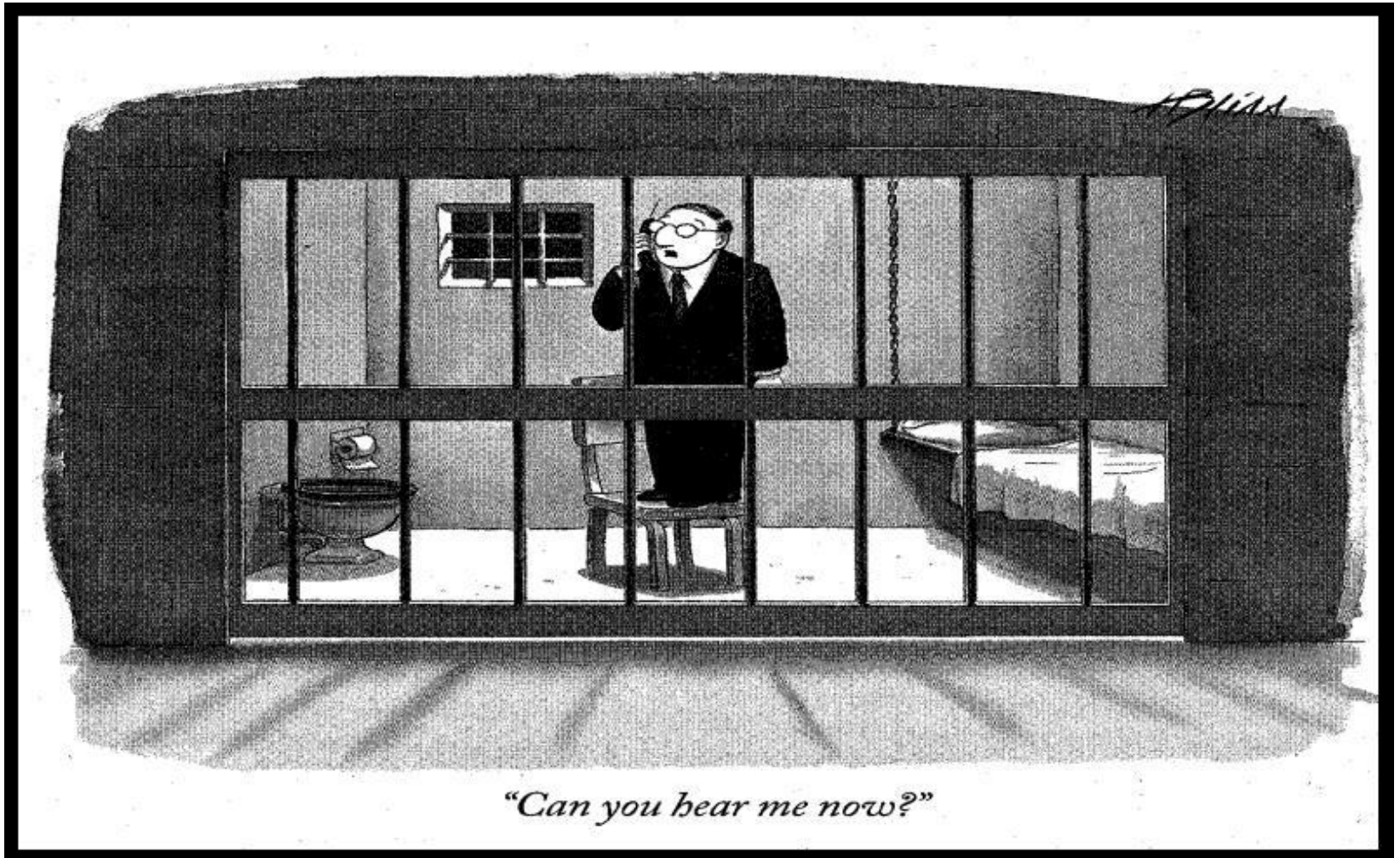
- Compliance for today's' discussion is not about following methodology
- It is about ensuring that business risk is mitigated and external authorities are satisfied

# Changing World



# Current State Of Business Risk

# So Why Is This Important?



# Recent Data Breaches

Date	Organization	Description
Jan	Check Free	Some of the banks that use its electronic bill payment service say that criminals took control of several of the company's Internet domains and redirected customer traffic to a malicious Web site hosted in the Ukraine. The company believes that about 160,000 consumers were exposed
Feb	St. Anthony Central Hospital (Denver , CO)	Boxes, filing cabinets and trash bags full of hundreds of U.S. passports, birth certificates, driver's licenses, Social Security cards and other documents were found in a storage unit.
Mar	CVS Pharmacies	Disposing of documents, such as labels from prescription bottles and old prescriptions, in unsecured dumpsters.
Apr	New York Police Department	A civilian employee of the department's pension fund is accused of stealing eight tapes containing the Social Security numbers and direct-deposit information for 80,000 current and retired cops.
May	MySpace	Confidential employee information, including "at least" name, Social Security numbers and compensation, was taken by an employee in the company's benefit's department without authorization.
Jul	Internal Revenue Service	The U.S Treasury Inspector General for Tax Administration found in a fiscal year 2008 audit that in more than a dozen IRS document disposal facilities, old taxpayer documents were being tossed out in regular waste containers and dumpsters
Aug	AT&T	A temporary employee for AT&T was arrested today on charges she stole personal information on 2,100 co-workers.
Sep	Bank of America Corp.	Recently issued replacement cards to consumers, telling them that their account numbers may have been compromised. Account information from certain Bank of America debit cards may have been compromised at an undisclosed third-party location.
Dec	Bernard Madoff Investors	More than 2,200 Bernard Madoff investors are learning that some of their personal and financial information has potentially been breached after the theft of a laptop in Dallas

# *Boston Sunday Globe*

January 3, 2010

## **Data Breaches Affect Millions Of State Residents**

“One million Mass residents – or 1 in 6 people- have had their credit card numbers, medical records, or other personal information leaked or stolen over the past two years, according to records provided to the Globe by state officials.”

# PwC 2010 Global State of Information Security Survey

## *Source of Incidents*

Likely Source of Incidents	2008	2009
Current Employees	35%	34%
Former Employees	18%	22%
Hacker	38%	21%
Unknown	40%	43%

## *Business Impact*

Business Impact	2008	2009
Financial Impact	21%	30%
Brand/Reputation Compromised	21%	27%
Fraud	16%	20%
Legal Exposure/Loss of Shareholder Value	26%	21%
Intellectual Property Theft	42%	36%

# Desired Skill\*

**Job Title:** Senior Project Manager- Various Locations in RI and MA

- **Job #** 202014
  - **Location** Providence, [RI](#)
  - **Type** Contract
  - **Date Posted** 12/21/2009
- Category** [Project Management](#)  
**Industry** [Retail](#)  
**Required Experience** 3 years

## Job Description

- Many of our top clients are looking for senior level Project Manager to work in Providence, Rhode Island or Framingham, MA on a contract basis. There is an opportunity for the role to become permanent, but if you are only interested in consulting opportunities please still apply.
- The clients are looking for a very strong, experienced detail oriented Project Manager. We would prefer candidates that have worked in the Retail, Healthcare or Pharmacy space in the past. Also, any Big Five consulting experience is a huge plus.
- Skills desired include
  - PMP, CISSP, and ITIL certification huge plus
  - Experience with IT risk and compliance
  - Exposure to PCI compliance, Sox, and Hipaa

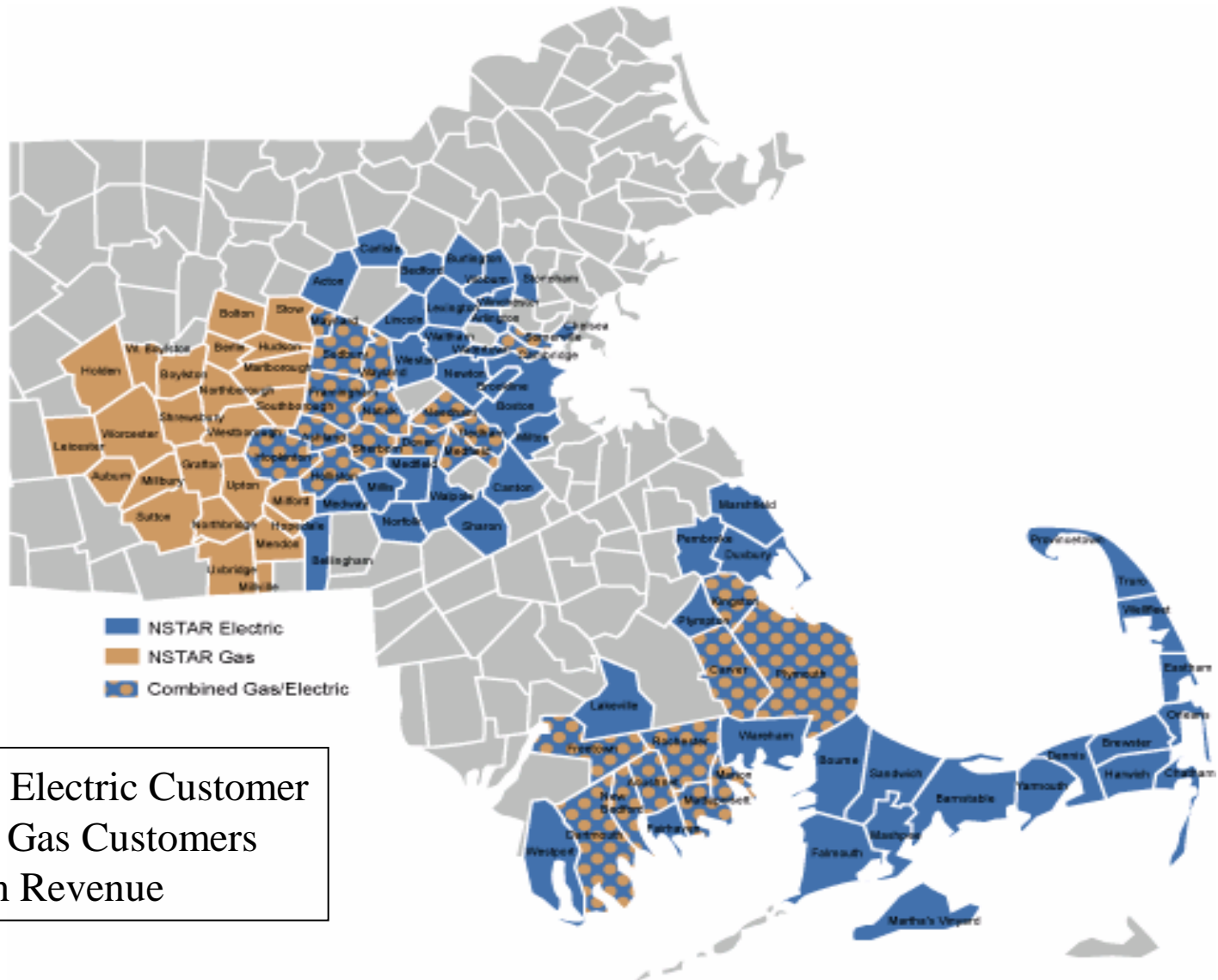
\* Source: [www.sapphire.com](http://www.sapphire.com)

# Participant Roundtable

- At your tables, discuss the top compliance issues facing your company
  - What are the threats?
  - What are the regulations?
  - Who is watching your company?
  - How has your company responded?
- Report out on your findings
  - Include industry
  - Specific regulations and external compliance requirements
  - Actions taken to ensure compliance

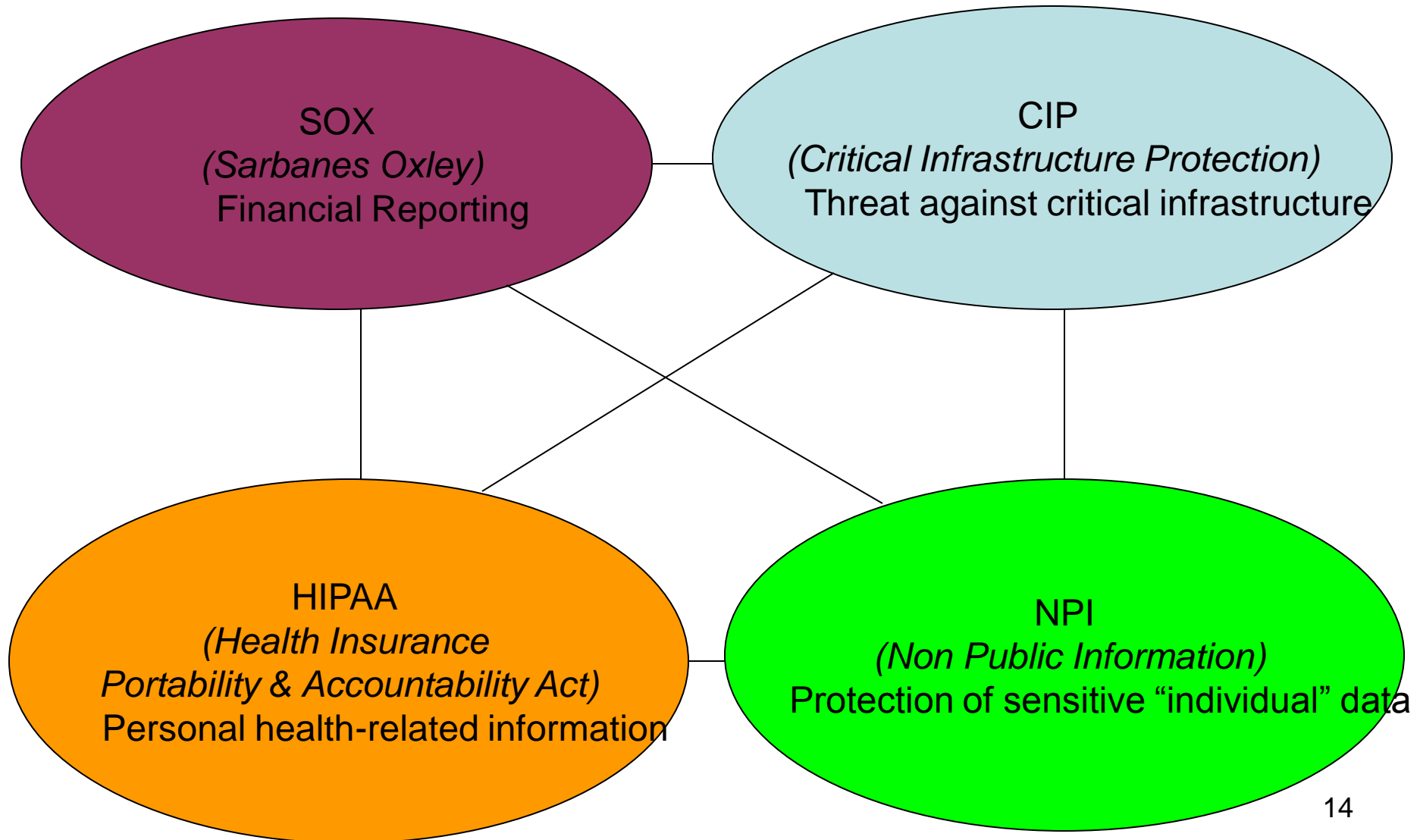
# Compliance At NSTAR

# NSTAR Service Territory



- 1.1M Electric Customer
- .2M Gas Customers
- \$3B in Revenue

# Compliance Programs At NSTAR



# Approach to Compliance at NSTAR

## Institutionalizing Compliance

*Program Development*

*Rollout*

*Transition to Steady State*

*Adoption*

*On-going Governance*

**INFORMAL**

**STANDARDIZED**

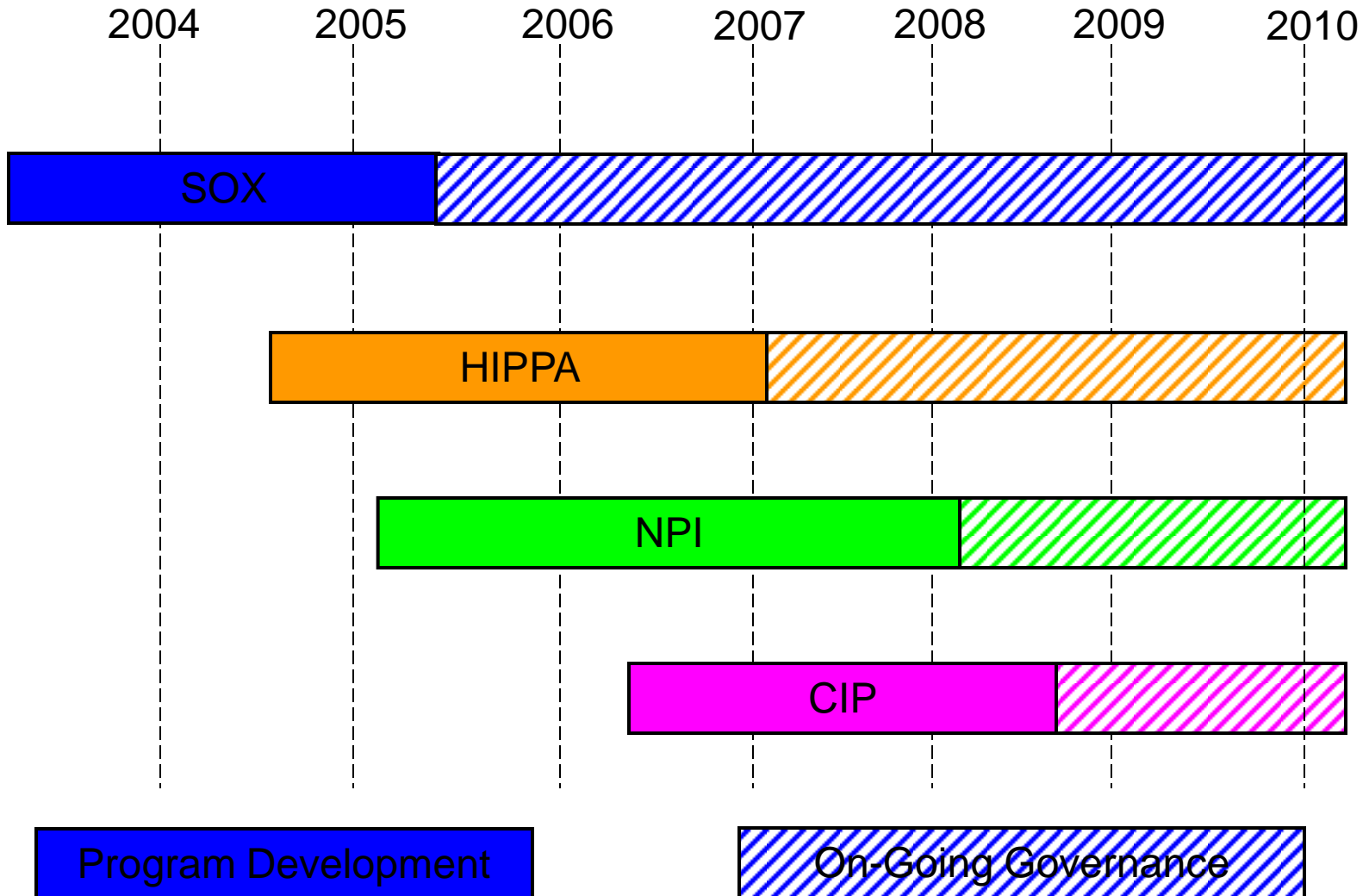
**OPTIMIZED**

- *Evaluate Risk*
- *Document Existing Controls*
- *Identify Gaps*
- *Develop Additional Controls*
- *Perform Baseline Testing*

- *Develop Governance Model*
- *Identify Business Owners*
- *Roles and Responsibilities*
- *Perform Education*

- *Quarterly Certification*
- *Management Testing*
- *External Testing*
- *Senior Reporting*

# On-Going Process



# General Computer Controls Framework

**General Computer Controls**  
Maintain the integrity and currency of data in automated systems from source of original data entry to preparation of output

<b>Business Controls</b>	<b>Applications/Program Changes</b>
--------------------------	-------------------------------------

<b>Infrastructure Controls</b>	<b>Operations</b>
	<b>Operating and Systems Software</b>
	<b>Network Operations</b>

**Information Security**

# Typical Risk Mitigation Activities

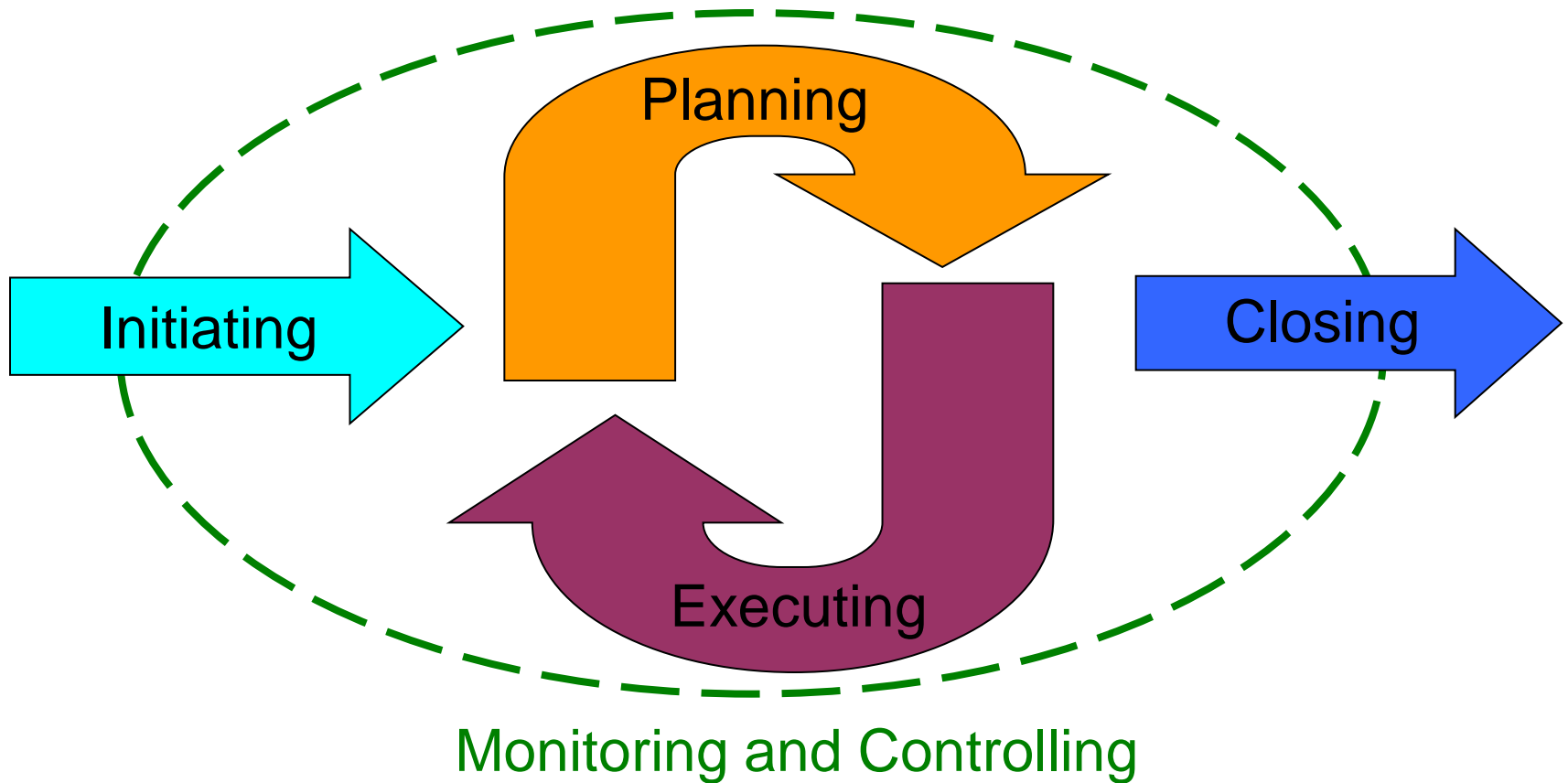
<u>Activities</u>	<u>Owner</u>
– Employee awareness and education	Business
– Up-to-date inventory of where data is stored	Business/IT
– Up-to-date inventory of who has access	Business/IT
– External vendor/partner assessment & mitigation	Business/IT
– Incident Response Plans	Business/IT
– Recovery Plans	Business/IT
– IDM (Identity Mgmt) solutions	IT
– Improved firewalls and intrusion prevention	IT
– Physical device protection	IT
– Vulnerability Assessments	Audit/IT

# NPI Training

**Non-Public Personal Information  
Awareness Program 2010**



# Project Management Processes\*



## PMBOK References to “Compliance”

- 5.1.3 Requirements
- 9.1 HR Plan

# What Does This Mean to You as a PM?

- What can go wrong?
  - Changes are made to the environment that create risk
  - It is assumed that someone else is taking care of this
  - Design of security an after thought
- What can you do?
  - Understand state & federal regulations that may impact your project
  - Understand the risk and controls in your company
  - Reach out to the compliance manager
  - Know who is responsible for ensuring controls are being followed
  - Build the appropriate business controls into the process
  - Make sure this is part of your production-turnover checklist and activity (Do it early in the project)

# What Does This Mean to You as a PM?

Have authorities or privileges been changed for the production environment?  
(Application, databases, etc.)

Does the business know what their role is?

Does this involve external parties? Are those communication secure?

## *Sample Questions To Ask*

Do you know what type of data is collected, how it will be handled, and who will have access to it?

Has security been notified?

Non-production data (test, development)

- Who has access?
- What is test data is being printed out?
- What have you left behind?

Has the technical environment been built to secure standards?

Does this involve portable devices? Are those secure/encrypted?

# What Does This Mean to You as a PM?

- Other things you can do
  - Add these and other steps into your methodology
  - Volunteer to work on one of these compliance efforts
  - Become an expert in one of these areas
  - Use this as an opportunity to understand the business process more
    - What are the risks?
    - What are the threats?
    - How can we make sure the project or change is ensuring that these are being mitigated or that current controls are not impacted

# Summary

- Increased risk
- Increased external scrutiny and oversight
- Increased need to have effective and efficient controls
- You can help to make that happen
- Get involved!!

# Questions??

Contact Info:

*john.bergen@nstar.com*