ARE YOU READY FOR A CFPB INVESTIGATION OF YOUR PRIVACY COMPLIANCE?

Start by Getting a Handle on Your Information

Jordan Lawrence™

Michael Thurman

Loeb & Loeb

Partner
Co-Head, CFPB Task Force

Rebecca Perry

Jordan Lawrence

Director Professional Services
CIPP/US/G

THE USUAL DISCLOSURES

This presentation is for informational and educational purposes only. It is not intended to provide legal analysis or advice on any specific set of facts and should not be relied upon as such. Please consult with an attorney who is authorized to practice law in the applicable jurisdiction regarding any specific questions and issues.

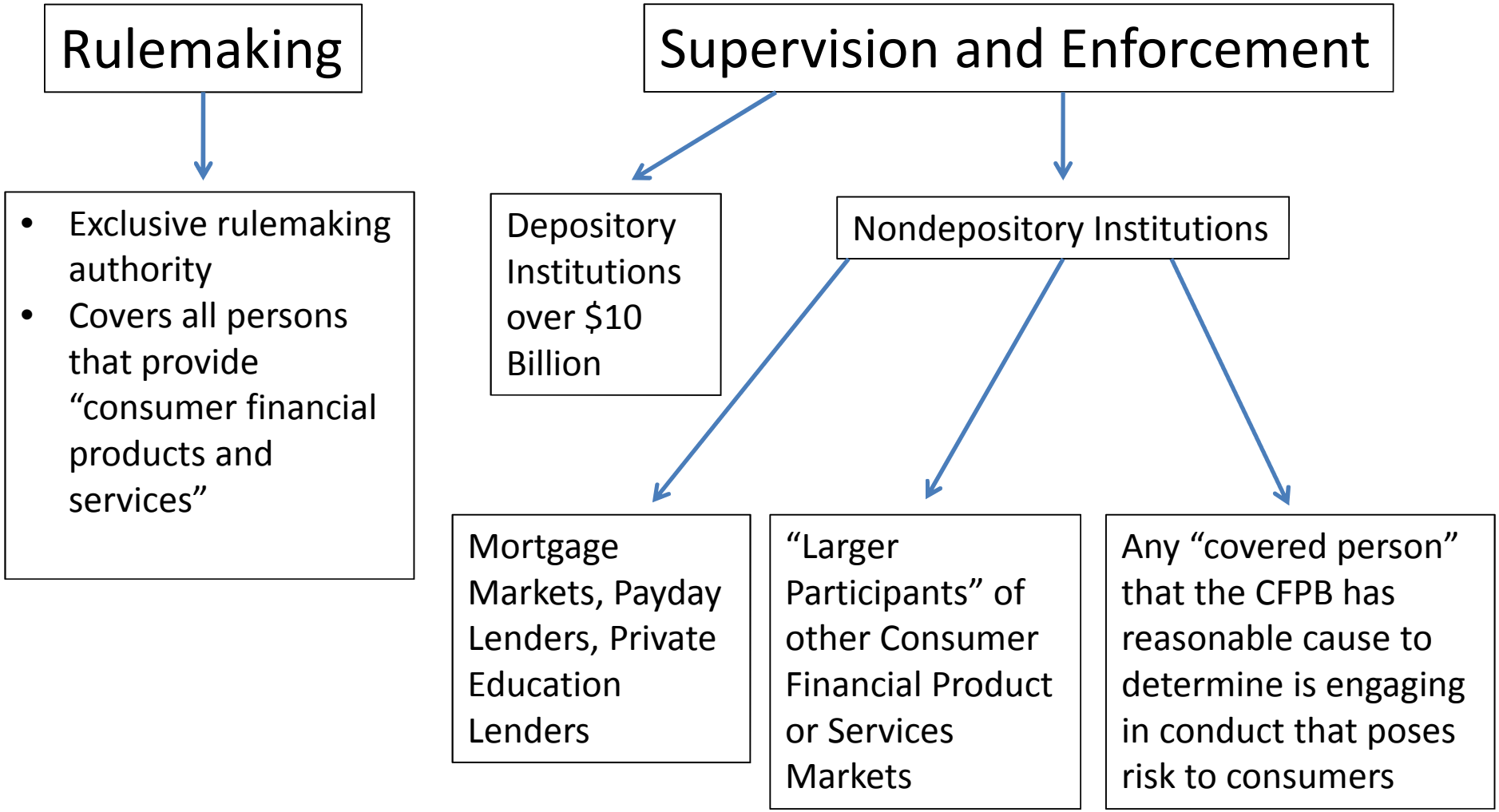
CFPB – THE BASICS

- Washington's newest federal agency
- Created by the Dodd-Frank Act of 2010
- Separately-funded by the Federal Reserve
  - 2013 expenditures: **$518 million**
  - 2014 budget cap: **$608 million**
  - Independent of the Congressional appropriation process
  - Uses civil penalties for consumer restitution and education
  - Civil penalties collected to date: at least $93.8 million
- Headed by a single Director appointed by the President
  - Consists of at least 1,380 employees
  - **About half of those assigned to supervision/enforcement**
  - **90% of those are attorneys and paralegals**

THE CFPB'S MISSION

- Primary rulemaking, supervisory and enforcement authority over *entities that offer consumer financial products and services*.
- Includes banks and "covered" non-banks.
- Responsible for ensuring that markets for consumer financial products and services are **fair**, **transparent** and **competitive.**

CFPB AUTHORITY



LAWS ENFORCED BY THE CFPB

Authority over a wide range of "enumerated" federal laws, including:

- Consumer Financial Practices Act (CFPA)
  - Unfair Deceptive and Abusive Practices (UDAAP)
- Federal Trade Commission Act (joint authority with the FTC)
- Truth in Lending Act (TILA)
- Real Estate Settlement Practices Act (RESPA)
- Mortgage Lending Acts
- Equal Credit Opportunity Act (ECOA)
- Fair Credit Reporting Act (FCRA) sections
- Fair Debt Collection Practices Act (FDCPA)
- Gramm-Leach Bliley Act (GLBA)

PRIVACY AND THE CFPB

Supervises and enforces privacy laws with respect to businesses that provide “consumer financial products or services” based on two primary statutory sources:

1. Gramm-Leach-Bliley Act (GLBA)
2. Unfair, Deceptive and Abusive Acts & Practices (UDAAP) under the Consumer Financial Protection Act (CFPA)

CFPB AUTHORITY: GRAMM-LEACH-BLILEY ACT (GLBA)

- Imposes requirements on “financial institutions” to disclose privacy policies and provide consumers rights to opt-out from having their personal information shared.
- Exercised thus far primarily through CFPB’s Supervision and Examination Manual:
  - 144-page “Privacy of Consumer Financial Information” section.
  - Provides guidance and checklists testing for compliance with the requirements of the GLBA.
  - Available on the CFPB’s website - www.consumerfinance.gov

CFPB AUTHORITY: UNFAIR, DECEPTIVE AND ABUSIVE ACTS & PRACTICES (UDAAP)

- FTC has made extensive use of its "unfair and deceptive" authority as a basis for privacy enforcement actions:
  - Accretive Health data theft settlement
  - Wyndham Hotel data breach litigation
  - Medical transcript services settlement (FTC's 50th data security case)
  - Home security video system settlement (TRENDnet, Inc.)
  - Unauthorized surveillance by rent-to-own computers
- CFPA authorizes CFPB actions based on "unfair," "deceptive" **and "abusive"** acts and practices.
  - "Unfair" and "Deceptive" acts and practices are well-defined through FTC Act and state ("Little FTC") actions.

CFPB AUTHORITY: UNFAIR, DECEPTIVE AND ABUSIVE ACTS & PRACTICES (UDAAP)

What is an "Abusive" act or practice?

1. One that interferes with consumer's ability to understand a term or condition.
2. One that takes unreasonable advantage of a consumer's:
   a. **Lack of understanding of risks**, costs, conditions.
   b. **Inability to protect own interests.**
   c. **Reasonable reliance on the seller to act in their interest.**

CFPB PRIVACY ENFORCEMENT ACTIONS

- No privacy enforcement actions have been brought by the CFPB to date.
- However, many reasons to expect future CFPB actions!
  - Use of enforcement actions to communicate initiatives.
  - CFPB's perceived need for development of its UDAAP authority, especially defining "abusive" conduct.
  - "Anything you can do, I can do better, FTC!"

GETTING READY FOR A CFPB INVESTIGATION

1. Learn and understand the CFPB's investigative process.
2. Determine what laws and regulations apply to your business.
3. Use the agency's Examination and Supervision Manual to determine what examiners will be looking at and for.
4. Perform "gap analyses" to identify and assess any deficiencies in your company's procedures.
5. Develop policies and procedures to respond to those deficiencies.
6. Develop and implement training materials and courses to train employees and agents on new procedures.

GETTING READY FOR A CFPB INVESTIGATION

7. Develop documentation that demonstrates the implementation of the new procedures.
8. Develop audit and monitoring systems to ensure (and document) that new procedures have been implemented.
9. Review and improve policies and procedures based on the results of audits and monitoring.
10. Involve management throughout the entire process of evaluating, developing, improving and approving policies and procedures and feedback received regarding their effectiveness.

CIVIL INVESTIGATIVE DEMAND ("CID")

1. Primary device for gathering documents or information.
2. May also be called a "civil subpoena."
3. Usually includes a general statement describing the nature of the investigation.
4. Requires production of various categories of documents and information related to the investigation.
5. Sometimes requires testimony from a specific identified person or from a "person with knowledge."

SIX KEY STEPS FOR RESPONDING TO AN INVESTIGATION

1. Evaluate the Requests With Your Legal Counsel.
2. Immediately Get Your IT Department Involved.
3. Preserve all Potentially Relevant Information.
4. Contact the CFPB.
5. Decide Whether to Challenge the CID
6. Respond as Quickly and Completely as Possible.

STEP 1: EVALUATE THE REQUESTS WITH YOUR COUNSEL

1. Assess the company's role in the investigation (Is your company a "target" or merely a "person of interest"?)
2. Evaluate the legal issues and potential violations implicated by the investigation.
3. Identify potential sources of documents/information responsive to the requests.
4. Assess potential problems in responding to the requests as written and determine whether changes can be made to the wording and/or relevant time periods to narrow the requests.
5. Ensure that personnel limit any discussions about the investigation to privileged communications.

STEP 2: IMMEDIATELY GET YOUR IT DEPARTMENT INVOLVED.

1. Identify all potential sources of electronic information responsive to the government's requests, including all potential custodians of records.
2. Disengage any systems that automatically delete, archive or modify emails, voicemail or other documents covered by the request.
3. Evaluate how to efficiently and economically retrieve the data requested in the CID.
4. Estimate the amount of data that will be involved in responding to the requests.
5. Identify electronic discovery vendors capable of ingesting, searching and producing the data in requested formats.

STEP 3: PRESERVE ALL POTENTIALLY RELEVANT INFORMATION

1. Shut down any systems that automatically delete, archive or modify emails, voicemail or other documents covered by the request.
2. Immediately issue a legal hold to all employees, contractors and other parties that may possess documents or information relevant to the investigation.

STEP 4: CONTACT THE REGULATOR

1. Discuss proposed changes to the CID requests to narrow the amount of data to be produced.
2. Discuss any anticipated problems in completing the production on a timely basis, including discussing relevant IT issues and/or limitations, document retention policies that will make data unavailable, etc.

3. Arrange for a “rolling production,” if needed, initially providing information that is readily available, followed by additional responses as soon as they can be produced.

STEP 5. EVALUATE WHETHER TO CHALLENGE THE CID

1. Identify whether there are legal challenges that must be raised before the responses are due.
2. Determine whether these challenges can be resolved through negotiation with the CFPB representatives.
3. Comply with the CFPB's **10-day deadline** for "meeting and conferring" about all potential objections
4. Document the "meet and confer" sessions in writing.
5. Determine whether the company is willing to waive confidentiality and any privileges that are addressed in any written challenges to the CID.
6. File any petition to quash the CID within the CFPB's **20-day deadline**.

STEP 6: RESPOND AS QUICKLY AND COMPLETELY AS POSSIBLE

1. Prompt and complete responses to CID requests are an excellent way to demonstrate the company's compliance with applicable laws and regulations.
2. Our experience has been that companies that can quickly provide relevant documents and information in response to a government investigation achieve better outcomes.

REQUESTS FOR ORAL TESTIMONY

1. Not typical, but regulators can compel witness testimony.
2. Similar to a civil deposition - the witness is sworn in, questioned by an examiner, the testimony is recorded and transcribed by a stenographer.
3. The witness may have counsel present, but counsel's rights to object to questions or conduct follow up examination may be limited or nonexistent.

POTENTIAL INVESTIGATION OUTCOMES

1. The agency takes no further action.
2. The agency requests for additional documents, information or oral testimony.
3. The agency offers a proposed consent order (settlement).
4. The agency initiates a civil enforcement action.
5. In very rare cases, the agency (or a counterpart) initiates a criminal enforcement action.

KEY ELEMENTS OF PRIVACY PROCEDURES

1. Disclose your privacy collection, use and sharing policies as required by GLBA and applicable state privacy laws.
2. Designate one or more employees to coordinate your information security program.
3. Identify and assess the risks to customer information in each relevant area of the company's operations, and evaluate the effectiveness of the current safeguards for controlling these risks.
4. Design and implement a safeguards program, and regularly monitor and test it.

KEY ELEMENTS OF PRIVACY PROCEDURES

5. Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information.
6. Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.
7. Assess what personally identifiable information is collected and maintained by your company (and its affiliates, vendors, etc.).
8. Keep only what is needed for your business for only as long as it is needed.

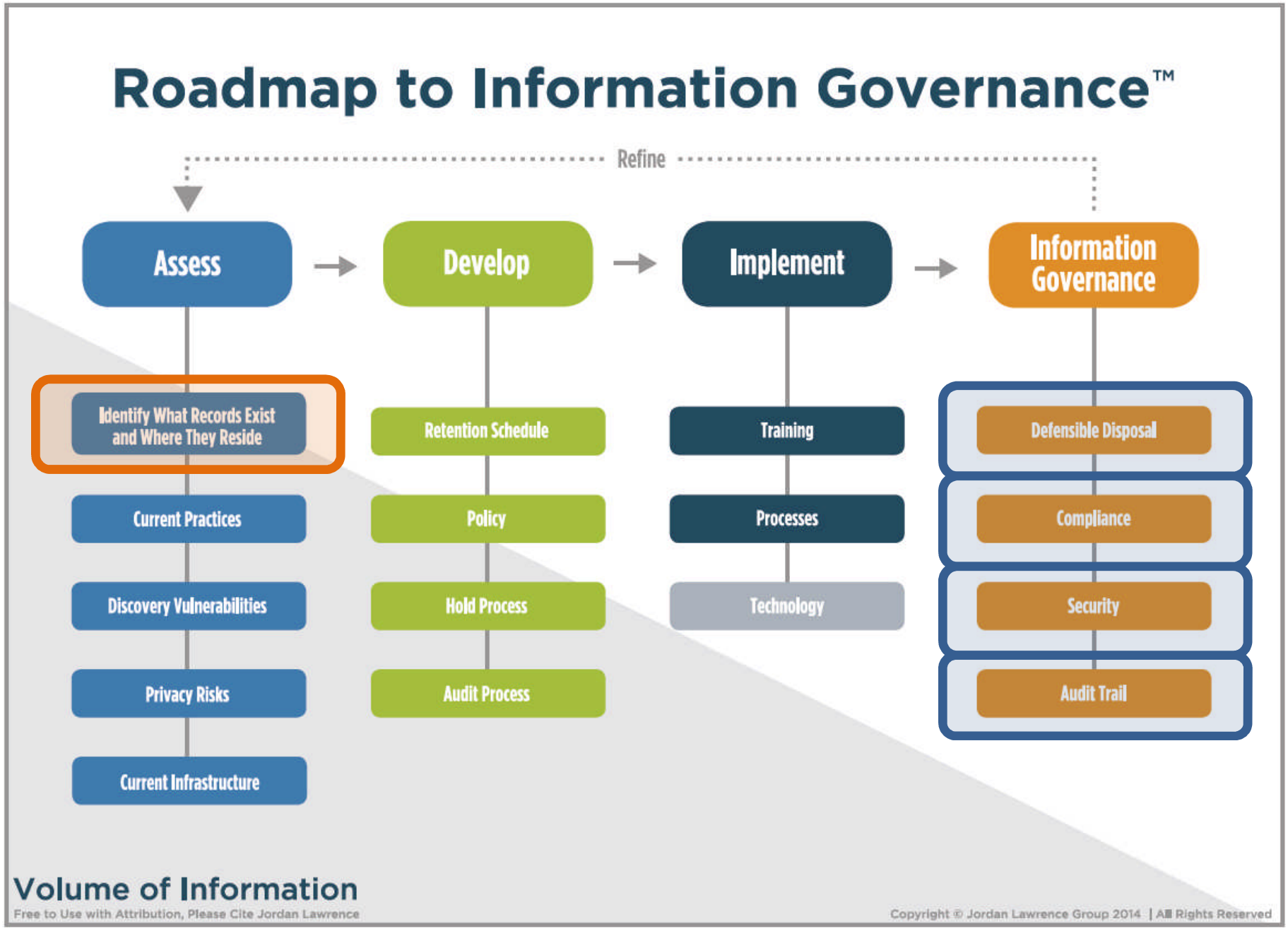
KEY ELEMENTS OF PRIVACY PROCEDURES

9. Protect the information your company keeps:
   - Physical and electronic security/firewalls
   - Wireless and remote access
   - Digital copiers
   - Breach monitoring and detection measures
   - Employee hiring, training, password management
   - Security practices of contractors and service providers
10. Securely dispose of data that is no longer needed.
11. Create a plan for responding to security incidents, including complying with reporting requirements.

IT'S THE LAW

PRIVACY BREACHES

STORAGE COSTS


Roadmap to Information Governance™
Refine
Assess
Develop
Implement
Information Governance
Identify What Records Exist and Where They Reside
Current Practices
Discovery Vulnerabilities
Privacy Risks
Current Infrastructure
Retention Schedule
Policy
Hold Process
Audit Process
Training
Processes
Technology
Defensible Disposal
Compliance
Security
Audit Trail
Volume of Information
Free to Use with Attribution, Please Cite Jordan Lawrence
Copyright © Jordan Lawrence Group 2014 | All Rights Reserved

DEVELOP A RECORDS INVENTORY

1. Identify Records
2. Tag Records
3. Storage & Movement

IDENTIFY RECORDS

- Accident/Incident Records
- Advertising Records
- Benefit Records
- Budget Records
- Contracts & Agreements
- Coupon Records
- Credit Approvals
- Customer Information
- Customer Orders
- Employee Medical Files
- Gift Card Functions
- Payment Records
- Sales Receipts

TAG RECORDS

BUSINESS NEEDS

SENSITIVITY

Cardholder Data

Corporate Sensitive

Government IDs

Intellectual Property

PII

Bio Metric

Patient Health Info.

REQUIREMENTS

DOL

PCI

GLB

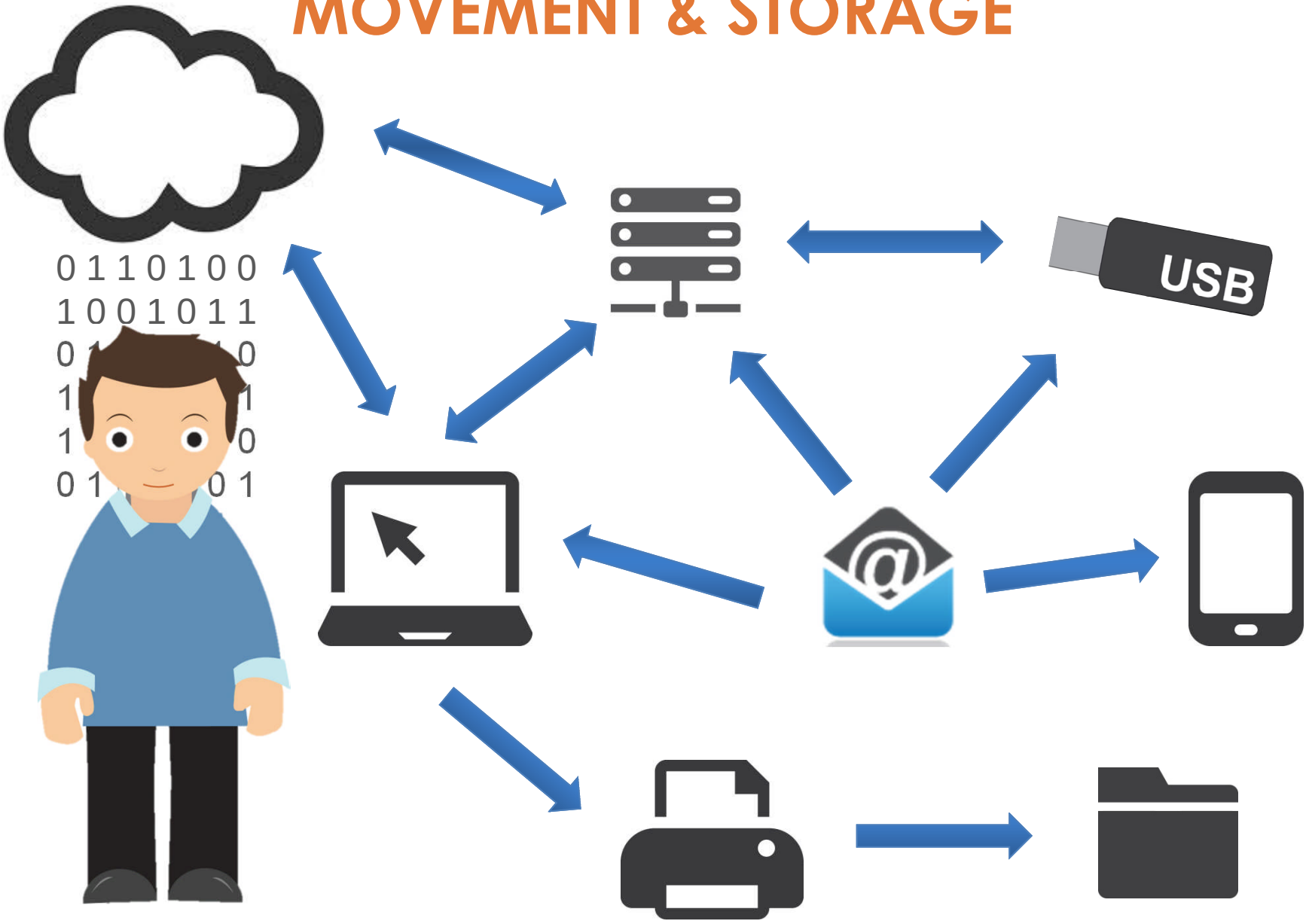
HIPAA

OSHA

SEC

State Privacy Laws

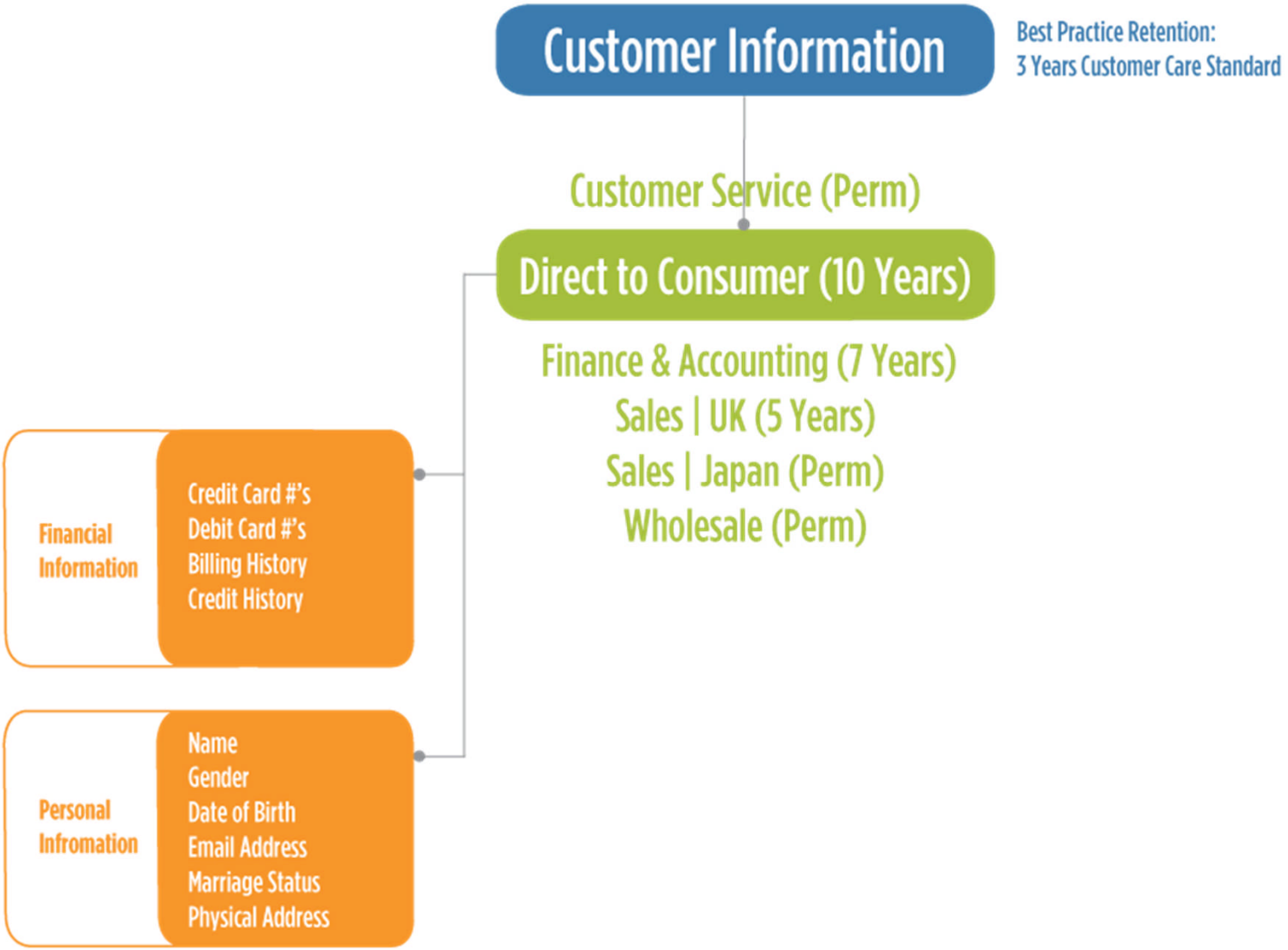
MOVEMENT & STORAGE

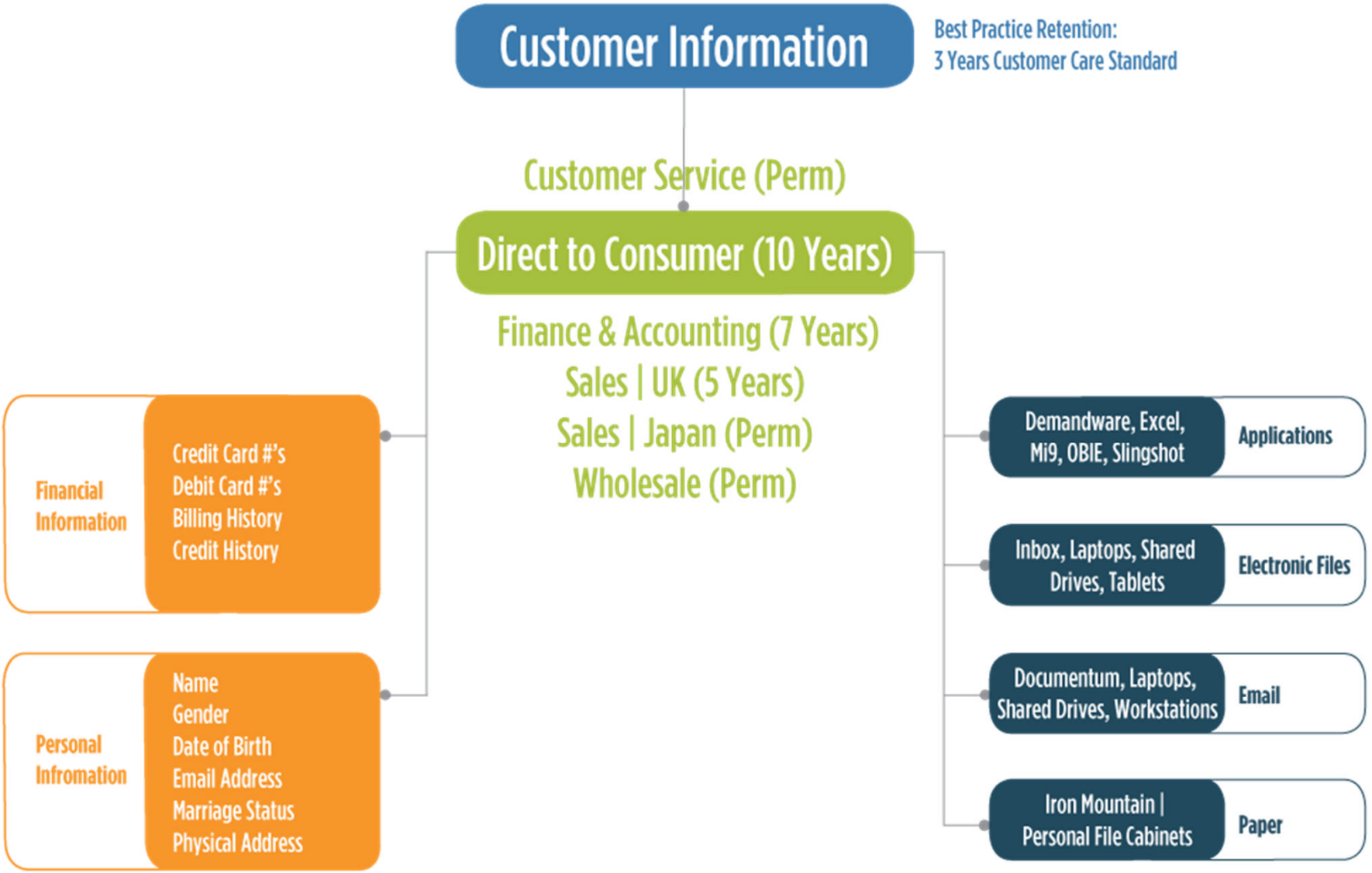


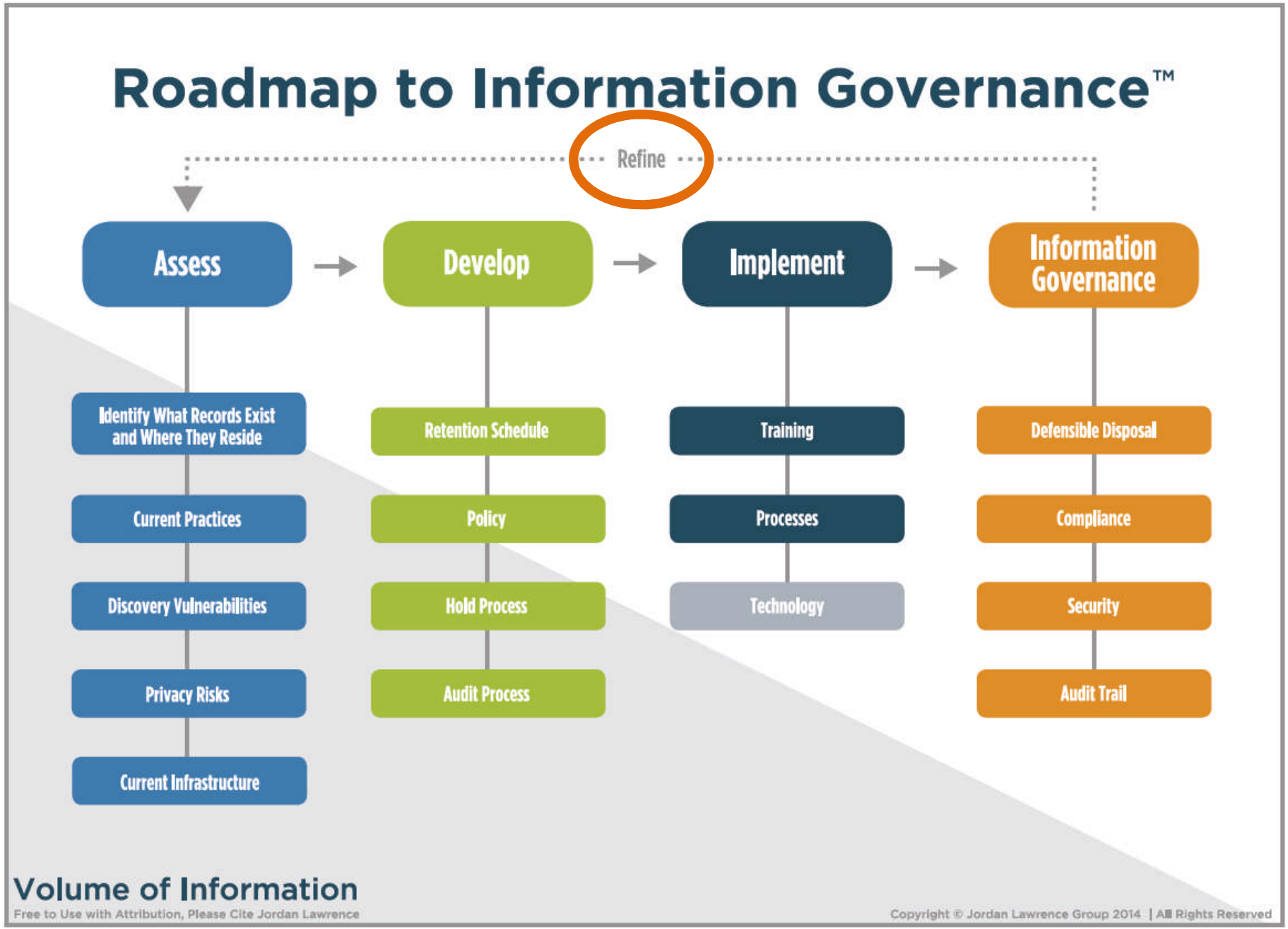
Customer Information

Best Practice Retention:
3 Years Customer Care Standard


Customer Information
Best Practice Retention:
3 Years Customer Care Standard
Customer Service (Perm)
Direct to Consumer (10 Years)
Finance & Accounting (7 Years)
Sales | UK (5 Years)
Sales | Japan (Perm)
Wholesale (Perm)


Customer Information
Best Practice Retention:
3 Years Customer Care Standard
Customer Service (Perm)
Direct to Consumer (10 Years)
Finance & Accounting (7 Years)
Sales | UK (5 Years)
Sales | Japan (Perm)
Wholesale (Perm)
Financial Information
Credit Card #'s
Debit Card #'s
Billing History
Credit History
Personal Infromation
Name
Gender
Date of Birth
Email Address
Marriage Status
Physical Address


Customer Information
Best Practice Retention:
3 Years Customer Care Standard
Customer Service (Perm)
Direct to Consumer (10 Years)
Finance & Accounting (7 Years)
Sales | UK (5 Years)
Sales | Japan (Perm)
Wholesale (Perm)
Financial Information
Credit Card #'s
Debit Card #'s
Billing History
Credit History
Personal Infromation
Name
Gender
Date of Birth
Email Address
Marriage Status
Physical Address
Demandware, Excel, Mi9, OBIE, Slingshot
Applications
Inbox, Laptops, Shared Drives, Tablets
Electronic Files
Documentum, Laptops, Shared Drives, Workstations
Email
Iron Mountain | Personal File Cabinets
Paper


Roadmap to Information Governance™
Refine
Assess
Develop
Implement
Information Governance
Identify What Records Exist and Where They Reside
Current Practices
Discovery Vulnerabilities
Privacy Risks
Current Infrastructure
Retention Schedule
Policy
Hold Process
Audit Process
Training
Processes
Technology
Defensible Disposal
Compliance
Security
Audit Trail
Volume of Information
Free to Use with Attribution, Please Cite Jordan Lawrence
Copyright © Jordan Lawrence Group 2014 | All Rights Reserved

COMPLY WITH LAWS

REDUCE RISKS

REDUCE COSTS

QUESTIONS?

Michael Thurman

Loeb & Loeb

Partner
310.282.2122
mthurman@loeb.com

Rebecca Perry

Jordan Lawrence

Director Professional Services
636.821.2251
rperry@jordanlawrence.com