



# Grant Thornton



## Addressing the New Massachusetts Privacy Law March 23, 2010

To receive 1.0 hour of CPE, you must individually participate by:

- Remaining logged in for the entire session
- Responding to all polling questions

For technical support, please contact LearnLive at:

E-mail – [support@learnlivetech.com](mailto:support@learnlivetech.com)

Phone – 206.812.4700

### **Disclaimer**

This document supports Grant Thornton LLP's marketing of professional services, and is not written advice directed at the particular facts and circumstances of any person. If you are interested in the subject of this document we encourage you to contact us or an independent advisor to discuss the potential application to your particular situation. Nothing herein shall be construed as imposing a limitation on any person from disclosing the treatment or structure of any matter addressed herein. To the extent this document may be considered to contain written advice, any written advice contained in, forwarded with, or attached to this document is not intended by Grant Thornton to be used, and cannot be used, by any person for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.

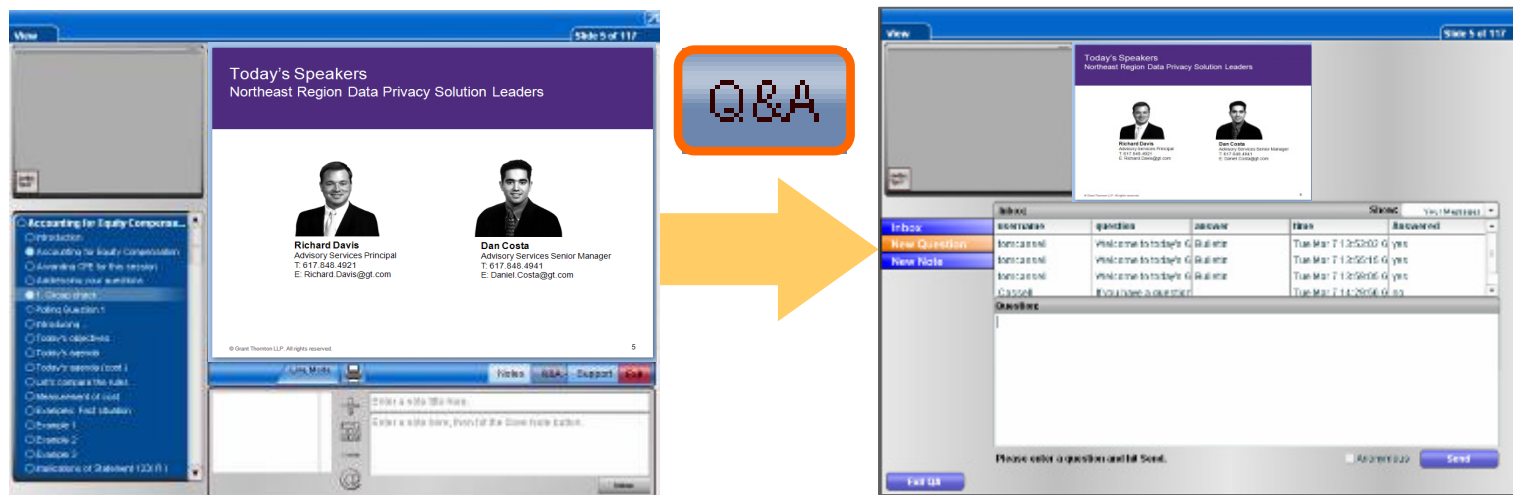
# Awarding CPE for this session

<b>Prior to session</b>	<b>In session</b>	<b>After session</b>
Registered via Grant Thornton Thinking portal	Individually participate in all interactions  Group participation will not receive CPE	Respond to online evaluation form  Print your CPE Certificate from an emailed CPE confirmation message  Download today's slides

**If you experience any technical difficulties,  
please contact 206.812.4700 or [support@learnlivetech.com](mailto:support@learnlivetech.com)**

# Addressing questions

We will address questions in Q & A at the end of the program.  
Please type in your questions at any time.



**If you experience any technical difficulties,  
please contact 206.812.4700 or [support@learnlivetech.com](mailto:support@learnlivetech.com)**

# Today's Speakers

## Northeast Region Data Privacy Solution Leaders



**Richard Davis**  
Advisory Services Principal  
T: 617.848.4921  
E: Richard.Davis@gt.com



**Dan Costa**  
Advisory Services Senior Manager  
T: 617.848.4941  
E: Daniel.Costa@gt.com

# Learning Objectives

- Evolution of Massachusetts Data Privacy
- Industry Insights
- Massachusetts Standard - MGL 93H 201CMR17.00
- A Pragmatic Approach
- Grant Thornton “PII” Life Cycle
- Summary and Questions

## What we're hearing...

“We're PCI compliant...”

“We're SOX compliant...”

“Legal's handling it...”

“This is an IT issue...”

“We're using a copy of someone else's WISP...”



# Question 1

*Where does your company stand with respect to addressing the new MA regulation implemented on March 1, 2010?*

1. Designed and implemented
2. In-process
3. Have not started



# Evolution of Massachusetts Data Privacy

## *Major Incidents*

**2006** → 45,000,000+ credit and debit card numbers stolen from TJX customers  
- TJX paid **\$65,000,000** to credit card issuers

**2007** → FTC reported 250,000 incidents of identity theft

**2008** → 4,000,000+ credit and debit card numbers stolen from Hannaford Bros. customers

**2009** → \$2,000,000 stolen in Citibank ATM PIN breach



## Question 2

What is your industry?

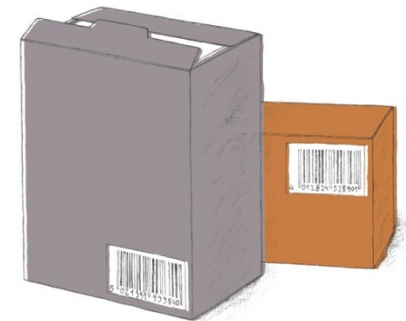
- ✓ Financial services and institutions
- ✓ Retail
- ✓ Not-for-profit
- ✓ Manufacturing and distribution
- ✓ Technology
- ✓ Other



# Industry Insights

## *Retail*

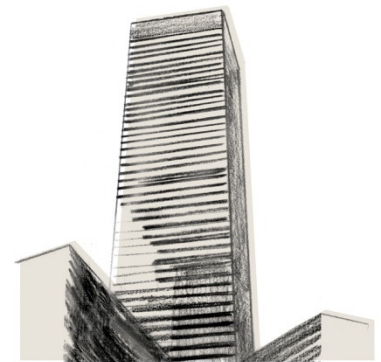
- Retail companies are constantly acquiring demographic information to more accurately predict consumer spending habits and as a result maintain large amounts of personally-identifiable information that attract hackers
- The retail industry is operating primarily on older technologies (i.e. archaic legacy systems) and is slow to meet up-to-date security standards
  - ✓ Use vulnerable point-of-sale systems
  - ✓ Remote access connections left open even if no longer in use - 68% of attacks occur through an open VPN connection or weak wireless security system



# Industry Insights

## *Financial Services and Financial Institutions*

- Financial institutions account for 93% of the approximately 285 million records involved in data breaches from 2004 to 2007
- Insiders pose the greatest threat to financial service firms
  - ✓ 42% of breaches in the financial services industry involve employee deceit
  - ✓ 68% of breaches in the financial services industry are “opportunistic” (as opposed to 32% which were a directly targeted attack)
- Attacks on financial service firms are more complex and generally involve multiple parties



# Industry Insights

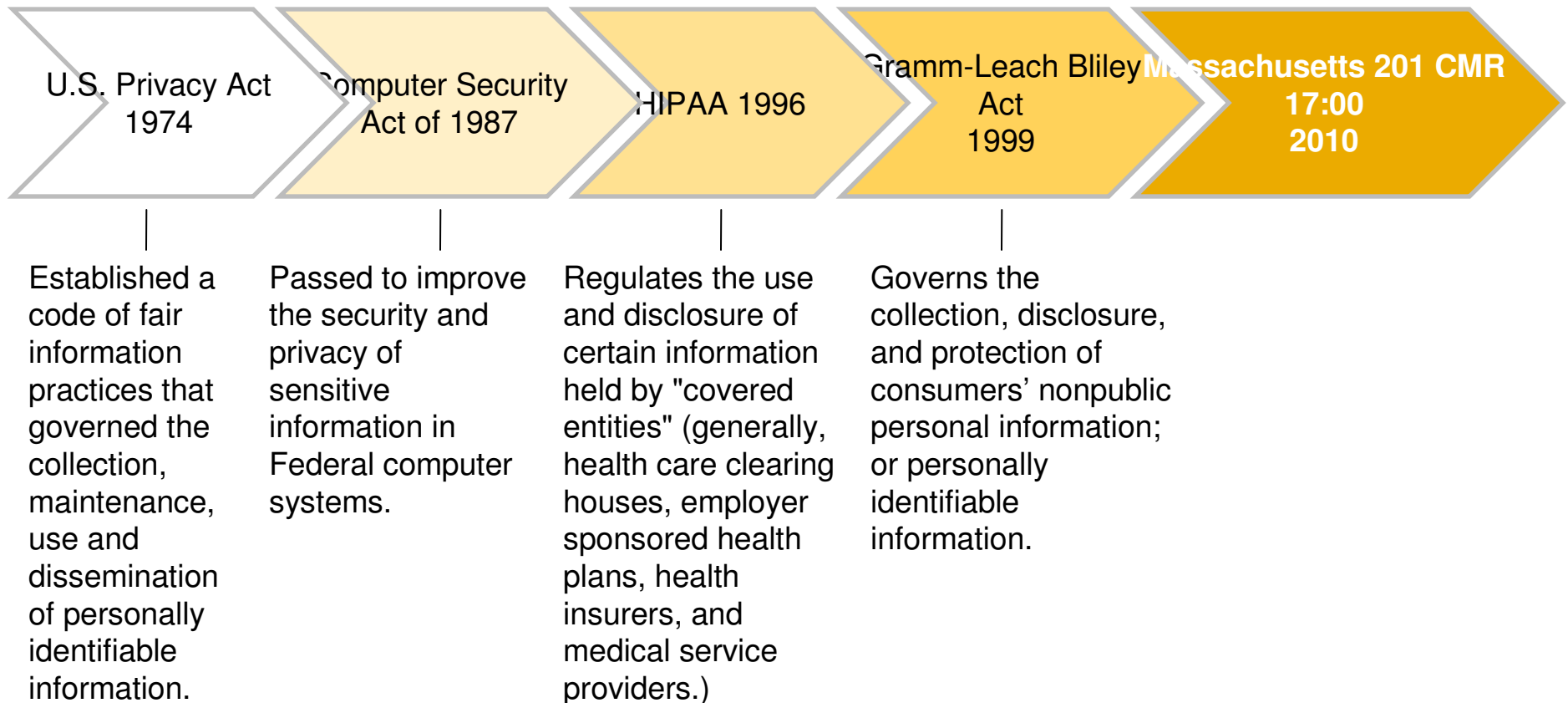
## *Not-for-Profit*

- Technology is enabling not-for-profit organizations to increase their reach into donor communities. As a result, this has increased the inherent vulnerabilities of the collection of consumer information over the years.
- In particular, information technology in the college and university setting is open and decentralized, affecting students, faculty, staff, researchers, etc. and all require extensive access.
  - ✓ Many universities have recently ceased the use of Social Security numbers as student IDs.



# Massachusetts Standard - MGL 93H 201CMR17.00

## History



# Massachusetts Standard - MGL 93H 201CMR17.00

*Deadline March 1, 2010*

The objectives of this regulation are to:

- (I) to insure the security and confidentiality of customer information in a manner fully consistent with industry standards;
- (II) protect against anticipated threats or hazards to the security or integrity of such information; and
- (III) protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

From: <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

## Question 3

*What Is Personally Identifiable Information (PII)? Outside of name and address, it is a combination of which of the following?*

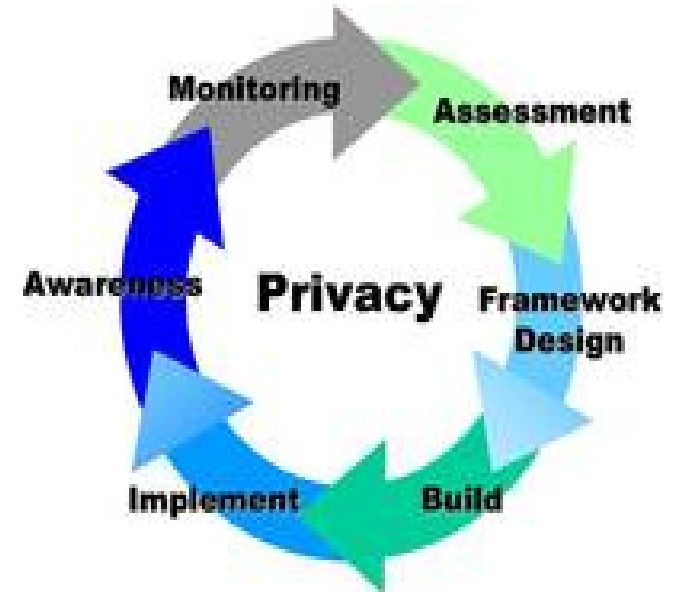
- ✓ Social Security number
- ✓ driver's license number or state-issued identification card number
- ✓ financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account
- ✓ All of the above

From: <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

# Massachusetts Standard - MGL 93H 201CMR17.00

## *Who Needs to Comply?*

According to the OCABR (MA Office of Consumer Affairs and Business Regulation), any business that “**receives, maintains or otherwise has access to personal information**” of MA residents “in connection with the provision of goods and services or in connection with employment” must comply with the regulation.



Source: [www.mass.gov](http://www.mass.gov)

# Questions Related to Non-Compliance

- The law is ambiguous with respect to penalties and fines. Some specific concerns relate to:
  - ✓ **IMPROPER** disposal of data?
  - ✓ Maximum financial impact **PER** Violation?
- What enforcement activities will occur?
- Ramifications regarding reputation and market-place image
  - ✓ lost business?
  - ✓ dealing with irate customers?
  - ✓ mailing out letters and other associated costs?

# A Pragmatic Approach

## *Roadmap to good privacy practices*

1. Identify Risks
2. Inventory Location of Personal Information
3. Limit Collection of Data
4. Routinely Evaluate and Adjust Program
5. Encrypt Hardware and Data Transmissions
6. Obtain Written Guarantees of Adherence from Third-Parties



# A Pragmatic Approach

## *Available resources*

- 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH
  - <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>
- Federal Depositors Insurance Corporation (FDIC) – Graham Leach Bliley Act (GLBA)
  - <http://www.fdic.gov/consumers/consumer/alerts/glba.html>
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security
  - <http://www.hhs.gov/ocr/privacy/>
- International Organization for Standardization (ISO)
  - [http://www.iso.org/iso/catalogue\\_detail?csnumber=42103](http://www.iso.org/iso/catalogue_detail?csnumber=42103)
- PCI Security Standards Council (PCI)
  - <https://www.pcisecuritystandards.org/index.shtml>
- American Institute of Certified Public Accountants (AICPA)
  - <http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/>
- European Union Data Protection Directive (EUDPD)
  - [http://ec.europa.eu/justice\\_home/fsj/privacy/](http://ec.europa.eu/justice_home/fsj/privacy/)

# A Pragmatic Approach

## *Steps to consider...*

- Gain knowledge of your current Personally Identifiable Information (PII) inventory through:
  - Discussions with key functional area personnel
  - Process Mapping with each functional area to identify the movement of PII through out particular processes
- Gather samples of the PII data identified in each process
- Document the inventory gathered in a manner so that the inventory can be maintained



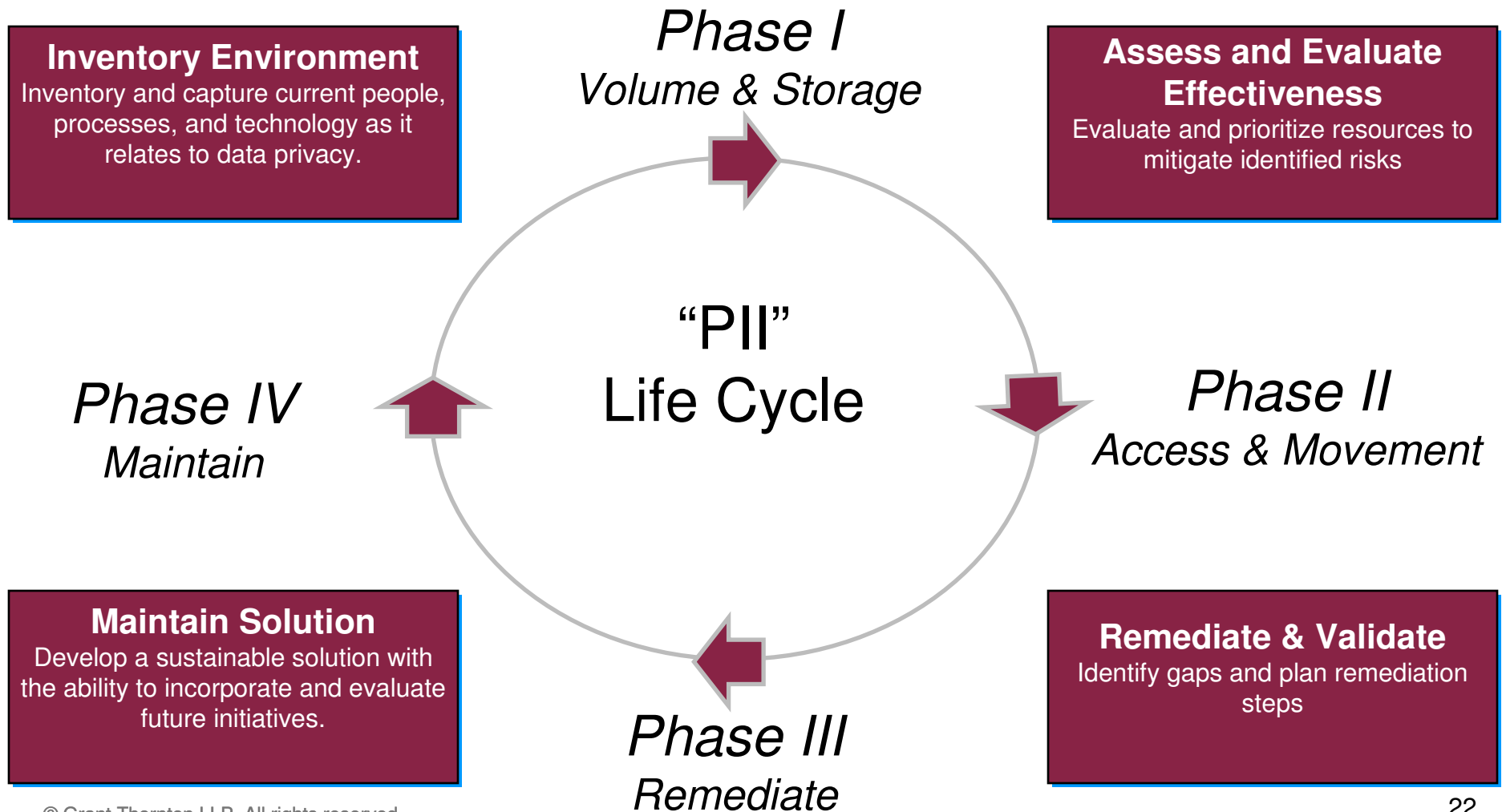
# A Pragmatic Approach

## *Steps to consider...*

- Assess the current privacy environment of the company with Generally Accepted Privacy Principles (GAPP)
- Elements to consider in your evaluation of PII processes and technology:
  - **VOLUME** – the amount and number of transactions on systems
  - **STORAGE** – the form, retention, and purging of information
  - **ACCESS** – the number of employees who touch data and the frequency of data usage
  - **MOVEMENT** – the distribution, third party involvement, and methods of movement

# Grant Thornton “PII” Life Cycle

## *Approach*



# Document Current Processes and Technology

## Inventory Environment

Inventory and capture current people, processes, and technology as it relates to data privacy.

## Privacy Database

<b>Inventory</b> Organizational Structure Process Structure GAPP Questionnaire Process Flow
<b>Privacy Assessment</b> Assess SubProcess View Ratings
<b>Mitigating Controls</b> Answer Questions Maintain Questions Gap Remediation
<b>Analysis</b> Statistics Reports
<b>Administration</b>
<b>About</b>



- Process flow which maps processes for collecting, processing and maintaining PII.
- Evaluate overall privacy practices to GAPP (AICPA).



- Assess PII sub-processes for volume, access, movement and storage.



- Control questions based on identified PII attributes to assist in identifying potential control gaps.



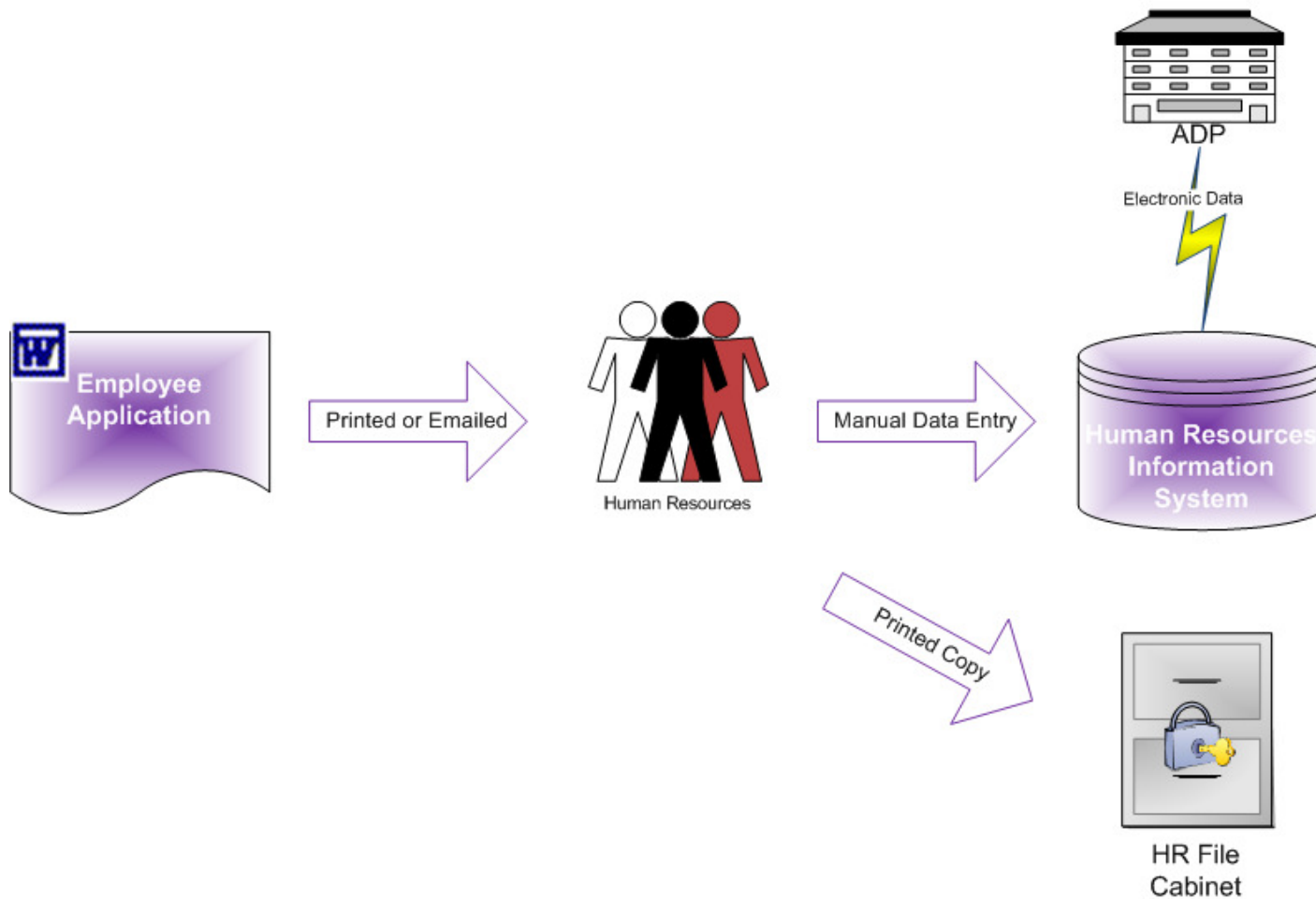
- Reporting and dashboard capabilities for evaluation of PII assessment and mitigating controls.

# Inventory Environment

## HR Department - New Employee Process

### Inventory Environment

Inventory and capture current people, processes, and technology as it relates to data privacy.



# Assess Inherent PII Risks

## Assess and Evaluate Effectiveness

Evaluate and prioritize resources to mitigate identified risks

APPLICATION FORM		
Application Type: <input type="checkbox"/> Post Secondary Program <input type="checkbox"/> Course <input type="checkbox"/> Workshop <input type="checkbox"/> Training Year: _____		
Name of Program: _____ Are you applying for: <input type="checkbox"/> Fall <input type="checkbox"/> Winter <input type="checkbox"/> Spring <input type="checkbox"/> Summer		
Applying As (please check one):		
<input type="checkbox"/> High School Graduate <input type="checkbox"/> High School Equivalency Graduate <input type="checkbox"/> Undergraduate Degree <input type="checkbox"/> Mature Student		
PERSONAL INFORMATION (please print)		
Title: <input type="checkbox"/> Mr. <input type="checkbox"/> Mrs. <input type="checkbox"/> Ms. <input type="checkbox"/> Miss		
Last Name: _____	First Name: _____	Middle Initial: _____
Mailing Address: _____	Town/City: _____	Postal Code: _____
Current Residence (if different from above): _____		
Home Phone Number: _____	Work Phone Number: _____	Fax Number: _____
Email: _____	Date of Birth(D/M/Y): _____	Gender: <input type="checkbox"/> M <input type="checkbox"/> F
SIN or SSN#: _____	Marital Status: <input type="checkbox"/> Single <input type="checkbox"/> Married	# of dependents _____

Internet <input type="checkbox"/>	FTP <input checked="" type="checkbox"/>
Telephone <input type="checkbox"/>	Email <input checked="" type="checkbox"/>
Fax <input type="checkbox"/>	Modem <input type="checkbox"/>
Application <input checked="" type="checkbox"/>	Logical Media <input type="checkbox"/>
Electronic File <input checked="" type="checkbox"/>	Paper <input checked="" type="checkbox"/>

VOLUME		ACCESS		MOVEMENT			STORAGE		
Amount	Volume	#Employees	Frequency	Distribution	3rd Party	Method	Form	Retention	Purge
<input checked="" type="radio"/> High	<input type="radio"/> High	<input type="radio"/> High	<input type="radio"/> High	<input checked="" type="radio"/> Multiple	<input checked="" type="radio"/> Yes	<input checked="" type="radio"/> Electronic	<input checked="" type="radio"/> Logical	<input checked="" type="radio"/> Multiple	<input type="radio"/> Variable
<input type="radio"/> Medium	<input type="radio"/> Medium	<input checked="" type="radio"/> Medium	<input type="radio"/> Medium	<input type="radio"/> Single	<input type="radio"/> No	<input type="radio"/> Physical or None	<input type="radio"/> Physical	<input type="radio"/> Single	<input checked="" type="radio"/> Fixed
<input type="radio"/> Low	<input checked="" type="radio"/> Low	<input type="radio"/> Low	<input checked="" type="radio"/> Low						
Medium		Medium		High			High		
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>OK</span> <span>←</span> <span>→</span> <span style="margin-left: auto;"><b>Overall High</b></span> </div>									

# Evaluate Mitigating Controls

## Assess and Evaluate Effectiveness

Evaluate and prioritize resources to mitigate identified risks

Sub Process Risk Level  
 High  Medium  Low

**Function**  
Payroll

**Department**  
Human Resources

**SubProcess**  
Employee Application

**Process**  
1- New Employee Process

---

21 Employee Application Question(s) 2 of 21 Answered

**Question**  
 Does the FTP connection require user authentication and validation?

Answer	Description
Yes	Each Human Resources associate is given a unique username and password

Navigation: [Left Arrow] [Right Arrow]

# Implement policy and procedure

## Remediate & Validate

Identify gaps and plan remediation steps

*Massachusetts businesses should develop a comprehensive written information security policy (WISP).*

### **The WISP should include:**

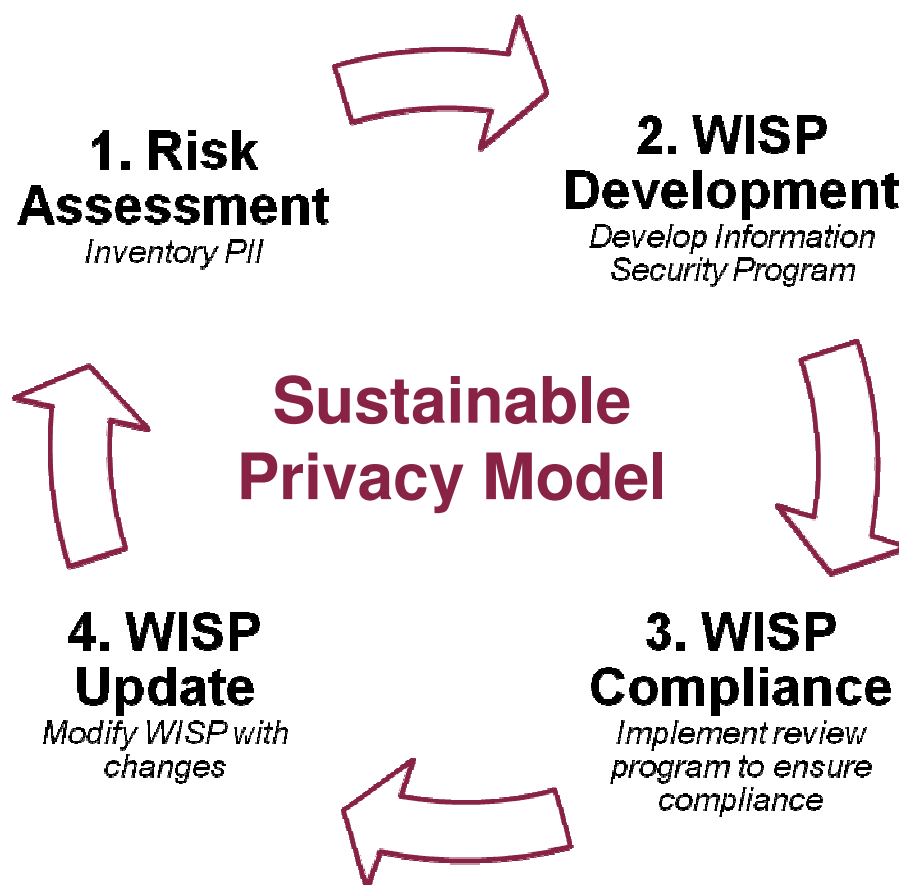
- Governance framework (Monitoring program)
- Privacy Awareness
- Compliance to MA regulation
- Access Control
- Data Security
- Data Retention
- Vendor management
- Encryption



# Sustainable Privacy Model

## Maintain Solution

Develop a sustainable solution with the ability to incorporate and evaluate future initiatives.



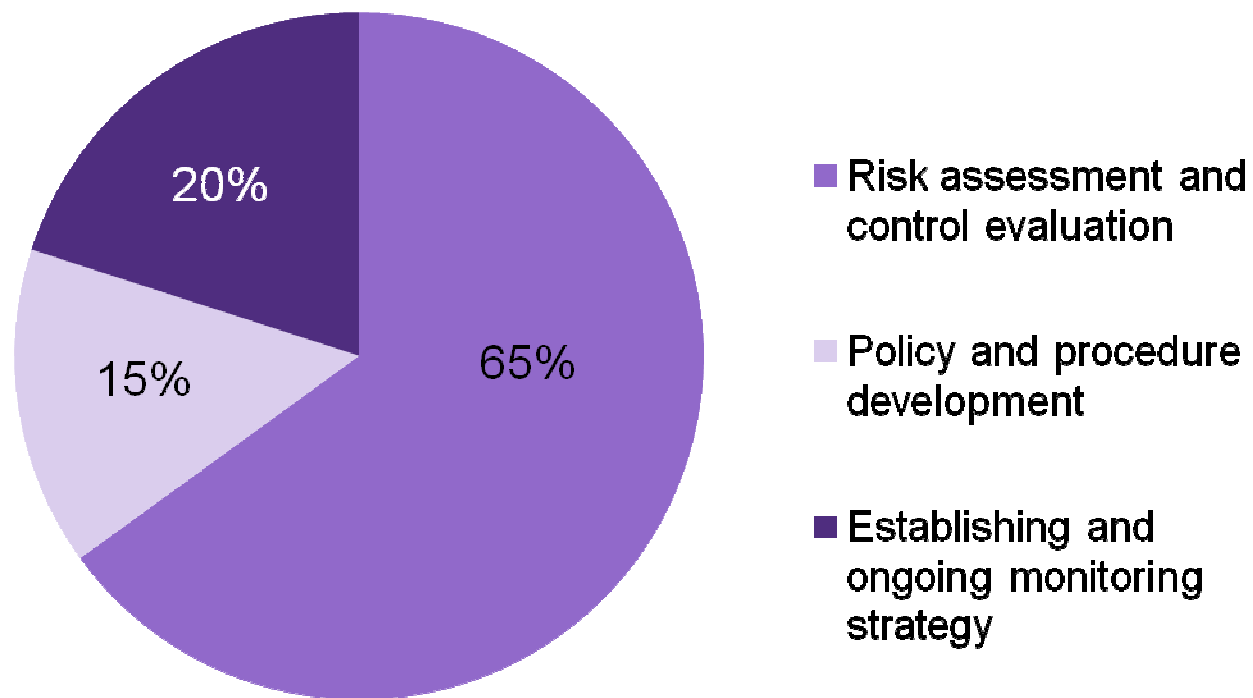
## Question 4

Where have you spent the majority of your time in preparing for Massachusetts compliance?

1. Risk assessment
2. Policy and procedure development (i.e., WISP)
3. Establishing an on-going monitoring a strategy



# Typical Privacy Project Investment



# Summary

- Conducting and documenting your risk assessment will focus your initiative on the needs and vulnerabilities of your organization.
  - Ensure the appropriate development of the WISP and will reduce unnecessary activities
  - Allow your Organization to focus on the execution and protecting of your PII data
- In the event of a breach, regulators will likely begin with an evaluation of your policies and procedures, before assessing fines

Questions?



# Contact information



**Richard Davis**  
Advisory Services Principal  
T: 617.848.4921  
E: Richard.Davis@gt.com



**Dan Costa**  
Advisory Services Senior Manager  
T: 617.848.4941  
E: Daniel.Costa@gt.com



# Thank you for joining us...

For more information about the firm, please visit

[www.GrantThornton.com](http://www.GrantThornton.com)



**Disclaimer**

This document supports Grant Thornton LLP's marketing of professional services, and is not written advice directed at the particular facts and circumstances of any person. If you are interested in the subject of this document we encourage you to contact us or an independent advisor to discuss the potential application to your particular situation. Nothing herein shall be construed as imposing a limitation on any person from disclosing the treatment or structure of any matter addressed herein. To the extent this document may be considered to contain written advice, any written advice contained in, forwarded with, or attached to this document is not intended by Grant Thornton to be used, and cannot be used, by any person for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.