A Complimentary Webinar Series:

Building a Data Privacy Compliant Records Management Program

Building an Effective *and* Compliant Records Management Program

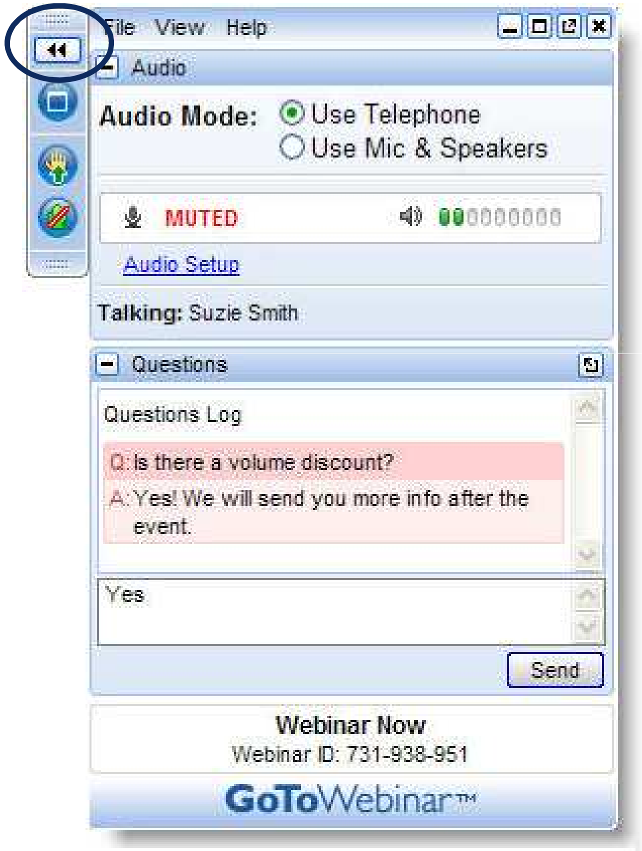
November 16, 2011

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS®
DOCUMENT MANAGEMENT

Welcome!

- **Housekeeping…**
  - Control panel on the right side of your screen.
  - Audio
    - **Telephone**
    - **VoIP**
  - Submit “Questions” in the pane on the control panel and we will address questions at the end of the session.
  - Minimize pane during presentation – Click double arrows icon top-left of the control panel.
  - Need help? Call 800-263-6317



Audio Mode: ● Use Telephone ○ Use Mic & Speakers

Talking: Suzie Smith

Questions Log

Q: Is there a volume discount?

A: Yes! We will send you more info after the event.

Yes

Webinar Now

Webinar ID: 731-938-951

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Introductions-Sponsors

PIVOT GROUP
Armed with Information Security Knowledge

Independent Audit, Assessment and Compliance Firm providing exclusively Data Privacy and Protection Services.

CINTAS
DOCUMENT MANAGEMENT

Cintas Document Management

Cintas was the first North American AAA NAID Certified and PCI-DSS Compliant Provider. Cintas has service locations throughout the entire US, parts of Canada and Europe and offers document imaging, records storage and secure shredding that keeps your business, employee and customer data protected.

Introductions - Host

Jim Soenksen – CEO, Pivot Group

- 20 years of experience in the information security and technology industries.
- As a CPA was also an internal auditor for a fortune 100 company for 7 years.
- Conveys the knowledge and conviction it takes to fight cyber crime
- Offers a realistic view of today's security issues and remedies for businesses.
- Blends business goals with technology, training, policies, and improved processes to provide the appropriate security program, technology controls, and regulatory compliance for each individual companies needs.

Introduction - Presenter

Patrick Cunningham, CRM, FAI, Senior Director, Information Governance, Motorola Solutions, Inc.

- His team's responsibilities include information security policies, information risk assessments, IT SOx audits, global records management, IT data privacy, and litigation and investigation support.
- 25 years of experience includes management, strategy, and consulting roles for government, non-profit, and publicly traded organizations.
- Holds Bachelor of Arts degree in History from Quincy University in Quincy, IL and a Master of Arts degree in Public History from Loyola University of Chicago.
- A Certified Records Manager and Fellow of ARMA International. Recently passed the AIIM International Information Certification examination.

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS® DOCUMENT MANAGEMENT

Learning Objectives

- Records Management Best Practices
- Mitigating Risks Associated with Data Breaches
- Auditing Techniques and Technologies that Overcome Common Hurdles
- RIM Data Privacy Compliance Checklist

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS
DOCUMENT MANAGEMENT

Current Data Privacy Regulations

Regulatory Compliance

- GLBA/NCUA Reg.748
- Important to viability of institution to securely safeguard member data
- Customers require that the institution comply with their applicable regulators
- Institutions have a tested Incident Response Program

Current Data Privacy Regulations (cont.)

Other Applicable Laws

- **PCI** – must protect credit card numbers, Mask PAN (*primary account number*) when displayed
  - First 6 and last 4 digits are the maximum number of digits to be displayed
- **HIPAA/HiTECH Act**
  - Security controls, how long retain data, and destruction procedures
  - Privacy of medical information
- **Fair Credit Reporting Act (FCRA) and Fair Accurate Credit Transactions Act (FACTA)**
  - Must take reasonable measures to dispose of sensitive information from credit reports and background checks
- **Red Flag Rules** – written identity theft prevention program
- **Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)**
  - Covers all industries and protects the collection, usage and disclosure of personal information

Current Data Privacy Regulations (cont.)

Data Security Breach Notification Laws

- 46 states plus the District of Columbia, Puerto Rico and the Virgin Islands

  (Except Alabama, Kentucky, New Mexico and South Dakota)

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS DOCUMENT MANAGEMENT

Federal Rules of Civil Procedures

- Electronically-stored information (ESI) is discoverable. May be used as evidence — for or against your company.
- Business record email, social media posts & other ESI must be saved, stored, & supplied *swiftly* and in a *legally compliant* fashion.
- To be accepted as legal evidence, email, social media content, and other ESI must be preserved and produced in a trustworthy, tamperproof, legally-compliant manner.
- OK to routinely purge ESI not relevant to litigation or pending cases (or otherwise required by law/regulator).
- You must anticipate likelihood of ***future*** litigation

Records Management Best Practices

- **Generally Accepted Recordkeeping Principles (GARP®)**
  - These principles of recordkeeping have been well developed by those who are fully involved in records and information management. They form the basis upon which every effective records program is built and are the yardstick by which any recordkeeping program is measured. Regardless of whether an organization or its personnel are aware of them, they form the basis upon which that organization's recordkeeping will one day be judged.
- **ISO 15489**
  - ISO standard that was developed to standardize international best practice in records management. It provides guidance on managing records of originating organizations, (public or private, for internal and external clients) to ensure that adequate records – in all formats and media – are created, captured, and managed.

See also: http://www.arma.org/standards/index.cfm

GARP® Principles

GARP® ARMA INTERNATIONAL

Generally Accepted Recordkeeping Principles®

- Accountability
- Transparency
- Integrity
- Protection
- Compliance
- Availability
- Retention
- Disposition

http://www.arma.org/garp/

Information Governance

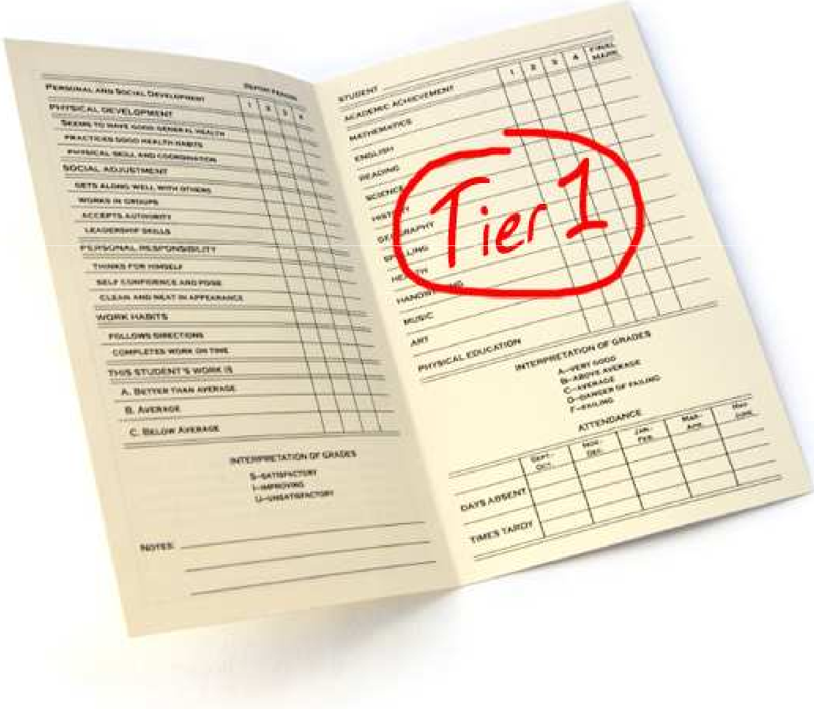
From Debra Logan (Gartner)…

Information governance is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/

Information Governance?

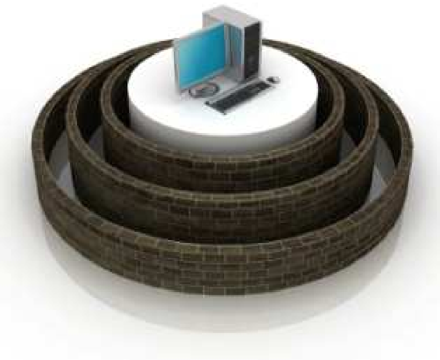
- **Governance activities which include:**
  - Policies and procedures
  - Training and communications
  - Assessments and audits
  - Risk identification and mitigation
- **Includes functions such as:**
  - Records management / retention
  - Computer forensics
  - Data security classification
  - Data mapping
  - Data privacy
  - P*I compliance



Records Management Core Elements

A Records and Information Management (RIM) program foundation is critical to successful compliance and includes:

- **RIM Policy**
- **Global Records Retention Schedule**
  - Functional – tie function & business process to retention
  - Documented legal research
- **Key RIM Guidelines and Procedures**
  - Records handling (hardcopy and electronic)
  - Disposition
  - Legal holds
- **Communication & Training – Live and Computer Based**
- **Review and Audit**
  - Annual review to stay current with changes
  - Audit business groups – ensure consistency



RIM Best Practices (Strategic)

- Audited
- Consistent
- Continuously improved
- Measurable
- Senior management support
- Global / enterprise-wide
- Mandated training

- Support legal discovery efforts
- Support data privacy efforts
- Support organizational heritage collections

RIM Best Practices (Operational)

- Efficiently locate and deliver needed records
- Associate appropriate information attributes (metadata) to all records
- Ensure that cost savings generates value for the organization
- Minimize negative impacts to end-users
- Efficiently disposition records on a regular basis
- Ensure preservation of records on legal or tax hold
- Leverage technology and workflow where appropriate and as part of a business process
- Centralize and manage information repositories
- Engage end-users in continuous program improvement
- Hold vendors accountable with meaningful penalties for non-performance

Data Mapping vs Retention Schedules

- Often very similar and integrated
- Data map may contain more specific information; many retention schedules are more functionally aligned
- Data map may include information about the application, location, data controller, data processor, and users
- Data map may include narrative about how the information is used and how it integrates with other applications and data sets
- Data map may include information about historical uses of the data
- Retention schedules document the intended retention periods, but often do not show actual implementation of the schedule

Information Attributes

- **Record Series**
  - What is it?
  - What dates are associated with it?
  - Who owns this record?
- **Security**
  - What level of protection is required?
  - Who can access the record?
- **Resiliency**
  - Is this a vital record?
  - How do we need to ensure its availability?
- **P*I Type**
  - Is this PII, PHI or PCI?
  - What regulations are we concerned about?

- Where is this record?
- Who is custodian?
- Are there relevant holds for Tax or Audit?
- What are the technical attributes of the file or database?

RIM Risks

- Loss of, or inability to find, data that matters
- Court sanctions for spoliation
- Regulatory sanctions
- Inability to defend intellectual property, enforce contracts
- Increased costs to recreate documents
- Increased costs to store, manage, and migrate data
- Increased costs of e-discovery
- Inability to collect payments and debts
- Privacy breaches

A Risk Equation

$$Risk = Threat \times \left(\frac{Vulnerabilities}{Countermeasures} \right) \times Value$$

- You only have Risk if you have a Threat and the information has Value
- Vulnerabilities increase Risk
- Countermeasures decrease Risk, but can’t be greater than the Value
- We need to think about how we manage the risk of poor records management
- We need to think beyond records management

Mitigating Risks Associated with Data Breaches

- Know your P*I (PII, PHI, PCI)*
- Develop a layered defense
- Limit access (physical and electronic)
- Search for P*I continually
- Don't use live data when testing systems
- Employ encryption liberally
- For physical records containing P*I, the best defense is often a generic storage box

Locating Critical Data

Use monitoring tools and DLP (Data Loss Prevention) systems to identify SSNs, credit card information, and other high risk information.

“How do we know we have a problem if we can’t see it?”

“If you don’t know what you have, you can’t protect it.”

Regular Monitoring and Audits

“How do we avoid problems in the future?”

- Regular Audits and Follow-up
- Policy Enforcement
- Changing Processes/Behaviors

Auditing Techniques and Technologies that Overcome Common Hurdles

- Follow standard auditing protocols
  - Statistically sound sampling
  - Preparation of evidence to support audit findings
  - Auditor independence
- RIM / IG team should be consultative, not punitive
  - Use audit findings as “teaching moments” and opportunities to get the “voice of the customer”
- Grow into auditing compliance, don’t expect 100% right away
- Leverage security monitoring / logging to discover external storage locations
- Limit and standardize repositories for data
- Have a focus on the most critical data – use the data maps to identify that first

Data Discovery Results

1. Audit

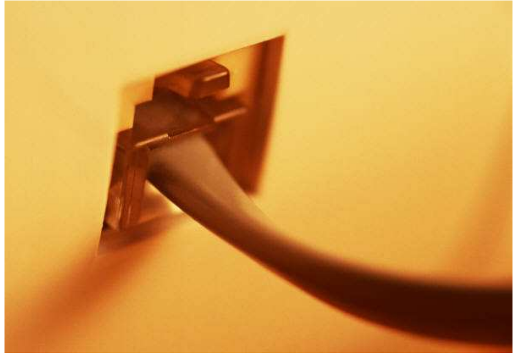
- System
- Data
- Processes

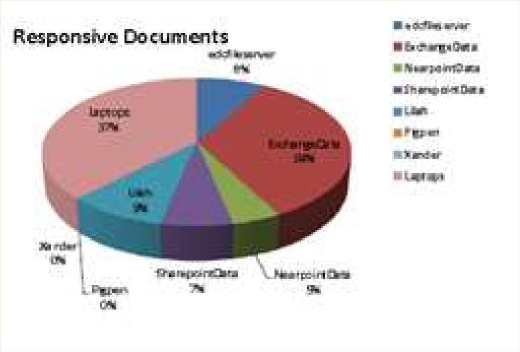
2. Analysis

- Process overview
- Data discovery
- Behavioral observations

3. Actions

- Plan for today
- Prevention for tomorrow





RIM Data Privacy Checklist

- ID Critical Data
- ID Customers Residency
- ID Applicable Laws & Regulations
- Determine Risk
- Implement a Records Management Program
- Implement Risk Controls
- Implement, Maintain, & Test ISMS and IR Program
- Perform PII Routine Audits: Risks & Controls

☑ ID Critical Data
☑ ID Customers Residency
☑ ID Applicable Laws & Regulations
☑ Determine Risk
☑ Implement a Records Management Program
☑ Implement Risk Controls
☑ Implement, Maintain, & Test ISMS and IR Program
☑ PII Routine Audits: Risks & Controls

Information Governance / RIM Mission

- Prevent Loss of Data that Matters
- Minimize Disruption to the Business

Prevent Loss of Data that Matters

- Intellectual Property
- PII, PCI, PHI
- Financial Data
- Business Plans and Product Road Maps
- Anything that becomes material in litigation
- If you don't know what you have, you can't protect it
- If you don't know what is valuable, you may be wasting money protecting the wrong things
- "Loss" can also mean "spoliation"

Minimize Disruption to the Business

- We’re not just talking about disaster recovery and business continuity…
- Nor is this focused on malware
- Consider solutions for information management problems – do they interfere with the running of the business?

Webinar Take Aways

- Consistency
- Top management support
- Integrated team of security, IT, records, law
- Communicate and train
- Identify risks and audit the program
- Identify where information is stored and used

Resource References

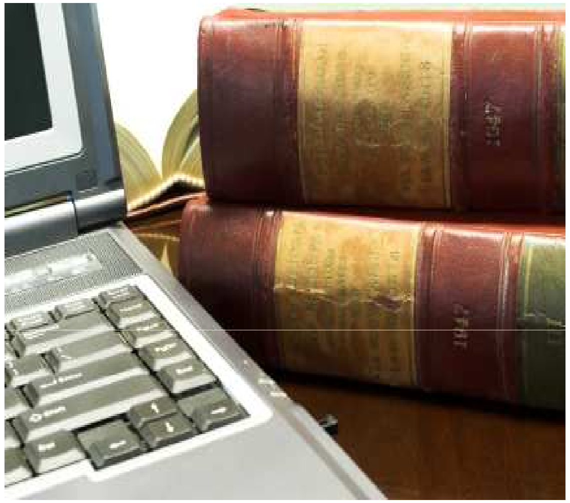
- GARP® – ARMA International
- RIM Core Competencies – ARMA International
- ISO 15489
- RIM Standards Page – ARMA International

Additional Resources

- ARMA Conference and Expo
- Webinars
- Local seminars and workshops
- Publications
- Other training

Reference Resources

- CSO Online
- National Conference of State Legislatures
- ISO 27000
- PCI Security Standards
- Ponemon & PGP *2010 Annual Study: Cost of a Data Breach*
- MER Conference/Sedona Group
- AIIM
- ARMA
- International Threat Resource Center
- Pivot Group Critical Data Check List
- Cintas Records Compliance Guide



Join Us for Our Next Webinar

Topic: Is your Mobile Device and Social Media Program Compliant?

Featured Speaker: Nancy Flynn
The ePolicy Institute

Date & Time: December 7
2:00pm-3:00pm Eastern

Learning Objectives:

- Risks and Liabilities of Mobile Devices and Social Media
- Mitigating Risks Associated with Data Breaches
- Mobile Devices and Social Media Best Practices
- ePolicy Health Check

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS® DOCUMENT MANAGEMENT

How to Register

- Webinar Follow Up E-mail
- Webinar E-vites
- www.pivotgroup.com/webinars

Q&A

For more information contact:

Pivot Group

- Jim Soenksen, CEO
- Call: (888) 722-9010
- Email: jsoenksen@pivotgroup.com
- Visit: www.pivotgroup.com

Cintas

- Call: 1-800-Cintas-1
- Visit: www.cintas.com/documentmanagement

PIVOT GROUP
Armed with Information Security Knowledge

CINTAS® DOCUMENT MANAGEMENT