Gable
Consulting
Document-Based Information Management

ARMA Liberty Bell Chapter

October 13, 2011

Understanding RIM Legislation, Regulations and ISO Standards

Julie Gable,
CRM, CDIA, FAI

Overview

- The difference between regulations and standards
- Broad based & industry specific regulatory requirements
- Important records-related standards
- Trends in standards and regulations

Regulations vs. Standards

- Laws
  - Compliance is mandatory; Must meet all applicable laws in countries where firm does business
    - U.S. National
    - State
    - Local
    - European Union
    - Country-specific
- Regulations
  - Compliance is mandatory for industries to which regulations apply

- Standards
  - Compliance with standards is always voluntary;
  - However, many standards provide guidance for meeting regulatory requirements
- Guidelines and Codes of Practice
  - May provide guidance for meeting regulatory requirements

Nutshell: Regulations vs. Standards

- Regulations
  - What you must do
  - What happens if you don’t

- Standards
  - An approach to doing what you must do
  - A basis for the decisions you made

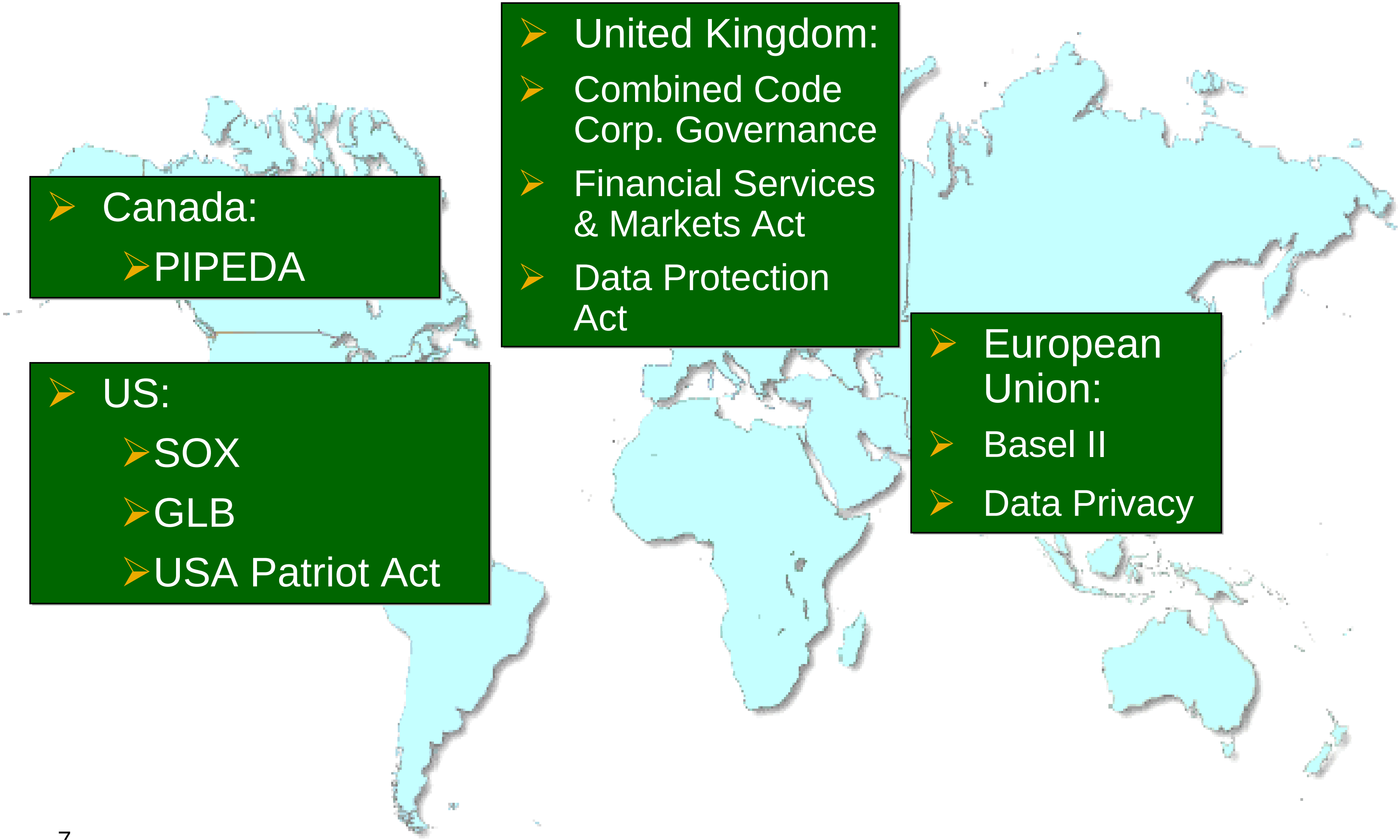
Sources of Confusion

- Secondary sources (articles, seminars, etc.)
  - Writers aren’t lawyers
  - Trade publication articles edited to fit space
  - Whitepapers focus on issues that vendor product can solve
- Imprecise language
  - Mixing mandatory regulations with standards, guidelines, etc.

Sources of Confusion

- Regulations change over time
  - Final rules
  - Deadline changes
  - Test cases
- Standards evolve from other standards
  - BS 7799 (security) = ISO 17799
  - Dublin Core = ISO 15836

Regulation: A Worldwide Trend



- Canada:
  - PIPEDA
- US:
  - SOX
  - GLB
  - USA Patriot Act

- United Kingdom:
- Combined Code Corp. Governance
- Financial Services & Markets Act
- Data Protection Act

- European Union:
- Basel II
- Data Privacy

Broad-based Laws: Apply to all or many industries	Industry Specific Regs: Apply to companies within certain industries
Sarbanes-Oxley (Corp. Governance) PIPEDA (Privacy) USA PATRIOT Act (Anti-Terrorism)	Financial Services
	SEC 17a-3 & a-4
	Dodd-Frank
	Basel II
	Gramm-Leach Bliley
	Public Sector
	FOIA
	Right to Know Laws
	Healthcare
	HIPAA
	21 CFR 11

Sarbanes-Oxley Summary

Applies to:	All publicly traded US companies; All companies that list on US stock exchanges;
Purpose:	Transparency in corporate governance and financial reporting
Major Provisions:	
Sections 401-409:	Management assessment of internal controls in annual report [404]
Section 801-807:	Must keep audits and review of financial statements 7 years [802]
Section 1101-1107:	Criminal penalties for willing destruction, alteration or falsification of records [1102]

PIPEDA Summary

Country of Origin	Canada
Applies to:	All Canadian commercial entities, including foreign companies with subsidiaries, headquarters, or offices in Canada
Purpose:	Protection of personal information held or transferred to third parties
Major Provisions:	Identify reasons for collecting personal info Obtain individual’s consent Limit information collected Retain personal information only as long as needed Assure accuracy, safeguard against theft Open information policies to inspection Allow individuals access to their info

USA PATRIOT Act Summary

Applies to:	Communications providers: Cable companies, phone companies & Internet Service Providers Banking and financial institutions
Purpose:	Expand search and surveillance powers of domestic and foreign intelligence agencies
Provisions:	
Section 215:	Court orders to obtain individuals' library, financial, phone, travel and medical records
Section 216:	Records regarding Internet traffic including email, web page and IP addresses
Section 319:	Financial institutions must produce records relating to accounts within 120 hours

Industry Specific: SEC Regs

SEC 17a-3 :	Specifies records to be kept regarding transactions, assets, customers, trades, employees, and internal broker-dealer systems
Applies to:	Stock exchange members, brokers, & dealers
SEC 17a-4:	Specifies retention times for records to be kept regarding transactions, assets, customers, trades, employees, and internal broker-dealer systems
Provisions:	Records in 17a-3: Kept 6 years, the first 2 years in an easily accessible place Communications: Originals of all communications received and sent (including inter-office memoranda) kept 3 years Customer records: Kept 6 years after close of account

Dodd-Frank Title IV

Origin	U.S.
Applies to:	Investment Advisers to Private Funds
Purpose:	Gives SEC monitoring power via inspections and examinations
Highlights:	All records of private fund subject to periodic & for cause audits. Not limited to records required to be kept by law. Must make copies or extracts available Must file reports containing whatever info SEC deems necessary for protection of investors or assessment of risk Must present data in newly prescribed format.

Federal Freedom of Information Act

Applies to:	Federal government agencies
Purpose:	Governs requests for public records, including electronic records
Provisions:	Agency provides record in any format requested Searches to fulfill records requests include electronic records 20 days to determine whether to comply with request

PA Right to Know Laws

Applies to:	Commonwealth agencies; All legislative, judicial & local agencies; Private entities that perform government functions; All state universities; Agency-related independent entities
Purpose:	Provide greater access to government records in PA
Provisions:	Creates Office of Open Records Presumes government record is public; agency must demonstrate why record should not be turned over Includes any information that documents an agency's transactions or activiies Exceptions do apply (HIPAA, taxpayer records, personnel records, criminal investigations, etc.) Initial response in 5 days; agency has 30 calendar days; can charge for copying

Industry Specific: HIPAA

Applies to:	Health plans, clearinghouses, certain healthcare providers, prescription drug card sponsors (Medicare);
Purpose:	Protect individually identifiable health information; Foster electronic exchange of healthcare information
Highlights:	Privacy Rule: Stipulates protection of individually identifiable health information Security Rule: Designed to ensure confidentiality, integrity and availability of electronic patient data Standard Unique Employer Identifier - uses Employer Identification Number or tax ID. National Provider Identifier for Medicare & Medicaid

Regulatory Trends

- Broader legislation
  - Especially when reactive
- More records under scrutiny
  - Dodd-Frank
- Enforcement depends on $
  - PIPEDA case
  - HIPAA cases
- Letter vs. spirit of law

Standards

Uses for Standards

- International, national consensus on professional best practice
  - Advice on specific aspects of RM issues
- Starting point for initiatives
  - Lists of issues, questions, decision points
- Assessment of existing RM programs
- Aspiration point for developing RM programs
  - Ways to prioritize activity
- Strategic realignment of RM

Sources of Standards

- International Standards Organization (ISO)
- Country-specific standards bodies
  - American National Standards Institute (ANSI)
  - British Standards Institute (BSI)
- Industry consortiums
  - Electronic Discovery Reference Model
- Professional organizations
  - ARMA International, AIIM
  - Information Systems Audit and Control Association

Important Records-related Standards

Standard	Title:
ISO 15489 Parts 1 & 2	Information & Documentation – Records Management
ISO/TR 26122	Information & Documentation – Work Process Analysis (DIRKS – Australia)
ISO 23081 Parts 1, 2 & 3	Managing Metadata for Records
ISO 15836	Meta data for resource description (the Dublin Core)
ISO 16175 Parts 1, 2 & 3	Guidelines and functional requirements for digital records management systems
ISO/TR 13028	Implementation guidelines for digitization of records (images)
ISO 30300 & 30301	Management Systems for Records (In development)

ISO 15489

Part 1

- Non-RIM managers, individuals, all personnel
- Guidance on organization responsibilities for records
- Describes principles of RIM programs
- Explains records authenticity, reliability, integrity, usability

Part 2

- RIM Professionals
- Adequacy considerations for
  - □ Policies
  - □ Strategies
  - □ Design & implementation
  - □ Processes & controls
  - □ Monitoring & auditing
  - □ Training

ISO 15489 Part 2 - Key Points

- Principles of Records Management Programs
  - Determining which records should be created
  - Deciding form and structure
  - Metadata requirements
  - Retrieval requirements
  - How to organize records
  - Assessing risks
  - Preserving records
  - Complying with legal and regulatory requirements
  - Security
  - Records retention
  - Improvement opportunities

ISO/TR 26122: 2008

- Practical application of theory outlined in 15489
- Work process analysis for records creation, capture & control
- Two types of analyses:
  - Functional (Decompose functions into processes)
  - Sequential (Flow of transactions)
- Not workflow automation

ISO 23081-1 Metadata for Records
Part 1: Principles

- Guide to understanding, implementing and using metadata within ISO 15489 framework
- Addresses relevance of RM metadata in business processes
- Roles and types of metadata for RM processes
- Sets framework for managing those metadata

Metadata at record capture

- Context of record creation
- Business context
- Agents involved
- Record content, appearance, structure and technical attributes
    - Record structure
        - Physical or technical structure
        - Logical structure, i.e., relationships between data elements comprising the record

ISO 23081-1:2006

Metadata Management

- "Metadata about the record and metadata accruing in its management form a metadata record which must be managed"
- "It is essential to keep this metadata record at least as long as the original record exists"
- "In disposition, metadata may still be needed to account for existence"

Ibid.

ISO 23081-2 Metadata for Records Part 2:

- Framework for defining metadata elements from Part 1
  - Standardize description, enable interoperability of records between systems
- Identify critical decision points
  - Issues in implementing metadata
  - Explain options for addressing issues
  - Decision paths in implementing metadata

ISO 23081-3 Metadata for Records

Part 3: Self-assessment

- Helps to identify
  - Current state of organizations metadata capture & management
  - Priorities of what to work on next
  - Development progress
  - System and project readiness when including records metadata functionality in a system

ISO 15386: The Dublin Core

Standard for information resource description across domains

Library oriented

- Descriptive meta data elements:
  - Title
  - Creator
  - Subject
  - Description
  - Publisher
  - Contributor
  - Date
  - Type
  - Format
  - Identifier
  - Source
  - Language
  - Relation
  - Coverage
  - Rights Management

ISO 16175 - Software

Part 1	Fundamental principles and functional requirements for software used to create and manage digital records in office environments
Part 2	Set of functional requirements for digital records management systems in office environments (ERMS & ECMS)
Part 3	Guidelines for the appropriate identification and management of evidence (records) of business activities transacted through business systems

DeFacto Standards:
Records Management Software

Standard	Title:
DoD 5015.2	Design Criteria Standard for Electronic Records Management Software Applications (2007)
U.K. National Archives	ERMS, aka PRO2
MoReq 2	Model Requirements of the European Union

ISO 30300 & 30301– MSR series of standards

- MSRs are aimed at management to:
  - Communicate re benefits of good RM
  - Get commitment for leadership, funds & people
  - Support accountability and effective business
  - Direct & control an organization with regard to records (ISO/DIS 30300)
  - Get records on agenda of top management

Other examples of MSS

- ISO 90001 –
  - Quality Management Systems
- ISO 14001 –
  - Environmental Management Systems
- ISO 27001 –
  - Information Security Management Systems

ISO 30300 & 30301: Management System for Records

- For a list of frequently asked questions & very good information go to
- http://project-consult.net/files/N1069_FAQ_on_ISODIS_30300_and_30301.pdf

Standards at a Glance

Topic	Standard(s)
Management Level	ISO 30300 & 30301 (in progress)
Records Management – General	ISO 15489 Parts 1 & 2
Analysis Techniques	ISO TR 26122
Digitizing Paper Records	ISO TR 13028
Long-term Storage & Access	ISO TR 18492, 15801, ISO 14721
Records Metadata	ISO 23081, Parts 1, 2 & 3
Descriptive Metadata	ISO 15836
Software Specifications	ISO 16175, Parts 1, 2 & 3

Gable
Consulting
Document-Based
Information
Management

Thank You

juliegable@verizon.net

www.gableconsulting.com