



Virginia Information Technologies Agency

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

November 14, 2007



**Veterans Day!**



**Thanksgiving Day!**



**Cooler Weather**





# NOVEMBER MINI-SPYWARE QUIZ

**(1) Approximately how many computers on the Internet are infected with spyware?**

- a. 25%
- b. 45%
- c. 60%
- d. 80%

**(2) What is the single best thing you can do to protect your computer against spyware?**

- a. Disable Active-X in Internet Explorer
- b. Protect your computer with a firewall
- c. Install anti-spyware and keep it updated
- d. Only browse websites that you know and trust



# NOVEMBER MINI-SPYWARE QUIZ

## November Security Mini-Quiz Answers

**(1) D. While expert opinions vary, most sources agree that 80% is a reliable estimate.**

**(2) C. Anti-spyware is as important as antivirus software for protecting your computer.**



# ISOAG November 2007 Agenda

- |       |  |   |
|-------|--|---|
| I.    | Welcome and Opening Remarks              | Peggy Ward, VITA                          |
| II.   | Virginia Enterprise Application Program  | Will Goldschmidt, GOV                     |
| III.  | Electronic Records                       | Ariel Billmeier, LVA                      |
| IV.   | COV IS Council Identity and Access Mgmt. | Marie Greenberg, SCC<br>Mike Garber, VDOT |
| V.    | SWECS                                    | Scott Quinn, NGC                          |
| VI.   | IT Security Guidelines                   | Cathie Brown, VITA                        |
| VII.  | Web Security                             | Tripp Sims, VITA                          |
| VIII. | Upcoming Events & Other Business         | Peggy Ward, VITA                          |



VEAP

Virginia Enterprise Applications Program

*Visibility – Efficiency – Accountability – Progress*

Will Goldschmidt

Wednesday November 14, 2007

# Business Problem

- The centralized systems do not support the needs of most agencies
  - Proliferation of systems to support “the system”
  - Hindering the effectiveness of other large Commonwealth systems
- Commonwealth’s administrative systems are too stove-piped and disparate to operate efficiently
  - Manual and redundant business processes predominate
  - Lack of automated and timely reporting capability
    - Internal and external
  - Differing capacities within the agencies
- Increased risk of system failure and a diminishing pool of knowledge to support current antiquated systems
  - Ultimately will result in decreased service delivery to citizens

# Proposed Solutions

- **An integrated, enterprise-wide business capability**
  - Financial Management, Performance Budgeting, Human Resources, and Supply Chain Management and Administration
- **Data consolidation and standardization effort**
  - Improve the quality of information for management decision making
- **Competency Centers**
  - Service centers for business needs
  - Cross functional Business Intelligence
    - Rapid querying and reporting capabilities for staff and management
  - Systems development, maintenance and support
- **“One-stop shopping”**
  - 30,000 vendors transacting business with the Commonwealth using an online portal for registration, bids, awards, and payments
  - 70,000 Commonwealth employees using online portal for benefits, retirement, and leave

# Enterprise Applications Benefits

- “Gold Source of Data”
  - Provides enhanced services to citizens & businesses
    - Today, CoVA does not have the capability to be a one employer, one vendor organization
  - Improves efficiencies and capabilities across agencies
    - Access to data without depending on or tasking other agencies
- Centrally Managed
  - Allows agencies to focus on core business functions
    - Repetitive and routine administrative processes without losing the agency’s mission focus
  - Provides economies of scale for non-core functions of an agency
- Less “input” systems
  - Reduces redundant functionality and systems, better data quality

# What is the Vision ?

- Program (based on projects) to provide the Commonwealth with modern, effective and efficient business processes and systems
- Data Centric vice Application Centric
  - Near term focus on Financials business processes
    - Performance Budgeting
    - Financial Management
  - Common Reporting tools
  - Data Consolidation
- Long term, continuous upgrades of the systems

# Current State FM & Budgeting

(DOA, DPB, DGS, VEC, VDOT & VITA )

DBMS	Total
MS SQL Server	12
Oracle	10
VSAM	5
ADABAS	4
Oracle 7.x	1
Grand Total	32

Operating System	Total
MS Windows Server	13
Mainframe	9
MS Windows Desktop	6
Unix	3
AIX	1
Sun Solaris	1
Grand Total	33

Reporting	Total
EasyTrieve	3
nVision	3
Crystal	1
Mantissa	2
MS Analytical Services	1
Viador	1
Business Objects	1
Cognos	1
SQR	2
Grand Total	15

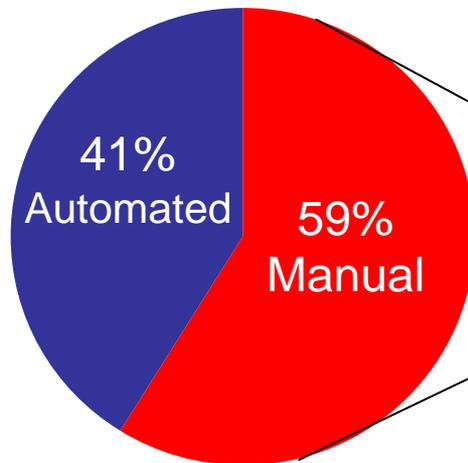
D&R Environment	Total
COBOL	7
ColdFusion	6
MS Access	6
PeopleTools	5
Natural	2
Oracle Forms	2
VisualBasic	2
.Net/C#	1
Powerbuilder	1
PeopleTools 6.1	1
Grand Total	33

Denotes "transitional / contained" technology\*

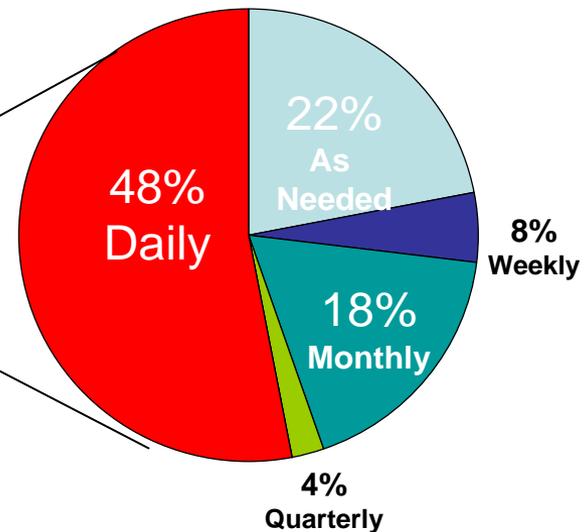
Denotes "obsolescent / rejected" technology\*

# 442 Current FM Interfaces\*

## Efficiency



## Frequency



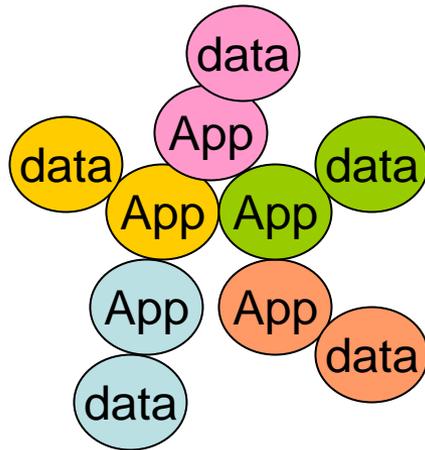
26%

### Reducing Manual Interfaces:

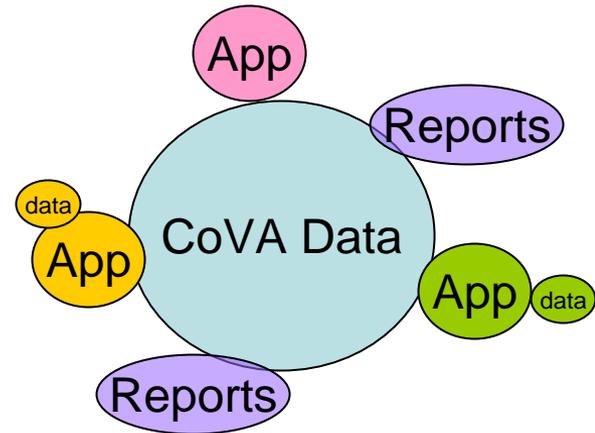
- Enhances Security
- Increases Data Accuracy
- Improves Data Timeliness
- Leverages system capabilities

\* EXCLUDES DMV, DSP, DOC, DOH, DEQ & DSS – along with Higher Ed

# Application Centric to Data Centric



Application  
Centric



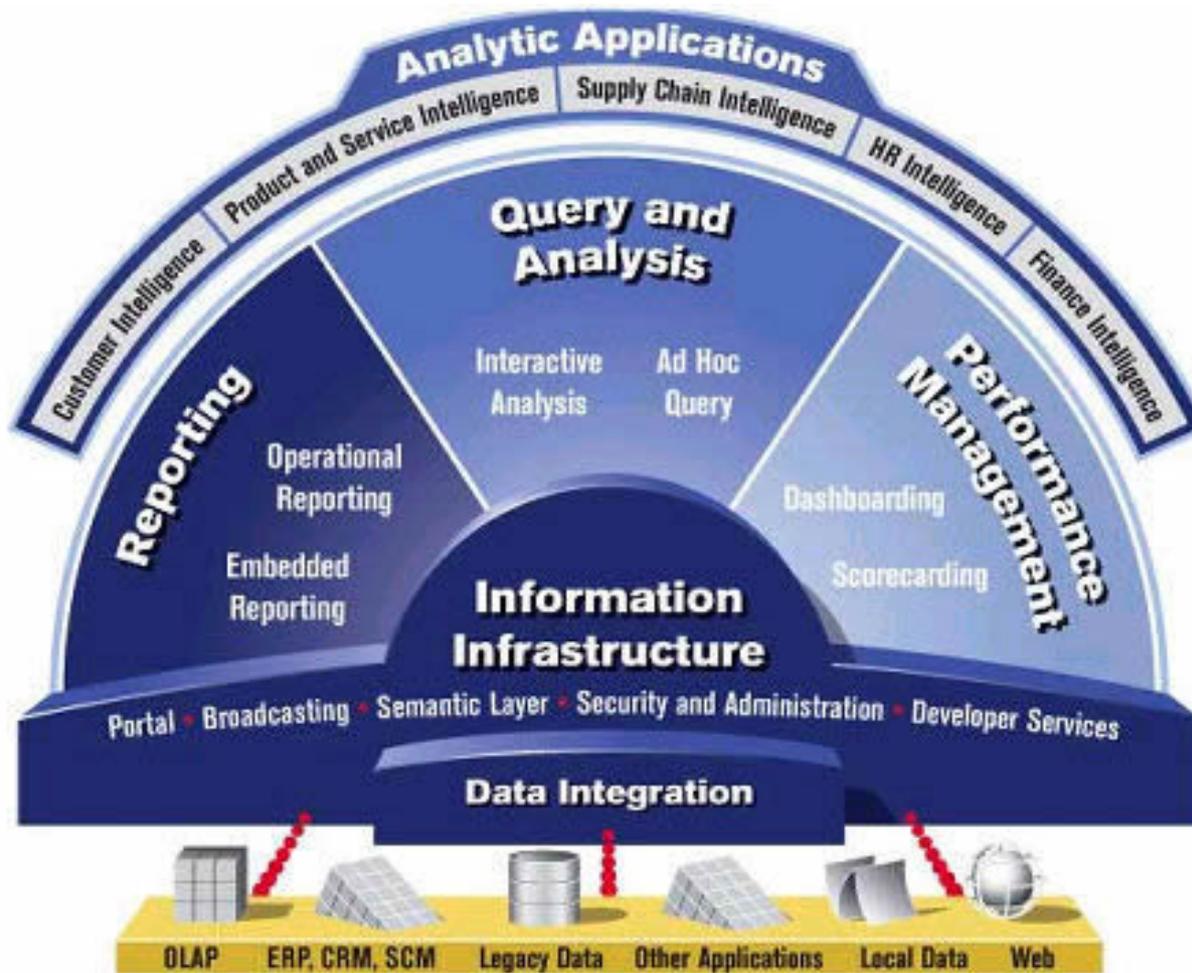
Data  
Centric



VEAP

Virginia Enterprise Applications Program

# EA Objective



# What is Happening Now?

---

## **Three Procurements**

- Financial Management
- Planning and Budget
- Business Intelligence
  - Reporting
  - Analytics

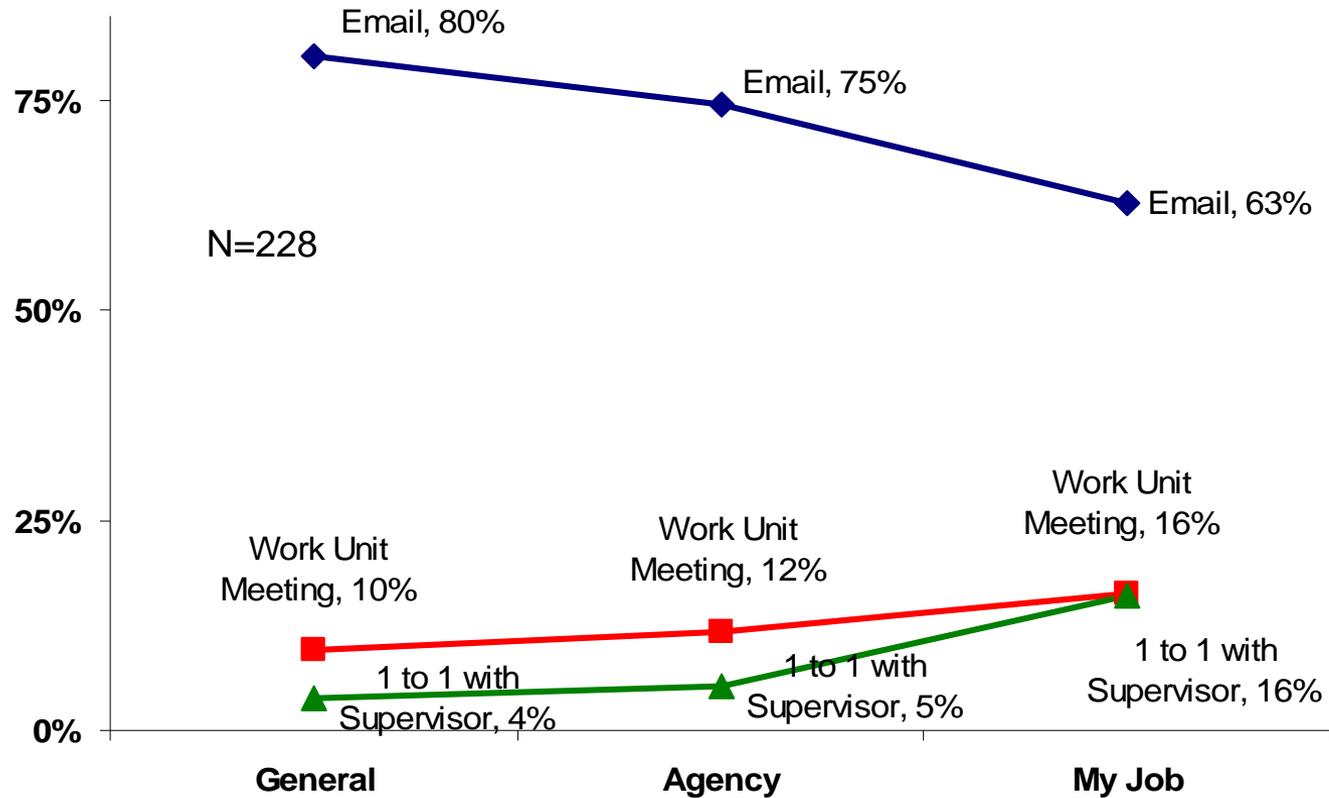


## Agency Surveys

- Functional Capabilities
- Technical data
- Readiness to Change

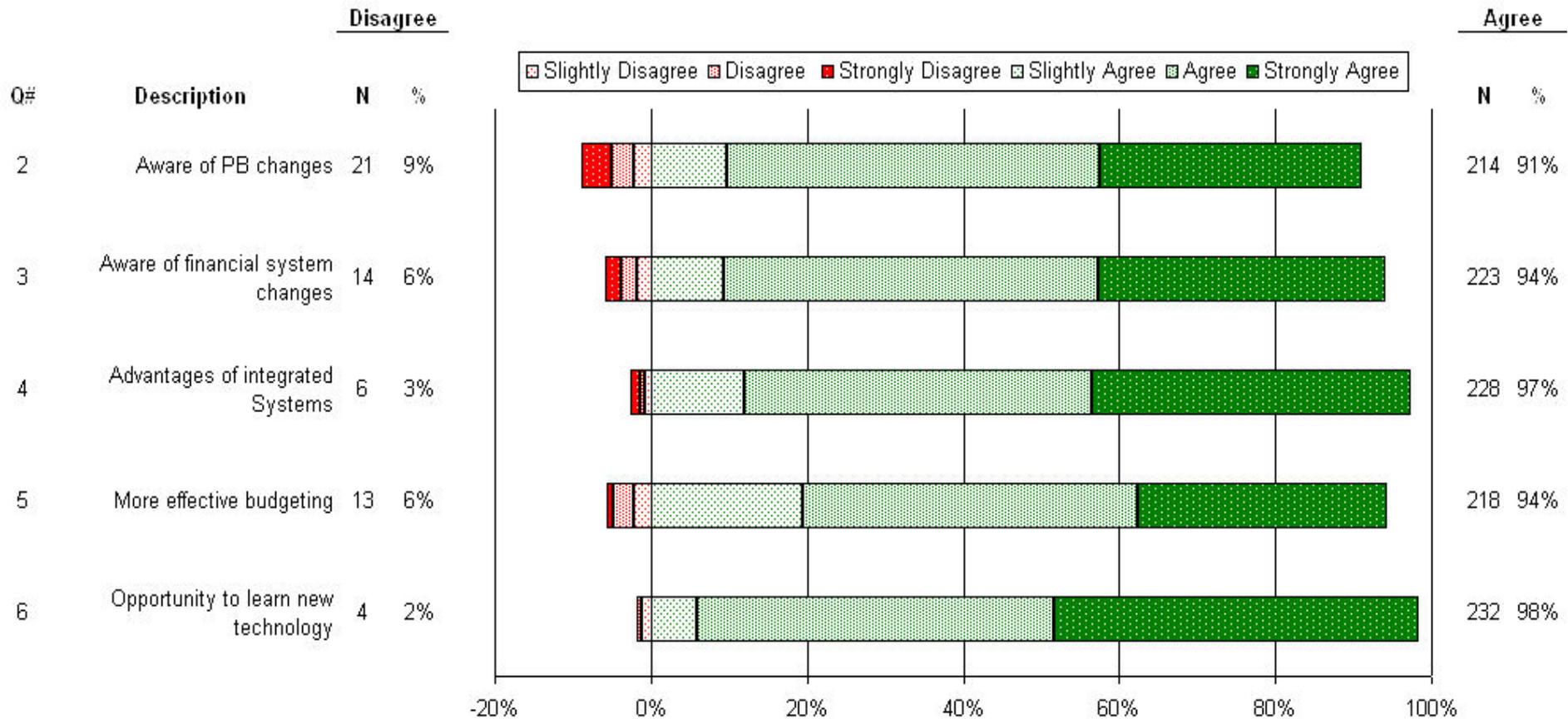
Data Management, Interfaces and Conversion

# How Should We Communicate Changes?

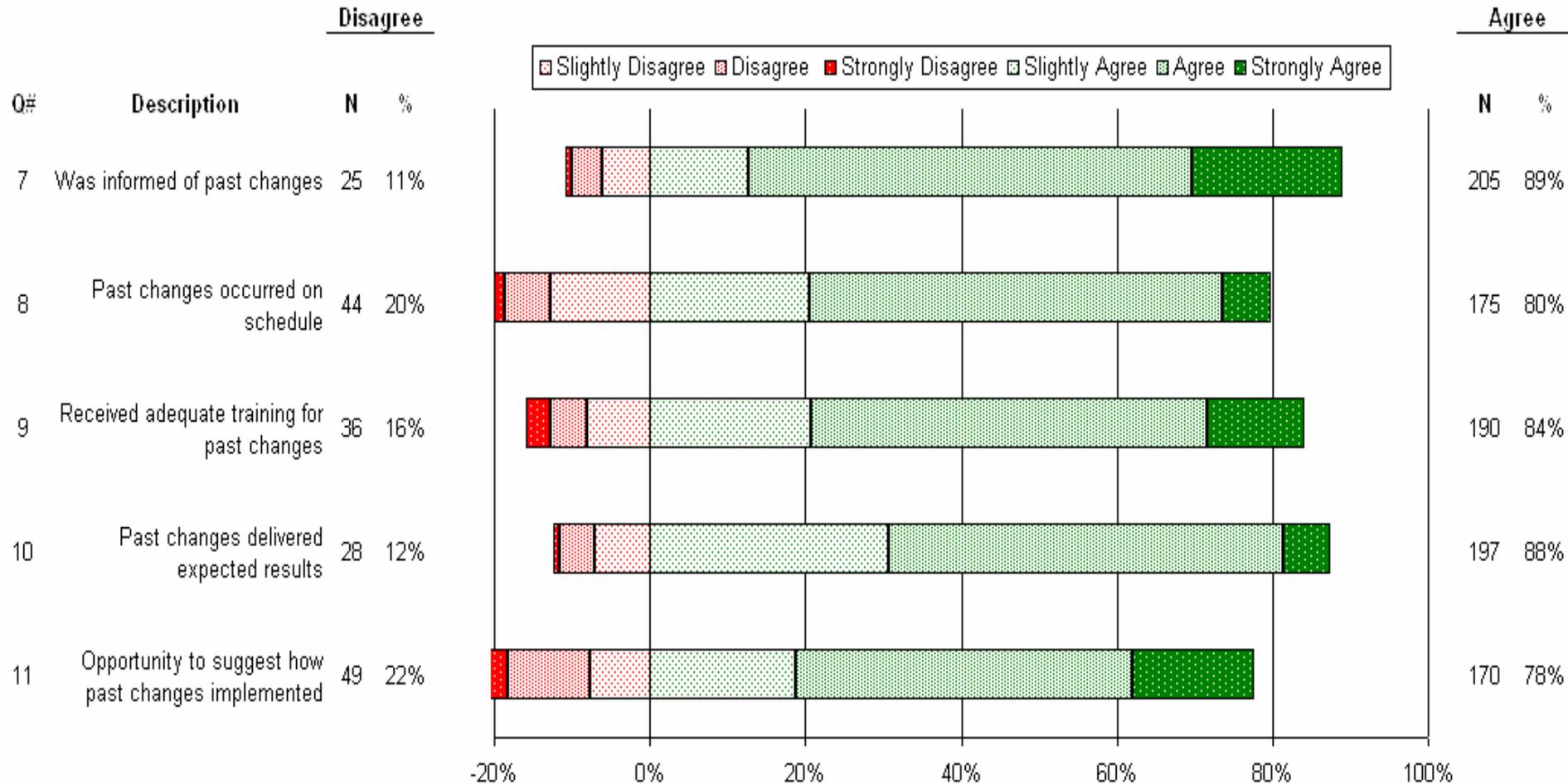


The closer it gets – the more personal touch is needed.

# General Agreement on the Future



# Some Issues With the Past





VEAP

Virginia Enterprise Applications Program

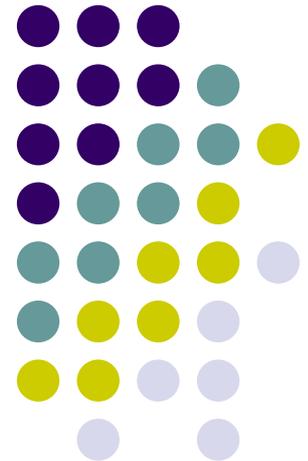
---

Questions?

# Electronic Records Management

---

Ariel Billmeier  
Electronic Records Analyst  
Library of Virginia



**Process of Public Records Management in Virginia**

VA Public Records Act  
Code of Virginia  
Title 42.1, Chapter 7

Legal Mandate

Library of Virginia  
Records Management Authority

ROC

Records  
Retention and  
Disposition  
Schedules

Two Types

General  
Schedules  
(Covers records found  
in multiple agencies)

Agency-Specific  
Schedules  
(Covers records  
specific to agency)

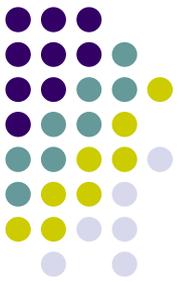
Together the general and agency-specific schedules provide for the retention and disposition of all public records

Guidelines, Best Practices, Manuals

Educational Resources

Agency Management of Commonwealth's Public Records

# Electronic Records General Schedule (GS-110)



- Currently being revised
- Will be replaced with “IT Records” schedule
- Current General Schedules for State Agencies available at:  
[www.lva.lib.va.us/whatwedo/records/sched\\_state](http://www.lva.lib.va.us/whatwedo/records/sched_state)
- Please contact me if you would like to provide comments on GS-110 revisions and I will provide you with the current draft



# What is a public record?

- Recorded information that documents a transaction or activity by or with any public officer, agency or employee of an agency
- Regardless of physical form or characteristic, the recorded information is a public record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of public business
- The medium upon which such information is recorded has no bearing on the determination of whether the recording is a public record

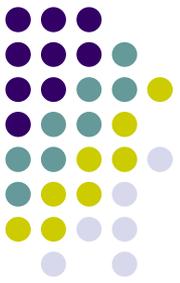
(Source: Virginia Public Records Act, *Code of Virginia*, Section 42.1-77)



# What is not a public record?

- Reference materials including reference texts, magazine and newspaper articles, textbooks, and notebooks of seminars or classes
- Personal e-mail and administrative e-mail regarding meeting times, lunch dates, staff association events, and similar subjects
- Listserv messages
- Personal materials such as errand lists, bills, checkbooks, and photos
- Stationary, blank forms or templates, and publications for distribution
- Copies of policy and procedure manuals

# Metadata

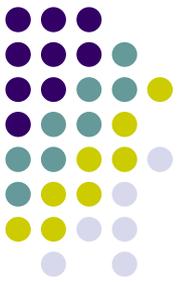


**Data describing context, content and structure of records and their management through time (e.g. contributor, creator, date, identifier, status, or title).**

## **Metadata functions:**

- Legal and statutory reasons (e.g. to satisfy records management laws and the rules of evidence)
- Technological reasons (e.g. to design and document systems)
- Operational or administrative reasons (e.g. to document decisions and establish accountability)
- Service to citizens, agency staff, and others (e.g. to locate and share information)

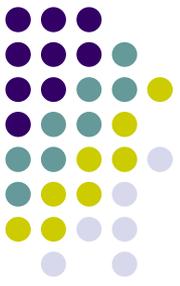
# Characteristics of Trustworthy Records



- Reliability: content can be trusted as a full and accurate representation
- Authenticity: what it purports to be; created or sent by person purported to have sent it; and created or sent at time purported
- Integrity: complete and unaltered
- Usability: can be located, retrieved, presented, and interpreted

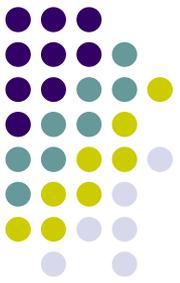
This is why “access controls” are necessary!

# Maintaining Trustworthy Records



- Content: conveys information (e.g. text, data, symbols, numerals, images, and sound)
- Structure: appearance and arrangement of the content (e.g. relationships between fields, entities, language, style, fonts, page and paragraph breaks, links and other editorial devices)
- Context: background information that enhances understanding of technical and business environments to which the records relate (e.g. metadata, application software, logical business models) and the origin (e.g. address, title, link to function or activity, agency, program or section)

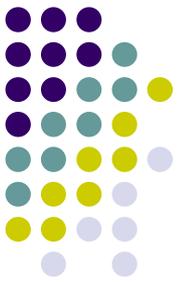
# Records Appraisal



**The administrative, fiscal, legal, and historical value of a public record shall be considered in appraising its appropriate retention schedule:**

- Administrative: continuing utility in the operation of an agency
- Fiscal: needed to document and verify financial authorizations, obligations, and transactions
- Legal: document actions taken in the protection and proving of legal or civil rights and obligations of individuals and agencies
- Historical: contain unique information, regardless of age, that provides understanding of some aspect of the government and promotes the development of an informed and enlightened citizenry

# RM & IT Semantics: Archive

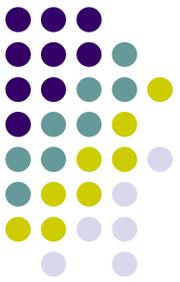


## RM

- Used primarily as repository for historical information
- Hard media perceived as being cared for and preserved for perpetuity

## IT

- Used primarily as an off-line, less expensive means of storage
- For active access or file backup



# RM & IT Semantics: File

## RM

- An organized grouping of related records
- Rules for various filing methods
- Accepted methods of organizing groups of files

## IT

- A group of records to be stored or processed as a unit
- No rules or preferred practices for organizing or labeling
- Choices left up to users



# RM & IT Semantics: Record

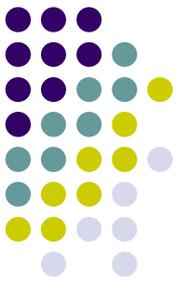
## RM

- Primarily used as evidence of a transaction, decision, instruction, action, evaluation, etc.
- Has specified administrative, legal, fiscal and historical value to the organization

## IT

- A group of data elements related to a common subject
- Value is the data it represents and the information it is meant to convey

# Recent Electronic Records Management Survey Results



- 75-80% of survey participants report a formal program for paper-based records management
- Only 55-60% report a program for managing electronic records

Source: AIM Industry Watch, Electronic Records Management: For Most It's "Still Waiting for Godot", 2006

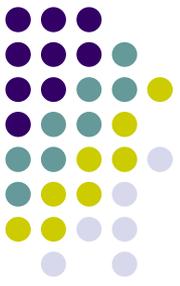
# Electronic Records Management Responsibilities



- It shall be the duty of any agency with public records to cooperate with the Librarian of Virginia in conducting surveys and to establish and maintain an active, continuing program for the economical and efficient management of the records of such agency
- The agency shall be responsible for ensuring that its public records are preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic records as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration

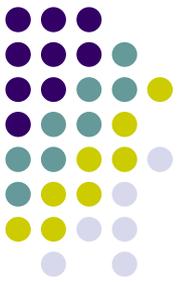
(Source: The Virginia Public Records Act, *Code of Virginia*, Section 42.1-85)

# Electronic Records Management Challenges



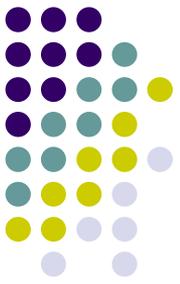
- Involves cooperative effort between records management staff, administration, legal counsel, and information technology department
- The ease of copying and modification—the great advantage of digital media—is a major liability
- Media degradation and obsolescence
- Format obsolescence
- Uncontrolled accumulation and duplication

# More Electronic Records Management Challenges



- Maintaining records in a way which will enable retrieval of all documents relevant to a transaction when they are needed
- Ensuring that the records are not retained for any longer than necessary, in order to avoid both overloading systems and to avoid indiscriminate dumping
- Maintaining content, structure and context of electronic records is both more vital and difficult than with traditional records

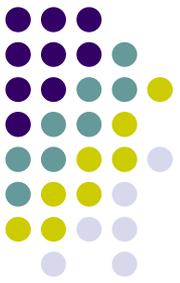
# Records Containing Identifying Information



- Non-permanent records containing identifying information shall be destroyed within six months of the expiration of the records retention period
- Identifying information includes: social security numbers; driver's license numbers; bank account numbers; credit or debit card numbers; personal identification numbers (PIN); electronic identification codes; automated or electronic signatures; or passwords.

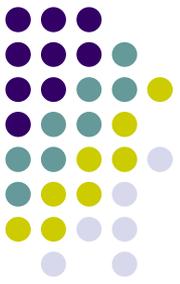
(Source: The Virginia Public Records Act, *Code of Virginia*, Section 42.1-86.1)

# Amendments to the Federal Rules of Civil Procedure



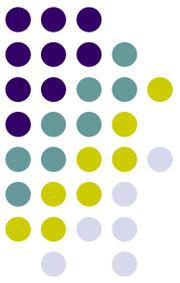
- **Identify** all sources of electronically stored information in your possession, custody, or control (Fed.R.Civ.P. 16, 26(b), 34).
- **Preserve** that information from loss or destruction (Fed.R.Civ.P. 16, 37).
- **Plan for discovery** of that information as soon as litigation begins - and agree with your opponent on a discovery plan to be adopted by the court (Fed.R.Civ.P. 16, 26(f)).
- **Disclose** crucial electronically stored information without waiting for a discovery request from your opponent (Fed.R.Civ.P. 26(a)).
- **Produce** relevant electronically stored information upon request (Fed.R.Civ.P. 26, 33, 34, 45).
- **Protect** privileged and other appropriate information (Fed.R.Civ.P. 26(b)).

# Storage Media Rules

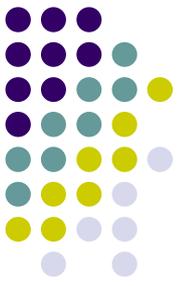


- Storage systems should be large enough to accommodate future growth
- Should also provide an appropriate level of certainty for the recovery and security of data
- Where data longevity or records integrity is a primary concern, non-rewritable media should be used
- Due to the limited life expectancy of digital media, no digital storage medium is adequate for the long-term or archival preservation of records – assume the need to migrate files to new storage media on a regular basis

# E-mail as a Public Record



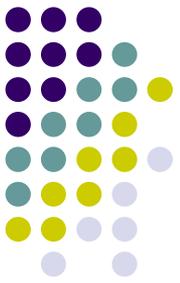
- More and more business is conducted by e-mail, replacing memos and letters
- State agency employees are responsible for managing e-mails, including messages sent and received



# E-mail Retention

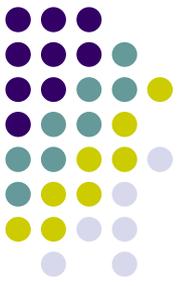
- Content and context of messages determine appropriate records series – usually covered under the general schedules published by LVA
- Retention for “correspondence” ranges from “as long as administratively useful” for routine correspondence to “permanent” for agency head and historically significant correspondence

# E-mail Management



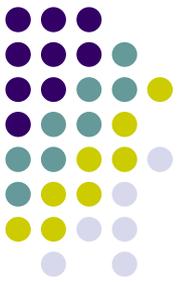
- Organizing e-mail in folders according to records series or subject area and fiscal or calendar year allows for monitoring of retention periods and disposal of e-mails at the appropriate time without manually sifting through messages
- It is helpful to establish agency- or division-wide filing structures

# “Archiving” E-mail



## Four methods of archiving e-mail outside of the system:

- Print e-mails and maintain them in a manual system
- Create personal folders (or .pst files) and store on a secure shared network server, not a local hard drive
- Establish an electronic filing process
- Store, access, and manage e-mail messages and other electronic records in an e-mail management program or Enterprise Content Management System (ECM)



# Issues with .PSTs

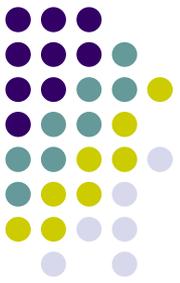
- Backup issues (especially if they're saved to a local drive versus a shared drive)
- Messages take up more space in a PST than in an Exchange store
- Cannot use OWA to read messages in a PST
- Security issues
- Lose single instance store (SIS)
- FOIA and e-Discovery – global searches no longer possible
- Application of retention schedules

# Archiving versus Auto-Archiving

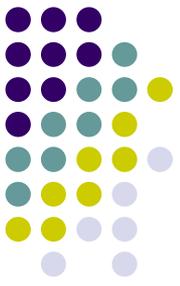


- “Archiving” involves a manual transfer by the user
- “AutoArchiving” is an automatic process (if turned on within Outlook) that takes place at regular intervals
- Rather than using the “AutoArchiving” function, users should set aside time (every week or month, for example) to clean up mailboxes and manually archive appropriate folders

# Is e-mail subject to FOIA?



- E-mail records are subject to the same accessibility requirements as other public records – they are exempt from access only if they fall within the exemptions provided under FOIA
- Requests from the public for e-mail records must be honored in the same manner as other public records
- E-mail records must remain accessible during their entire retention period and should be maintained in such a manner as to permit easy access and timely retrieval



# Instant Messaging

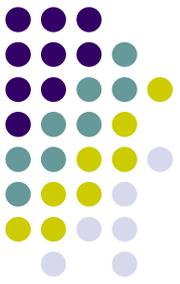
- Same “rules” apply if messages document a transaction or activity by or with any public officer, agency or employee of an agency
- Difficult to separate record traffic from non-record traffic
- Need for agency IM policies
- Gateways and enterprise IM (EIM) allow for more effective management of IM



# Voicemail

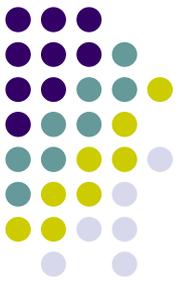
- Covered in GS-101 and GS-110
- Routine: Retain as long as administratively necessary then destroy.
- Relevant to Specific Actions: Transfer information in electronic or paper format to the relevant records series listed on this or other retention schedule.

# Audio and Visual Recordings

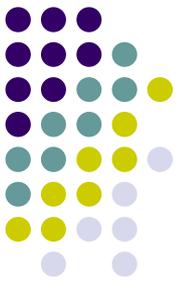


- Covered in GS-101
- Historically Significant: Retain permanently.
- Other Recordings: Retain as long as administratively necessary then destroy.

# Recordings of Electronically Held Meetings



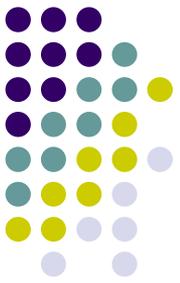
- Covered in GS-101
- Boards, Commissions, Conferences, and Committees Having Regulatory or Decision Powers: Retain 3 years or until minutes are transcribed and approved, whichever is greater, then destroy.
- Boards, Commissions, Conferences, and Committees Without Regulatory or Decision Powers: Retain 3 years, then destroy.



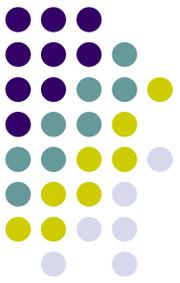
# “Desktop” Management

- Develop an organized file plan or directory structure organized by record series – that parallels e-mail directory structure
- Dated folders may be helpful in applying appropriate retention periods
- Don’t forget the metadata!
- Make sure your records are protected – stored on network server that is backed up
- Do not use CDs, DVDs, or other external media for long-term storage

# Web Content Management



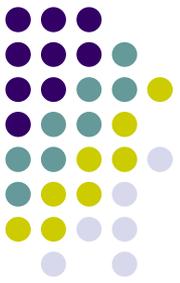
- Agency websites are public records and need to be managed as such
- They may contain information that is not duplicated elsewhere
- Archiving options:
  - ❖ PDF
  - ❖ Web harvester
  - ❖ Web files can be retained on server or external media
- Currently, LVA is archiving agency websites once per year (but this does not fulfill records retention requirements)



# Database Management

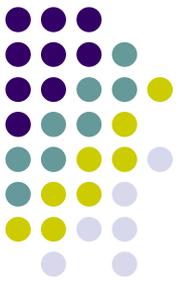
- Represent a “born digital” record type
- No functional paper equivalent
- Frequently require a specific schedule to ensure proper management of information

# Necessary Records Management Functions of a Database



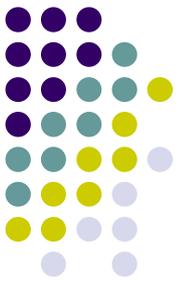
- Ability to take files offline and store them (inactive table)
- Retrieval of inactive files for the full duration of the retention period
- Identification of records eligible for deletion or preservation
- Documentation of what has been deleted or transferred

# Digital Imaging in the Code of Virginia



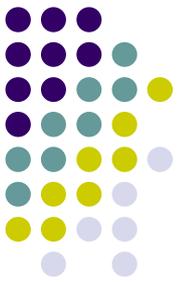
- According to the Virginia Public Records Act, any public official who converts or migrates an electronic record shall ensure that it is an accurate copy of the original record – the converted or migrated record shall have the force of the original
- The Copies as Evidence Section 8.01-391 of the *Code of Virginia* allows agencies and localities to produce a digital image of a record in response to a court subpoena or FOIA request

# Digital Imaging Responsibilities

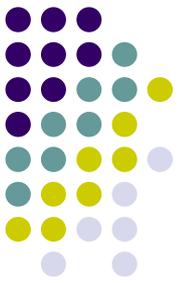


- Agencies are responsible for maintaining access to reformatted records for entire retention period
- For most non-permanent records, agency can destroy originals without using Certificate of Records Destruction (Form RM-3)
- Permanent records may be reformatted, however consultation with LVA records analysts is suggested

# Required Components of the Reformatting Process

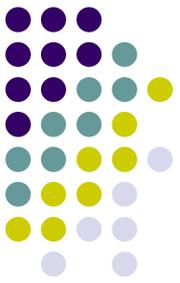


- Quality control process to certify that imaged records are visually inspected for legibility and integrity
- Indexing system
- System must be able to reproduce technical drawings and blueprints to scale
- If records are considered vital, security copy of records, application, and indexing system must be stored off-site
- Form RM-3 required when records are deleted



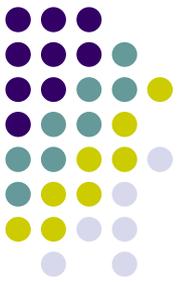
# What is EDM?

- Electronic Document Management (EDM)
- Controls the capture, indexing, processing, storing, transferring and use of electronic documents to facilitate workflow
- Manages documents as individual units, as opposed to preserving its relationship to a larger group of documents that provide evidence of the same particular organizational function



# What is ERM?

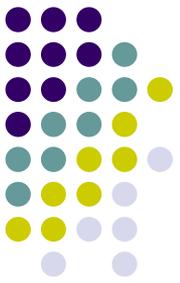
- Electronic Records Management (ERM)
- Enables the capture and management of electronic documents as records
- Typical ERM functions include declaration, capture, organization, security, retrieval, preservation, audit/oversight and disposition



# What is ECM?

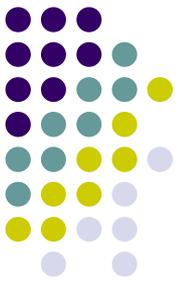
- Enterprise Content Management (ECM)
- Technologies used to capture, manage, store, preserve, and deliver content and documents related to organizational processes
- EDM and ERM are components of ECM

# ECM in the Commonwealth



- Governor Kaine’s “Paperless Government” initiative
- ECM software RFP released on February 2. Included document management, records management, workflow, document imaging, enterprise report management and eForms
- Awarded to IBM FileNet
- Implementation contracts currently being negotiated

# IT & RM: Benefits of Collaboration



- Better storage and retrieval of information
- Greater efficiency in terms of time and money
- More consistent and accurate records
- Improved records retrieval and management
- Destruction in compliance with the law
- More flexibility, tighter security



# Shared Responsibilities

**In an ideal situation, IT and RM staff work together to develop:**

- Directory structure / file plan / ECM
- Data management / rights management
- Backup policies
- Deletion responsibilities
- Disaster recovery plan



Questions or Comments?

Ariel Billmeier

Electronic Records Analyst

[ariel.billmeier@lva.virginia.gov](mailto:ariel.billmeier@lva.virginia.gov)

804-692-3607



# IAM

---

Identity and Access Management  
And  
Account Management

# IAM Committee Members

---

- Marie Greenberg – SCC, [marie.greenberg@scc.virginia.gov](mailto:marie.greenberg@scc.virginia.gov)
- Mike Garner – TAX, [mike.garner@tax.virginia.gov](mailto:mike.garner@tax.virginia.gov)
- John Willinger – DMHMRSAS, [John.Willinger@co.dmhmrzas.virginia.gov](mailto:John.Willinger@co.dmhmrzas.virginia.gov)
- Joel McPherson, DSS, [joel.mcpherson@dss.virginia.gov](mailto:joel.mcpherson@dss.virginia.gov)
- David Hines, SCV, [dhines@courts.states.va.us](mailto:dhines@courts.states.va.us)
- Maria Batista, DMV, [maria.batista@dmv.virginia.gov](mailto:maria.batista@dmv.virginia.gov)
- Easton Rhodd, VITA, [easton.rhodd@vita.virginia.gov](mailto:easton.rhodd@vita.virginia.gov)
- Jim Austin, VDOT, [james.austin@vdot.virginia.gov](mailto:james.austin@vdot.virginia.gov)
- Chris Nicholl, VEC, [christopher.nicholl@vec.virginia.gov](mailto:christopher.nicholl@vec.virginia.gov)



# What is Identity & Access Management

---

- Identity management is the capability to manage all user accounts and profiles that can be identified with each person across the IT environment via user roles and business rules.
- Access management is the ability to manage access control policies across multiple platforms.
- Access management (authentication, authorization and auditing) referred to as the gold standard because of the symbol “**AU**” from the first two letters of all three processes.



# The five main drivers for an IAM solution:

---

- Regulatory compliance
- Operational effectiveness
- Business facilitation
- Cost reduction
- Security risk management

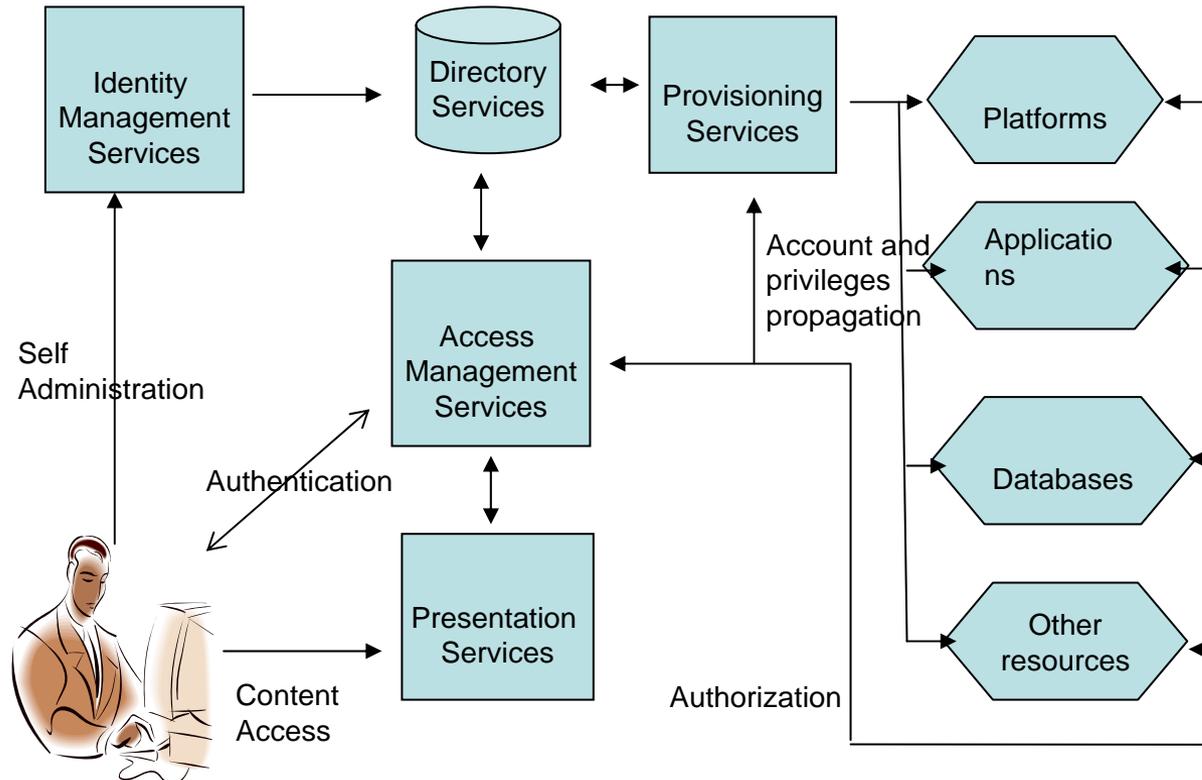


# A successful IAM Solution

---

- IAM is a set of processes used to control the access of people and applications or services to IT resources. It requires business process changes and senior management support to be effective.
- A successful IAM solution will require multiple products from multiple vendors. No product does everything.

# An overview of Identity and Access Management is as follows:





# Goal of the IAM Committee

---

**Establish a secure and effective methodology focused on identification and authentication across the Commonwealth.**

# Scope of the IAM Project

---

- Applicable to all systems and networks owned and operated by or on behalf of state entities (SE) and other COV government agencies (city, county) that choose to comply.
- Includes all local, state and federal government agencies and third party entities who support the mission of the Commonwealth.
- All information.



# Deliverables

---

- Create a trust model for the Commonwealth.
- Survey the COV agencies to determine their needs for identity and access and account management and verify the drivers for an IAM solution to include:

# Deliverables (cont)

---

- Regulatory compliances
- Current IAM solutions in place
- Planned projects that will utilize or require identity, access and account management.



## Deliverables (cont)

---

- Perform Gap Analysis.
- Develop proposal based on best practices
- Provide recommendations to CISO



## Progress to date:

---

- Created a Trust Model for the Commonwealth based on the New York State Trust Model as a guideline to establish standards and processes for identity management.



## Progress to date (cont)

---

Vendor demonstrations on Identity and Access and Account management from:

- CA
- Oracle
- Microsoft
- Imprivata

# Solution that provides for:

---

- Account Management/User Life-cycle Provisioning
- Provisioning & Deprovisioning - employee, Supplier, Contractor, Citizen, etc
- Single Identity - Intra- & Inter- Agency
- Cost-effective scalability & compatibility
- Reduced Complexity, Risk/Compliance & Scalability of 100 + Agencies
- Credentialing the user community (i.e. multiple: processes, passwords, etc.)
- Agility for changing Business Processes/Environment
- Web-based access - Securing Web Applications and enabling Collaboration/Federation
- Virginia Citizen Provisioning (in the future)



# Current situation

---

- Created a survey to be completed by all agencies to identify needs and requirements for an identity and access management solution.



# IAM Survey

---

- Survey questions have been designed to solicit information from COV agencies regarding:
  - regulatory requirements for access management
  - current state of Agency IAM practices
  - discovery of any existing IAM projects or plans at the Agency level



# Sampling of Survey Questions

---

- Once requested, how long does it take (on average) to establish the required system and application access for new users?
- When user accounts are no longer needed, how long does it usually take to disable or remove access?
- What regulatory requirements drive your agency's Identity and Access Management needs?
- Does your Agency have the means to audit and report on account activity and accesses?

# IAM Survey (cont)

---

- Questions to be included in overall online survey being developed by Commonwealth Information Security Council
- Survey results will be compiled and a summary of existing products/processes across the Commonwealth produced
- Agency-specific follow up questions will be asked, if necessary
- Responses/results fed into IAM gap analysis



## Next Steps

---

- Review the ITRM SEC 500 Policy and SEC 501 Standard to ensure support of IAM Trust Model.
- Review agency responses to IAM survey.
- Review available solutions from the Partnership offering.



## Next Steps (cont)

---

- Perform Gap Analysis between agencies needs and partnership offerings.
- Develop proposal based on best practices
- Provide recommendations to CISO



# Thank You

---

- Marie Greenberg – SCC
- Mike Garner – TAX
- John Willinger – DMHMRSAS
- Maria Batista, DMV
- Joel McPherson, DSS
- David Hines, SCV
- Easton Rhodd, VITA
- Jim Austin, VDOT
- Chris Nicholl, VEC



# Southwest Enterprise Solutions Center Security Overview

Scott Quinn

November 14, 2007



***NORTHROP GRUMMAN***



## Located in the southwestern portion of VA in the Heart of Appalachia region

- Russell County
- Population: 29,000
- Size: 475 square miles
- Town of Lebanon
- Population: 3,201
- Size: 4.10 square miles



**SLIDES OMMITTED INTENTIONALLY**

**SLIDES OMMITTED INTENTIONALLY**



# IT Security Guidelines & Standard

Cathie Brown, CISM, CISSP  
Deputy Chief Information Security Officer

---

11/13/2007



## Status

- IT Security Audit Guideline
  - ORCA – 10/30/07
- IT Personnel Security Guideline
  - Reviewing with DHRM
  - Look for on ORCA by end of November
- IT Systems Security Guideline
  - Including information on Systems Security Plans
  - Look for on ORCA by end of December
- Removal of COV Data from Surplus Computer Hard Drives and Electronic Media Standard
  - Look for on ORCA by end of November
- Planned in 2008
  - IT Facilities Security Guideline
  - IT Asset Management Guideline



# IT Security Audit Guideline

- Introduction
- Planning
- Performance
- Documentation
- Templates and Examples
  - IT Security Audit Plan
  - IT Security Audit Engagement Letter
  - IT Security Audit Checklist of Access Requirements
  - IT Security Audit Corrective Action Plan
  - General Audit Program



# IT Security Audit Guideline

- Introduction
  - Guideline suggests actions to make efforts of auditors and agencies more productive, efficient and effective
- Planning
  - Place reliance on any existing audits
  - For multiple systems that share similar characteristics (logical access control method, database or infrastructure) the agency may wish to audit that common area once as a system



# IT Security Audit Guideline

- Performance
  - Specific scope
    - Compliance with IT Security Policy & Standard
    - Regulations IRS 1075, HIPAA, etc.
  - Mutually agreeable schedule
  - Checklist of information and access required
  - Audit process phases
    - Familiarization
    - Preliminary Survey
    - Fieldwork
    - Reporting



# IT Security Audit Guideline

- Documentation
  - Work Papers
  - Reports
  - Corrective Action Plans
  - CAP Periodic Reporting
    - Once each quarter, submit a report to the CISO of any newly completed audits as well as updates on any outstanding corrective actions



## IT Security Audit Guideline

HELP! My agency doesn't have an IT Security Auditor

Coming Soon! Working with VITA Contractors & setting up statement of work

- Supplier Managed Staff Augmentation (SMSA)
  - Based on Hourly rate
- VITA Advanced IT Resources
  - Scope is project-based, set fee



## Revised: Removal of COV Data Standard

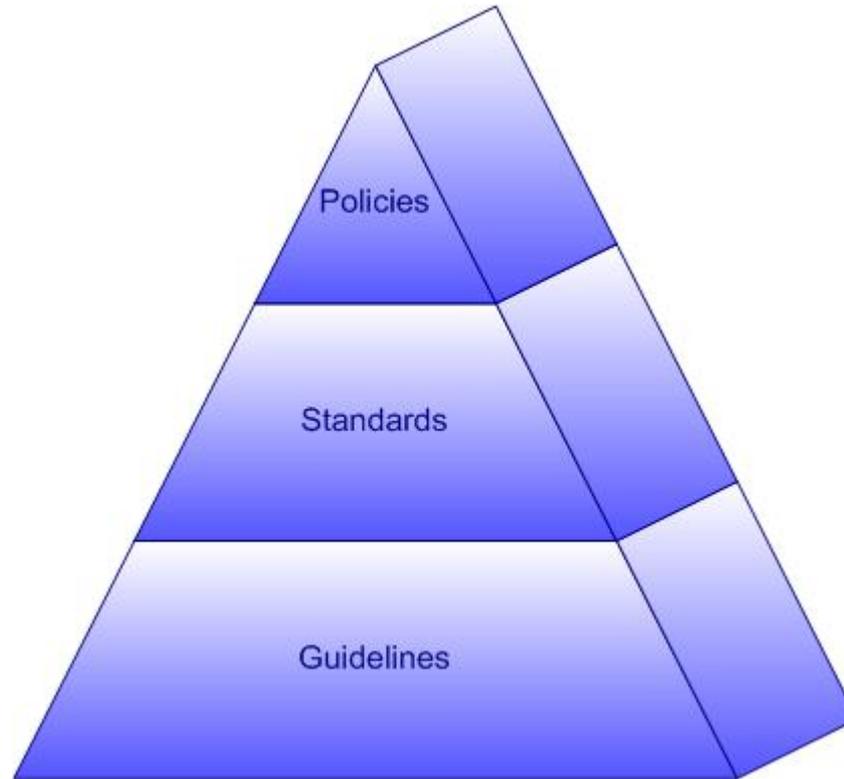
- Section G. Maintenance and Warranty
  - a) If the hard drive malfunctions and data can be removed in accordance with the requirements, the drive may be returned to the supplier for replacement under warranty or maintenance
  - b) Hard drives that are inoperable and do not allow data to be removed in accordance with the requirements, shall be physically destroyed...



## Recap on Guidelines

- Guidelines Currently Published for:
  - IT Contingency Planning
  - Logical Access Control
  - Data Protection
  - Threat Management
  - Risk Management
- Guidelines in Process for:
  - IT Security Audit
  - IT Personnel Security
  - IT Systems Security
- Guidelines Planned for:
  - Facilities Security
  - IT Asset Management

# Questions and/or Comments?



Thank you!



# Security Tips for Webmasters

**Tripp Sims**

Commonwealth of Virginia Security Architect

---

ISOAG

November, 2007

Comments: [vitasecurityservices@vita.virginia.gov](mailto:vitasecurityservices@vita.virginia.gov)



**California State Internet services shut down over website intrusion.**

**Bank of India Distributes Malware due to website hack.**

**Chinese Internet Security Response Team website distributing malware.**

**US State Dept. Russian Consulate website distributes malware due to hack.**

**Hacker Defaces Nuclear Website with Exploding Bomb Photos**

**New Dept. of State Website Accidentally Hosts Loan Documents with SSNs**

**Indiana State Website Hacked, exposing 5,600 credit cards and 71,000 SSNs**

**A Sample of 2007 Website Hack Headlines**



# Cyber Security Awareness Web Tools



## Cyber Security Awareness Toolkit 2007

<http://www.vita.virginia.gov/security/default.aspx?id=5146>

Banner

Bookmarks

Brochures

Calendar

Posters

Citizen Guide to Online Protection



# Content

- Webmasters
- Web Server Management
- Application Security
- Resources
- Q&A



# Webmasters

Ask five different technical people what a webmaster does and chances are good that you could get five different but equally correct answers.

Webmasters can be programmers, system administrators, content managers, and generalists that do it all. One thing is clear, as the web and Internet have evolved, so too have the responsibilities of maintaining a successful website.

In today's enterprise environments the responsibilities of the "webmaster" can be split amongst numerous employees each with their own area of responsibility.



# Web Server Management

- Subscribe to your server vendors security list.
- Use sftp, scp, or some other form of encrypted file transfer to manage your site vs. ftp and other unencrypted services.
- Carefully consider your server configuration.
  - WebDAV and directory indexing are generally not needed, turn them off.
  - Lower your server's profile by reducing the amount of server information it gives your visitors.
- Segregate your private and public data/applications. Preferably isolate them to separate hardware and network segments.



# Application Security

- Evaluate the history of vulnerabilities on any third party applications you consider utilizing.
- It is generally better to whitelist possible user input vs. blacklisting perceived bad input.
- Take the time to learn about today's most common web application threats. Cross site scripting, SQL injection, and remote & local file includes are all highly utilized attack methods today.
- Use a penetration testing tool on your applications whenever possible.



# Resources

- OWASP Top 10  
[http://www.owasp.org/index.php/Top\\_10\\_2007](http://www.owasp.org/index.php/Top_10_2007)
- IIS Security Tips  
<http://technet2.microsoft.com/windowsserver/en/library/354f4539-982a-418c-bfe7-4d5155b83f4a1033.mspx?mfr=true>
- Apache Security Tips  
[http://httpd.apache.org/docs/2.0/misc/security\\_tips.html](http://httpd.apache.org/docs/2.0/misc/security_tips.html)
- cgisecurity.net  
<http://www.cgisecurity.com/>
- Acunetix  
<http://www.acunetix.com/>
- SPI Dynamics - WebInspect  
<http://www.spidynamics.com/products/webinspect/index.html>
- WebScarab  
[http://www.owasp.org/index.php/Category:OWASP\\_WebScarab\\_Project](http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)



## Q & A

# Questions?



## UPCOMING EVENTS!

**Monday November 19, 12:00 - 2:00 p.m.** ISO Council Meeting with committee meetings from 2:00 – 3:00

**Monday, November 20, 1:00 – 3:00** ISO Orientation CESC

**Thursday, November 22,** Thanksgiving Day!!

**Wednesday December 12, 1:00 - 4:00** ISOAG meeting



## SANS Partnership Series Q4 2007 and 2008

Multi State - special offerings Current eligible critical constituencies include:

- 1) State & Local Government
- 2) State & Local Law Enforcement
- 3) Educational Institutions
- 4) Developing Nations/International Partners to the US

### **A. SANS @Home Program for MS-ISAC**

Class: SEC401 SANS Security Essentials

Early Bird Price: \$995 for individual seats (discount code "msisac").

Price increases to \$1,045 for orders after 10/24 (use same discount code "msisac").

Price increases to \$1,195 for orders after 10/31 (use same discount code "msisac").

MS-ISAC Discount Code: msisac

Class dates: Every Wednesday from 7-10pm EDT starting November 28, 2007 Seats

Available at MS-ISAC rate: 40

Website: <http://www.sans.org/athome/details.php?nid=7266>

### **B. SANS OnDemand Program for MS-ISAC**

Class: MGT512 SANS Security Leadership Essentials For Managers MS-ISAC Price: \$895

MS-ISAC Discount Code: msisac Discount Expiration: December 31, 2007\*

Website: <https://www.sans.org/registration/register.php?conferenceid=1032>



## SANS Partnership Series Q4 2007 and 2008

### **C. Class: SEC503 Intrusion Detection In-Depth MS-ISAC**

Price: \$895 MS-ISAC Discount Code: msisac Discount Expiration: December 31, 2007\*

Website: <https://www.sans.org/registration/register.php?conferenceid=1032>

- The Discount Expiration date refers to the last date an eligible critical constituent (MS-ISAC student) may receive the discounted price. It does not refer to the length or start date of training. Once a student pays for their OnDemand training, SANS will upload the appropriate training into their SANS Portal account and that person will then have four months to complete the training (i.e. student has four months from the date of payment to access OnDemand).

### **D. 2008 Q1 @Home Class Offer: SEC504 Hacker Techniques:**

Special MS-ISAC pricing for SANS SEC504 @Home class starting Feb. 5 from 7-10pm EDT (as well as a possible day-time class starting January – more details to follow):  
Feb. 5 Registration & Details: (<http://www.sans.org/athome/details.php?nid=8866>).  
Early Bird Price: \$995 for individual seats (discount code "msisac").  
Price increases to \$1,045 for orders after 1/2/08 (use same discount code "msisac").  
Price increases to \$1,195 for orders after 1/9/08 (use same discount code "msisac").



# NEW REGISTRATION FOR ISOAG!!

- Go to: <http://www.vita.virginia.gov/registration/ISOAG/>

**ISOAG Meeting Registration**

**(\*) Denotes required fields**

**Registrant Information**

**Date: November 14, 2007**  
**Time: 1:00 pm - 4:00 pm**  
**Where: CESC**

\* First Name:

\* Last Name:

\* Agency/Organization:

\* Email Address:

**Will you be attending via teleconference?**

Yes  No

**Register**

- This information on this registration process will be included in the email announcement for the December ISOAG meeting.



# IT Security Roles & Responsibilities

Please do not forget to list the security roles and responsibilities in each employee's job description and performance plan



# Any Other Business ?

---





**ADJOURN**

**THANK YOU FOR ATTENDING  
HAVE A WONDERFUL DAY!**

