



METRO NYC CHAPTER



Long Island Chapter



# Educational Event

Spring 2015



## Privacy and IG

Joseph Steffan

Morgan Stanley, Chief Privacy Compliance Officer

# Context and Terms

## Colloquial “Privacy”

- Privacy and Information Security
  - Privacy focused on collection, use and sharing of PII
  - Information security focused on preventing unauthorized access generally
  - Tend to be programmatically distinct but with key relationships



Long  
Island  
Chapter



# Privacy - Overview

## Privacy History and Evolution

- Jurisdictional distinctions
  - US – Sectoral
  - EMEA – Omnibus
- Asynchronous development and conflicts
  - Risks and qualitative decision making
- Multiple regulatory channels
  - E.g., GLBA – Reg SP, FTC, etc.
  - FCRA, data breach notification
- Early stage - social dialogue
- Technology drivers



Long  
Island  
Chapter



# PII

## Personally Identifiable Information

- Generally broad definition
- But procedures may ultimately depend on subset and context, e.g.,
  - U.S. data breach notification
  - GLBA notice and opt-out (some opt-in)
  - FCRA – “eligibility” information
  - EMEA style – data processing and export



Long  
Island  
Chapter



# Regulatory Dynamics

## Post-Financial Crisis

- o Emphasis on governance and risk

## Data Breaches

- o Increased focus on “privacy”

- o Growing regulatory expertise and specificity

Creates Opportunities for IG Strategy



Long  
Island  
Chapter



# Privacy Relationship to IG

## Information Governance (or Mgmt.)

- Potential consensus for holistic discipline
  - Privacy
  - Information security
  - Information management
- Overlaps and distinctions
  - Program structure and administration
  - Principles of inventory and classification
  - Privacy focus on PII
  - Degrees of technical rigor/expertise



Long  
Island  
Chapter



# Parallel Program Issues

## Business Case Drivers

### ○ Risk

- Regulatory (use, sharing, security, under-retention, mode of retention, prompt retrieval)
- Litigation (e-discovery, preservation, spoliation)

### ○ Cost

### ○ Productivity

### ○ Relative Program Maturity



Long  
Island  
Chapter



# Organizational Current State

- Who “Owns” Information Governance?
  - Multidisciplinary problem, cross-divisional responsibility
  - Business units have primary operational responsibility for recordkeeping
  - Advisory, control and IT functions need relevant expertise for advice, policy, implementation and oversight assistance
  - Information governance (or management) is an increasingly distinct and necessary field of expertise



Long  
Island  
Chapter



Summit 2014





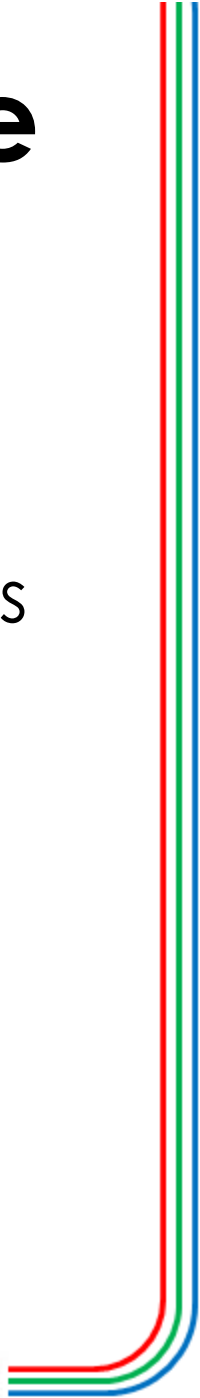
# Organizational Current State

## Organizational Views and Motivations

- Drivers and perspectives vs. consensus among key stakeholders
- Business, advisory and control functions
- Current vs. potential information governance/management function
- De facto cultural change



Long  
Island  
Chapter



# Program Scope

## Conceptual Scope

- Create/Receive
- Classify
- Store/Retain
- Protect
- Access/Distribute
- Analyze/Maximize Value/Quality
- Hold
- Dispose



Long  
Island  
Chapter



Summit 2014



10

# Related Program States

## Potential Scope of Related Programs

- Information Lifecycle Management (classify, retain, hold, dispose)
- Information Security and Privacy (receive, protect, access, distribute)
- Information Retrieval and Forensics (access, distribute, analyze)
- Information Optimization, Big Data . . . . (analyze, maximize value . . . .)



Long  
Island  
Chapter



# Governance

## Key Stakeholders

- Legal, Compliance, IT, BU, Firm Admin, Risk
- Management consensus on high-level objectives and scope

## Governance/Coordination Model

- Designated operational/BU contacts or committees
- Routine, documented governance meetings
- Feedback on strategies, consensus for priorities, participation in key processes, e.g., disposition
- Leverage control functions – Audit, Risk



Long  
Island  
Chapter



Summit 2014



# Staffing

## Dedicated Staffing

- Permanent core function
- E.g., Legal, Compliance, BU/Firm Admin, IT, Corporate Services
- Specific information management expertise
- Ideally includes dedicated staff in business functions



Long  
Island  
Chapter



Summit 2014



13

# Staffing (cont.)

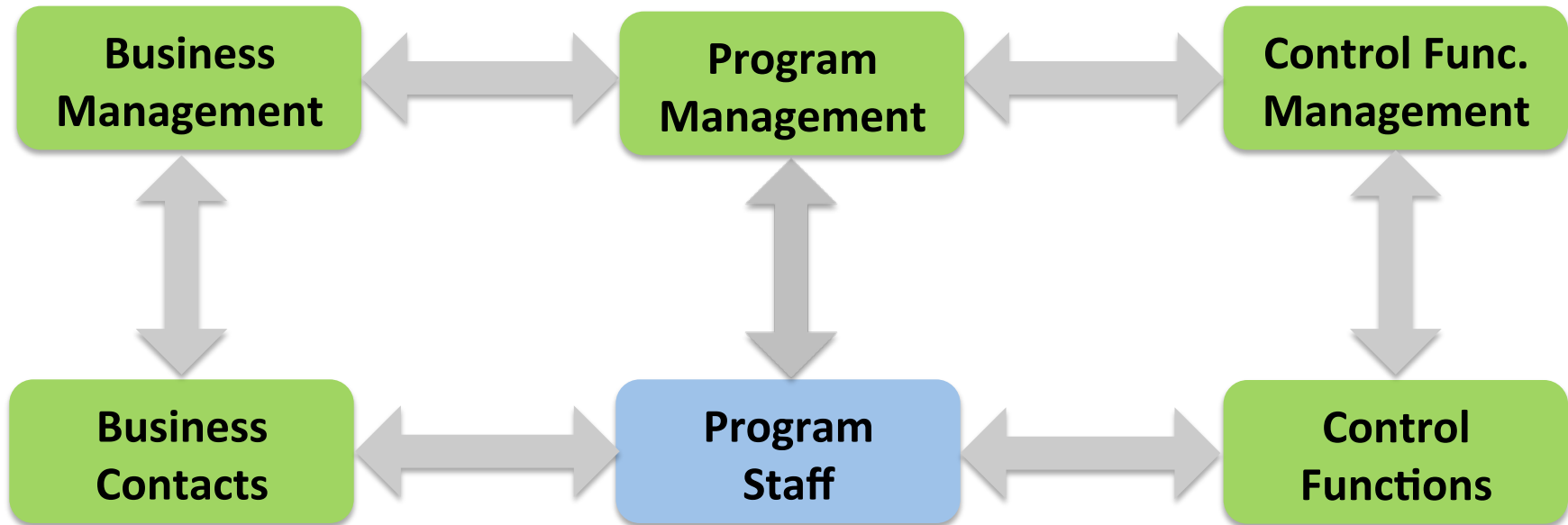
- Information management expertise drives strategy and execution
- BU contacts and management need to be aware, agree on overall strategy, express relative priorities
- Program and project management
- Cross-divisional opportunities and challenges



Long  
Island  
Chapter



# Coordination and Escalation



Long  
Island  
Chapter



Summit 2014



METRO NYC CHAPTER

# Execution – Strategy/Communications

- Tactical vs. Strategic
- Historical vs. Going Forward
- Communications
  - Terminology, audience, depth
  - Clarity – start at the beginning
  - Manage expectations



Long  
Island  
Chapter



Summit 2014





# Execution – Classification

## Classification

- Retention requirements
  - Regulatory vs. operational
  - Regulatory specificity
  - Mandatory vs. discretionary
- Authoritative vs. duplicate records
- Extension to more holistic program



Long  
Island  
Chapter



Summit 2014



# Execution – Policy, Inventory

## Program and Policies

- Program materials (examinability)
- Policy (principles)
  - Firm-wide vs. BU-specific
- Retention schedules (classification)

## Inventory

- Systems inventory
- Vendor inventory
- Records inventories (specific records and process)



Long  
Island  
Chapter



# Execution – Storage/Archiving

Manual/System-generated

Physical/Electronic

Process/Interfaces

- Storage, retrieval
- Metadata
  - Record vs. IG process metadata



Long  
Island  
Chapter



Summit 2014



19

# Execution – Storage/Archiving

## Storage locations and format requirements

- Systems vs. Archives
  - Shared drives, document management, production systems
- Format (e.g., WORM) requirements

## Records Inventory

- Trend toward information-centric transparency (e.g., PII)



Long  
Island  
Chapter



Summit 2014



20

# Execution – Legal Hold

- Document Retention Notices
- Preservation/Retrieval
- People vs. “System Holds”
- Individual vs. business ownership
- Relationship to classification
- Relationship to disposition



Long  
Island  
Chapter



Summit 2014



# Execution – Disposition

- Repeatable, scalable, defensible
- Authoritative and duplicate copies
- Affirmative or veto-based approval
- Manual vs. system-enabled review process
- Candidate lists
- Legal Dept. review vs. Legal Hold Process
- Mechanisms of disposal, validation
- Certificate of destruction
- Trend toward automatic disposition



Long  
Island  
Chapter



Summit 2014



# Execution – Potential Priorities

- PII Classification and Inventory
- Backup environment
- Email and other messaging content
- Routinely examined records
- Key operational records
- Largest storage-consuming systems



Long  
Island  
Chapter



Summit 2014

