



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

May 1, 2013



ISOAG May 2013 Agenda

- | | | |
|------|----------------------------------|---|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Homegrown IDM | Todd Dergenski, ODU |
| III. | Virginia e Identity: CAS | Michael Farnsworth, DMV |
| IV. | IS Council: ISO Manual Comm. | Bob Auton, DJJ |
| V. | ISO Certification | Ed Miller, VITA |
| VI. | Upcoming Events & Other Business | Michael Watson, VITA |
| VII. | Partnership Update | Bob Baskette, VITA
Michael Clark, NG |



Homegrown IDM

The Pains and Rewards of DIY IDM

Todd Dergenski
Old Dominion University



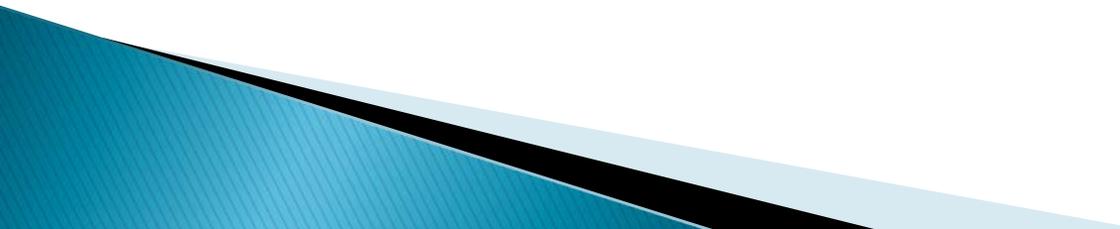
Background – ODU

- ▶ ~24k FTE
 - 35k Unique Daily SSO Logins
 - 50k Unique Yearly IDM Logins
- ▶ Computing Services
 - 200+ Employee's, Student Workers, Contracted Support
- ▶ Middleware
 - Natalie Metzger
 - Gabor Eszes

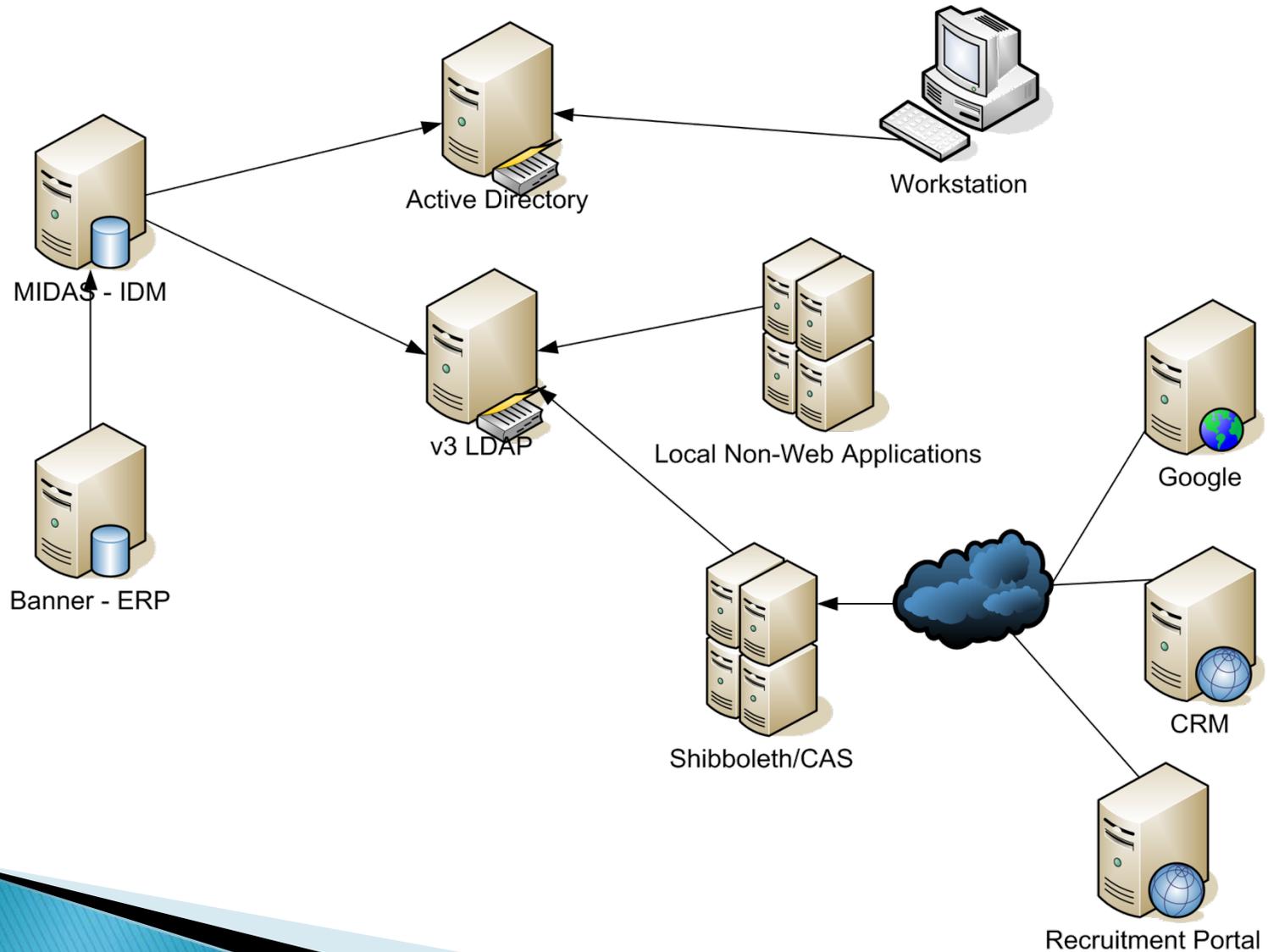
ODU Major Systems under IDM

- ▶ MIDAS Originally Scoped as a Password Reset and Student Services Provisioner 2003
 - ▶ Novell/Lotus 2003 -> 2008
 - ▶ LDAP/Shibboleth 2007 -> Present
 - ▶ AD/Exchange 2008-> Present
 - ▶ Banner 2013
- 

MIDAS Feature Release

- ▶ AUP/Role – Summer 2005 v.1.0
 - ▶ Sponsored/Guest Accounts –2007 v.1.5
 - ▶ Group Management – 2008 v.1.6
 - ▶ Password Profiles – Summer 2010 v.2.1
 - Role/Group based Password Requirements
 - ▶ Online Account Request – Spring 2012 v.2.2
 - ▶ Right Management – Spring 2012 v.2.2
 - ▶ Online Audits – Fall 2012 v.2.2
- 

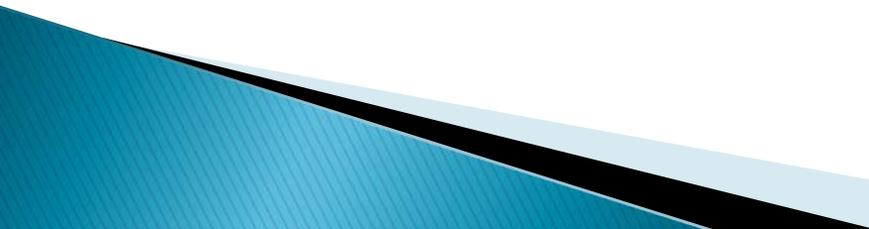
IDM/SSO Diagram



Shibboleth/CAS

- ▶ Shibboleth 2.3.x and CASShib 3.4.x provides Unified SSO between Academic Applications and Business Applications
- ▶ Allows IDM to spread authenticating beyond Perimeter while keeping Credentials Local
- ▶ Minimizes onboarding with applications
 - No distributing usernames and passwords

Integrated Systems Summary

- ▶ Active Directory
 - ▶ v3 LDAP (OpenDS, OpenLDAP, JDSEE)
 - ▶ Ellucian Product Suite (SSB, INB, Portal, TE...)
 - ▶ Google Apps
 - ▶ Hobsons CRM
 - ▶ VIVA Public Library
 - ▶ Blackboard
 - ▶ 100+ Shibboleth Systems
 - ▶ 50+ Internal LDAP/Other Systems
- 

Same Sign-On vs. Single Sign-On

- ▶ Use the right model for the situation
 - ▶ Application hopping need vs Application de-authorization
 - ▶ Application level de-authorization
 - Not every application supports Group/Role/Entitlement authorizations
 - Account level enabling/disabling only remaining option
- 

Difficulties

- ▶ Localized knowledge
 - No one to “call” to find solutions
 - Blessing and a curse.
 - Causes deep knowledge of problem domain but at the cost of time
 - No Training except in-house and sink or swim style training
- ▶ Ramp-up for new Developers can be high
- ▶ Finding the “right staff”
 - Adaptable to new technologies and knowledge of wide variety of systems
- ▶ Must design and develop many taken for granted concepts
 - What is a dictionary checker?

Difficulties cont..

- ▶ Login based on Affiliation difficult to manage and political
- ▶ Every rule has an exception
 - Must factor for exceptions in development cycle
- ▶ Balancing change/features requests can be political at times
- ▶ Account Management decisions can cause conflicts
 - Why did you set it up this way? vs. Because that is the way X company does it.

Benefits

- ▶ Developing our own concepts allows us to tailor concept to our needs
- ▶ Rapid development since developers have A-Z knowledge of system
 - Bug fixes usually take minutes/hours instead of days/weeks
- ▶ New features and requirements are a matter of time instead of cost

Benefits cont..

- ▶ Reduced administrative overhead
 - Application support teams focus more on user support than provisioning/de-provisioning
 - Common interface for account related queries/problems
 - Tailored administrative actions for your domain
- ▶ New Service rollouts are simple
 - Generally a few clicks to define service
 - Push request to create service for all or subset of users

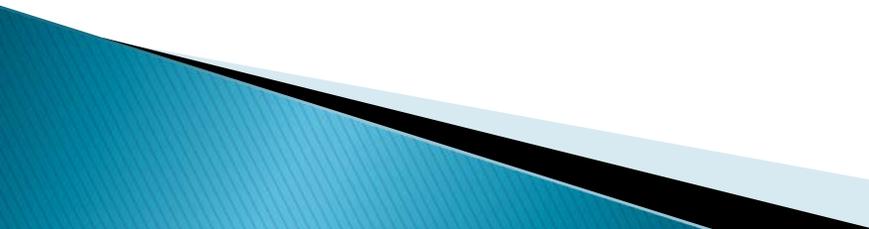
Lessons Learned

- ▶ Never be afraid to re-write
 - Nothing is perfect the first time
 - Once a feature is released, new use cases will appear
 - After a while, go back and refactor the original system with the new use cases
 - Rinse and repeat often

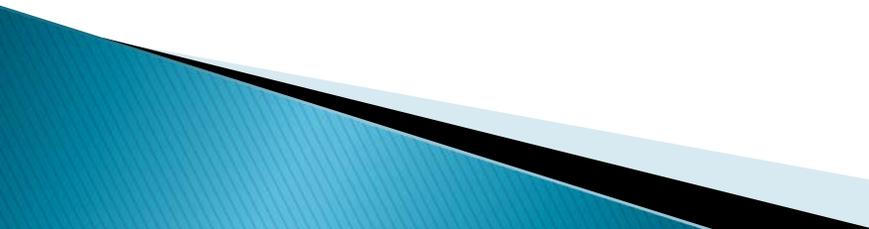
Lessons Learned cont..

- ▶ Don't fear "Lack of Support"
 - While initially rough, the knowledge gained feeds into a deep understanding of the system no training or support can match
 - Biggest hindrance to any home grown application
 - ▶ Local knowledge and experience beats support contracts any day
 - ▶ Always accept feedback/criticism
 - Middleware committee
 - Project Manager actively engaging stakeholders
 - Angry or Critical Customers
- 

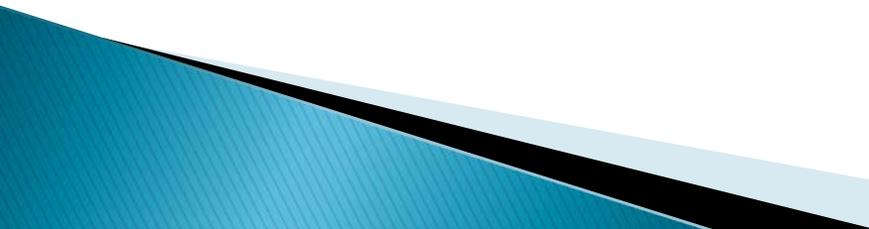
Lessons Learned cont..

- ▶ We have 2 developers.
 - One works on semester-ly project while the other handles integrations/small projects
 - ▶ Centralize Development as much as possible.
 - Constituent programs usually have other assignments. IDM development is typically not one of their priorities
 - ▶ Years of commitment
 - It's a **direction**, not a **project**
 - It never ends
 - ▶ Work tightly with subject matter experts on Constituent System Integrations
 - ▶ Give time for people to become acclimated to new features
- 

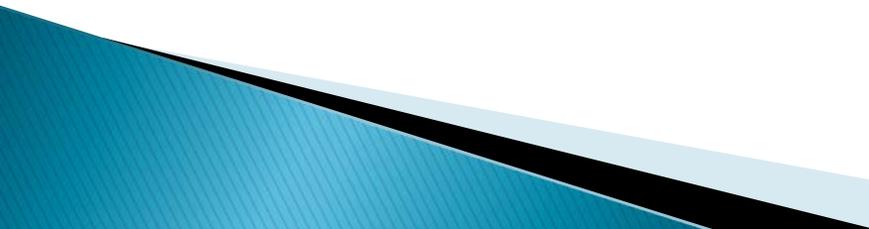
Lessons Learned cont..

- ▶ Ask your help desk their major source of pain and try and tackle that first
 - Solve the “biggest bang for the buck” applications first
 - ▶ Start small, but factor for the future
 - ▶ Always solve the big picture and not the problem at hand
 - Group up similar problems into a new component or management system
 - ▶ Always work towards “the way things should be” but accept “the way things are now”
 - Cheap/Easy solutions are usually not scalable or applicable to other problems
- 

Lessons Learned cont..

- ▶ Try and stick to standards as much as possible
 - DIY doesn't mean reinventing every wheel
 - ▶ Levels/stages of integration with systems
 - Password Only
 - Account creation/Deletion
 - Group/Right Management
 - Right Feedback and Change Tracking
 - Audited
- 

Futures

- ▶ Integration between SSO and IDM for seamless account management
 - While separate products, IDM becomes an increasingly backend service as SSO gains traction
 - ▶ Integration with Enterprise Service Bus for rapid application building and baked in IDM functionality
 - ▶ Revamped web experience and requirements for different classes of users (students / faculty / affiliates / non-credit)
 - ▶ Multifactor integration in SSO and IDM
- 

Questions?



Virginia e-Identity

Commonwealth Authentication Service (CAS)

Michael Farnsworth, DMV



The Phases of Evolution

- ▶ Initiation
- ▶ Concept
- ▶ Challenges
- ▶ Model Forward
- ▶ Lessons Learned

Initiation

- ▶ White Paper (Virginia Council on Technology Services)
 - ▶ Educational
 - ▶ Visionary, yet controversial
- ▶ Business Problem – Affordable Care Act/eHHR
- ▶ Strategic Alignment
 - ▶ COVA
 - ▶ AAMVA
 - ▶ CSDII
- ▶ NSTIC

Concept

- ▶ Government reform required to meet the need
- ▶ Authentication improvements become necessary
 - ▶ Fragmented processes lead to benefits fraud and problems with traceability
 - ▶ Problems worsen as on-line transactions increase
 - ▶ Government resources becoming scarce as population and benefits programs continue to grow

Concept

- ▶ Private sector authentication benefits not typically seen in government
 - ▶ Lower administrative costs, reduced theft and better/cheaper service to customers
 - ▶ Not using this technology results in losses

Challenges

- ▶ Initial Funding
 - ▶ Healthcare (ACA)
 - ▶ NSTIC
- ▶ Self Sustainment – Long term value proposition
- ▶ Monetization – (However, not about making money!)
- ▶ Privacy – NSTIC framework guidelines

Challenges

- ▶ Partnering States – Must demonstrate interoperability
- ▶ Interagency Relationships – Policy, regulations, territorial
- ▶ Legislative Impact
 - ▶ Liability
 - ▶ Public Perception

The Problems

- **Feds (HHS) estimates significant number of Virginia Medicaid Eligibility records are in an “error” status**
 - Represents hundreds of millions of dollars
 - Pressure on states by Feds to correct the problem
 - Eligibility fraud continues to grow
- **Duplicative Processes**
 - Processes performed by multiple agencies
 - Budget can no longer support duplication
- **No fully automated Commonwealth level communication exists between agencies for authenticating a citizen’s identity**



What Are We Doing About It?

▶ Collaborative effort

- ▶ Leverage current DMV business processes
- ▶ Technology implementation in tandem with VITA efforts (SOA/EDM)

▶ Phases

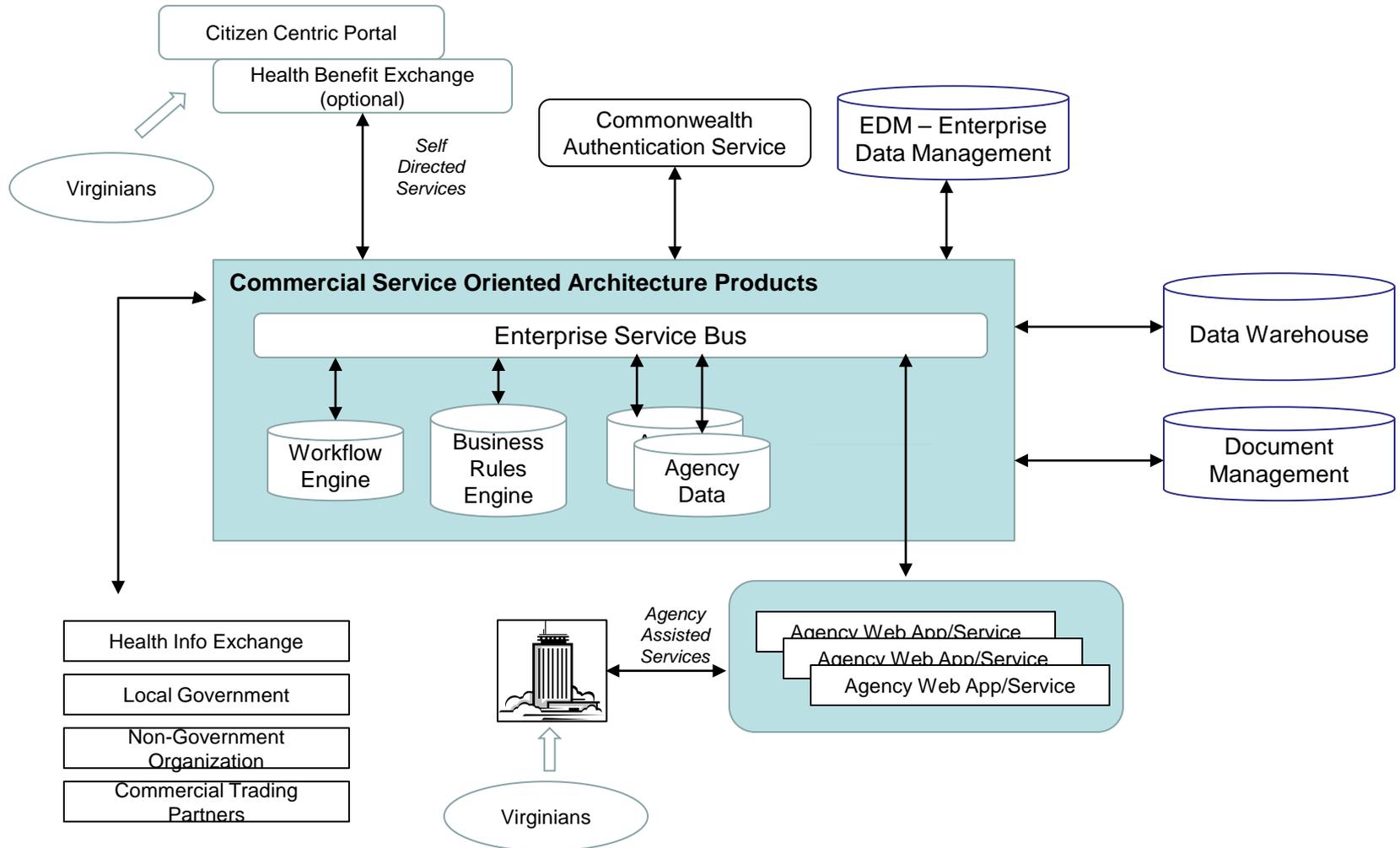
- ▶ Requirements and Design (Complete)
- ▶ Implementation (Underway)

▶ CAS offers

- ▶ NIST Level 1-3 compliant credentials, interoperable with Level 4
- ▶ Enterprise Identity Service
- ▶ Identity Proofing
- ▶ Multi-Factor (Strong) Authentication
- ▶ Identity Binding



Model Forward



CAS Essentials

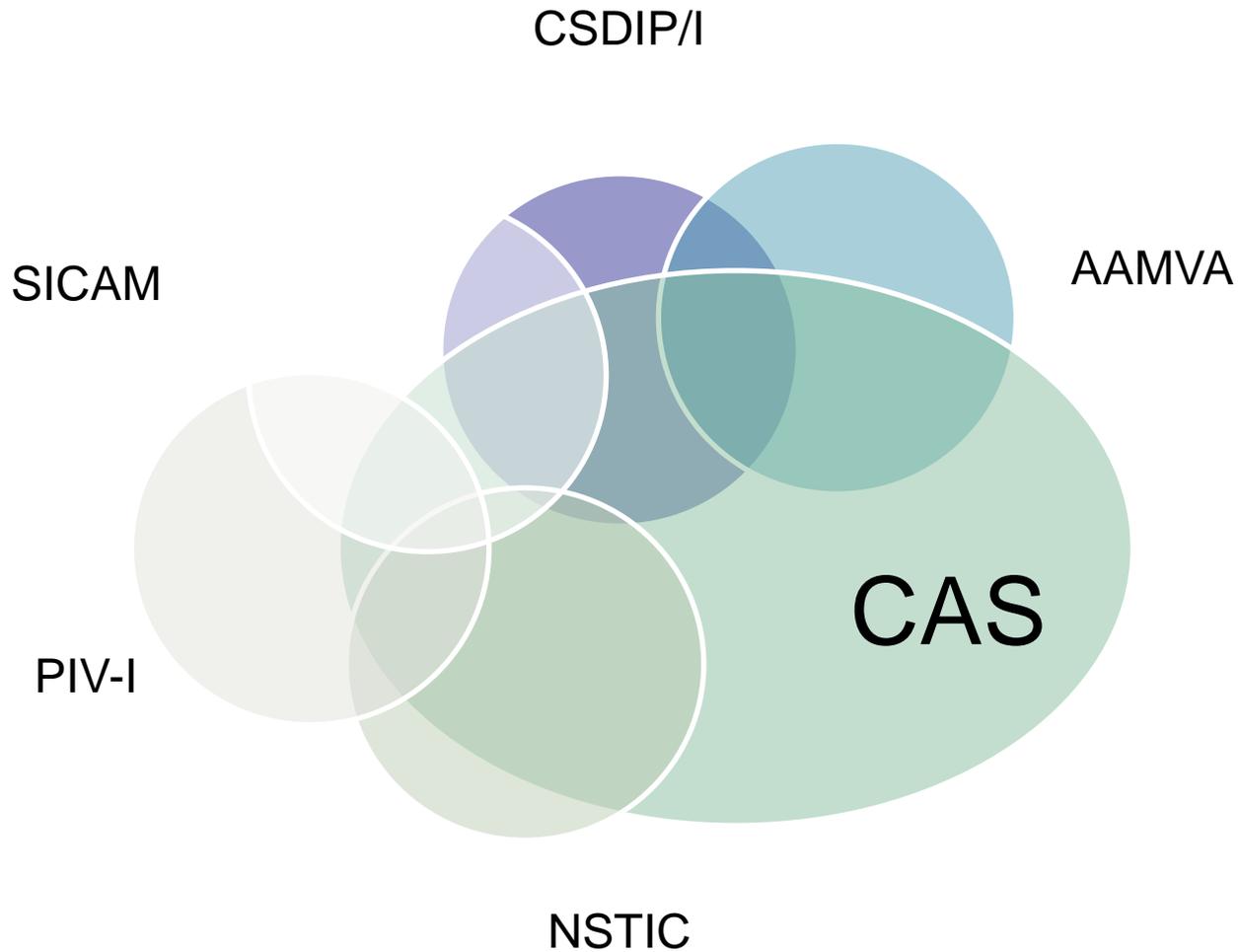
- **Designed for:**
 - Interoperability
 - Privacy
 - Ability to evolve and grow over time
 - Strategic positioning
- **What we have now**
 - Technology backbone in place
- **When**
 - Phase 1 Production January 2013 (Base Technology)
 - Phase 2 Production June 2013 (Strong Authentication/Binding)



Lessons Learned

- ▶ Must be driven from strategic vision
- ▶ Executive support is critical
- ▶ Funding must be in place
- ▶ Privacy community involvement is crucial
- ▶ Key stakeholders must see business value
- ▶ Must show results and tangible outcomes
- ▶ Start small
- ▶ Align initiative with industry leaders
- ▶ Leverage opportunities as they arise

Model Forward



Questions?

Michael P Farnsworth
CAS Project Manager

Michael.Farnsworth@dmv.virginia.gov





Virginia Information Technologies Agency

Information Security Council

ISO Manual Committee

Bob Auton, DJJ
IS Council Member

Benefits of ISO Manual

Provide information on IT security requirements for newly hired ISOs

Quick reference material for all ISOs

Central location for newly implemented requirements

Provides alternate methods for completing required processes

ISO Manual Committee Members

- Goran Gustavsson, Ex-officio, Auditor of Public Accounts
- Karen Ashby, Dept. for Aging and Rehabilitative Services
- Theresa Fleming, Dept. of Medical Assistance Services
- Melanie Seigler, Dept. of Forestry
- Cherrey Wallace, Dept. of Corrections
- Denny Casey, Virginia Museum of Natural History
- Bob Haugh, Co-Chair Dept. of Emergency Management
- Bob Auton, Co-Chair Dept. of Juvenile Justice
- **CSRM Support:** Bill Freda, VITA

ISO Manual Sections (Part 1)

1. So You've Just Been Appointed as Your Agency's Information Security Officer (10 Things You Should Do Immediately)
2. The Commonwealth's Information Security Governance Structure
3. Everything You Wanted to Know About SEC 501 But Was Too Afraid To Ask
4. The Agency's Information Security Program (The View From 50,000 Feet)
5. The Supporting Cast
 - Who (or what) is a System Owner and What Do They Do
 - Who (or what) is a System Owner and What Do They Do
 - What Is the Role of the Commonwealth Information Security Office
6. Business Process Analysis (Or Finding Out What Your Agency Really Does)
7. Sensitivity Analysis (Without the Help of a Shrink)
8. Risk(y) Assessment (Business)

ISO Manual Sections (Part 2)

9. Information Security Training
10. Agency Level Security Policy (The ISO's Opportunity to be King/Queen for a Day)
11. Responding to Security Incidents
12. Disaster Recovery Continuity of Operations
13. Exceptions, Exceptions, Exceptions
14. Audits Can Be Your Friends
15. How to Obtain Reports From Your Service Provider
 - What to Request and Who to Request It From
16. Mainframe Security

Appendices:

1. ISO Flow Chart
2. Documentation List
3. ISO Calendar

Assigned Sections

Committee Member	Topic Sections	Appendices
Bob Haugh	1 & 4	1
Cherrey Wallace	9 & 12	
Karen Ashby	13 & 14	3
Richard Benke	3	2
Theresa Fleming	2, 5 & 7	
Melanie Seigler	8	
Denny Casey	Reviewer	
Bob Auton	6, 15 & 16	

ISO Manual Sections Still Available:

10. Agency Level Security Policy (The ISO's Opportunity to be King/Queen for a Day)
11. Responding to Security Incidents

Yes, we are looking for volunteers who may have some spare time to write about the above open sections!

If you would like to volunteer to prepare one of the open sections please contact our Committee's CSRM Support:

Bill Freda (e-mail address Bill.Freda@vita.virginia.gov)

Questions?





Virginia Information Technologies Agency

ISO Certification Program Update

Ed Miller, VITA



Goal of the ISO Certification Program

- **GOAL:** The goal is to make Commonwealth IT systems more secure by assuring that the individuals who manage IT security understand and can apply the appropriate IT security controls and standards.
- Currently there are no prerequisites for being an Information Security Officer in the Commonwealth.
- There is also little consideration given to the security skill sets that an ISO needs.
- There is also no recognition given to an ISO who makes a commitment to improve or maintain his knowledge level in the field of information security.
- The COV ISO certification program is designed to set a minimum baseline for all ISO's to achieve.



Baseline for ISO Certification

Establishment of a baseline will provide the Commonwealth with:

- A better trained and knowledgeable staff
- An improved information security posture for the Commonwealth
- Increased protection for citizen and employee personal data
- An overall advancement of security goals



ISO Certification Paths

- CSRM recognizes that there are a number of IT security certifications already available and encourages *all* Commonwealth employees working the fields of IT Security or IT Auditing to obtain one or more of these certifications.
- There will be two paths to obtaining a COV ISO Certification.



PATH 1: If the ISO already has a professional security certification:

a. The ISO should send an email to CSRM indicating the professional security certification that they currently hold. CSRM will follow DoDD (Dept of Defense Directive) 8570 for recognizing certifications. DoDD 8750 requires individuals to carry an approved certification for IT security related job descriptions.

DoD DIRECTIVE 8570 Baseline Certifications

Information Assurance Technician Level 1	Information Assurance Technician Level 2	Information Assurance Technician Level 3
A+	GSEC	GSE
Network+	Security+	CISSP
SSCP	SCNP	SCNA
	SSCP	CISA
Information Assurance Management Level 1	Information Assurance Management Level 2	Information Assurance Management Level 3
GSLC	GSLC	GSLC
GISF	CISSP	CISSP
Security+	CISM	CISM

CND Analyst	CND Infrastructure Support	CND Incident Responder	CND Auditor	CN-SP Manager
GCIA	SSCP	GCIH	GSNA	CISSP
CEH	CEH	CSIH	CISA	ISSMP
		CEH	CEH	CISM



Commonwealth Accepted Certifications

CISSP (ISSA-Certified Info System Security Professional)
CISM (ISACA-Certified Information Systems Manager)
CISA (ISACA-Certified Information Systems Auditor)
CEH (Certified Ethical Hacker)
CSIH (Computer Security Incident Handler)
GCIA (GIAC Certified Intrusion Analyst)
GCIH (GIAC Certified Incident Handler)
GSE (SANS – GIAC Security Expert)



Commonwealth Accepted Certifications

GSEC (SANS - GIAC Security Essentials Certification)

GSLC (SANS - GIAC Security Leadership Certificate)

ISSAP (Information System Security Architecture Professional)

ISSEP (Information Systems Security Engineering Professional)

SCNA (Security Certified Network Architect)

SCNP (Security Certified Network Professional)

Security+ (CompTIA)

SSCP (Systems Security Certified Professional)



PATH 1: If you have a cert already

- b. Attend ISO Security Orientation at least once every 2 years.
- c. Successfully complete at least 1 course in the KC ISO Academy at least once a year
- d. Attend at least one ISOAG meeting per year (preferably the October meeting)
- e. Maintain compliance with the continuing educational requirements of the professional IT security certification body (by obtaining at least 20 add'l hours of training per year).
- f. It is the eventual goal for all ISO's to obtain one of the industry standard IT security certifications.



PATH 2: If the ISO does not currently hold a recognized professional IT Security certification:

- a. Attend ISO Security Orientation at least once every 2 years.
- b. Successfully complete at least 3 courses in the KC ISO Academy at least once a year
- c. Attend at least one ISOAG meeting per year (preferably the October meeting)
- d. Obtain an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to 3 hours each).



Current courses available in KC

System Owner Training
Sensitivity Analysis
Facilities Security (SEC517-00)
IT Data Protection Guideline (SEC507-00)
Contingency Planning (SEC508-00)
Systems Security: System Security Planning (SEC515-00)
Systems Security: Malicious code Protection (SEC515-00)
Systems Security: System Hardening (SEC515-00)
Threat Management: Threat Detection (SEC510-00)
Threat Management: Incident Handling (SEC510-00)
Threat Management: Logging and Monitoring (SEC510-00)
Logical Access: Account Management (SEC509-00)
Logical Access: Password Management (SEC509-00)
Logical Access: Remote Access (SEC509-00)
Personnel Security (SEC513-00)
Removal of Data (SEC514-03)
IT Asset Management (SEC518-00)
Use of Non-COV Equipment to Telework (SEC511-00)



Planned courses in KC

Data Owner Training

ISO Training

ISO Tools

Risk Management (under development, using NIST RMF, Risk Management Framework)

SDLC Security (SEC515-00)

IT Security Audit Standard (SEC502-00)

NIST Families (SEC501-07 / one/two courses for each family)

If you can't get to Knowledge Center, please contact the KC administrator at your agency. If its still an issue, contact Jane Carter at DHRM. Use of KC does require an MOA with DHRM but there are alternatives to that if your agency doesn't have one yet.

Steps to obtain COV ISO Certification for those who already have a professional security certification:

Possession of recognized professional IT Security Certification	CISSP, CISM, CISA, SANS (others to be determined)
VITA Training	Attend Information Security Orientation training
ISO Academy	Successful completion of at least one course in the KC ISO Academy per year
ISOAG attendance	Attend at least one mandatory ISOAG meeting per year (waived for calendar year 2012)
Continuing Education	Maintain compliance with the continuing educational requirements of the professional IT security certification body

Steps to obtain COV ISO Certification for those who do not have a professional security certification:

VITA Training	Attend Information Security Orientation training
ISO Academy	Successful completion of at least 2 courses per year in the KC ISO Academy
ISOAG attendance	Attend at least one mandatory ISOAG meeting per year (waived for calendar year 2012)
Continuing Education	Obtain an additional 20 hours of training in IT security related topics annually (ISOAG meetings count for up to 3 hours each!)



Summary

- We hope that this effort will enable the Commonwealth to assure that we have ISOs that:
 - Are equipped with the skills and knowledge needed to effectively manage an agency's security program,
 - Able to promote security awareness,
 - Able to implement & maintain the proper level of security controls,
 - Can mitigate / report security incidents,
 - And can maintain and enhance an effective working relationship with Commonwealth Security & Risk Management.

- Questions



- Thank You!



Virginia Information Technologies Agency

Upcoming Events





IS Orientation

When: Thursday, June 6, 2013

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1221

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>

Next IS Orientation will be held on Sept 5, 2013



Information Security System Association

ISSA

DATE: Wednesday, May 15, 2013

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: **TBD**

TOPIC: **TBD**

More info located here: <http://centva.issa.org/central-va-issa-feb-2013-meeting/>



SPRING 2013 CISA/CISM Review Classes

Training Sessions (3 Saturdays 9 am – 4 pm)

May 4, 2013

May 11, 2013

May 18, 2013

Courses include:

Overhead slides provided by ISACA

CISM or CISA test questions

Sample Test(s)

Study notes and other instructor provided materials

CISA or CISM Review Manual

Continental Breakfast and Lunch

Cost: \$500.00

Facility Location: EdgeComm

4913 Fitzhugh Ave., Suite 201

Richmond, VA 23230

Online registration will be open at <http://isaca-va.org/> very soon

Registration Closes: Monday, April 22, 2013



Future ISOAG Dates

June 5 **1:00 – 4:00 pm @ CESC**
Keynote Speaker: Zac Allen & Andrea Ross, DOC
on “KANBAN Project Management”

July 10 **1:00 – 4:00 pm @ CESC**
Keynote Speaker: Rosario Igharas, Virginia529
on “Data Management”

Aug 7 **1:00 – 4:00 pm @ CESC**
Keynote Speaker: Bennie Moore, Fed Reserve Bank
on “Crisis Management in Incident Response”

ISOAG meets the 1st Wednesday of each month in 2013



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

1 May, 2013



NORTHROP GRUMMAN



ADJOURN

