



Virginia Information Technologies Agency

Commonwealth Information Security Advisory Group (ISOAG) Meeting

January 25, 2007



ISOAG January 2007 Agenda

- | | |
|---------------------|----------------------|
| I. Welcome | Peggy Ward, VITA |
| II. IT Partnership | Don Kendrick, VITA |
| III. DMAS | Charles Lawver, DMAS |
| IV. Encryption | Don Kendrick, VITA |
| V. IT Legislation | Peggy Ward, VITA |
| VI. IREC | Jason Dolan |
| VII. Other Business | Peggy Ward, VITA |



Welcome!!!

Happy New Year!



Executive Orders Issued

Executive Order 43 (2007)

Protecting the Security of Sensitive Individual
Information in Executive Branch Operations

Executive Order 44 (2007)

Establishing Preparedness Initiatives in State
Government



Information Security Considerations

If your system contains sensitive data consider:

Is the data truly necessary?

If NO = Delete the field.

If Yes:

can the data collected be truncated (last four)?

&

are there other systems that collect the same data so the COV could consolidate the systems thereby reducing risk?



Commonwealth Information Security Officers Meeting

Don Kendrick
Senior Manager of Security Operations

January 25, 2007



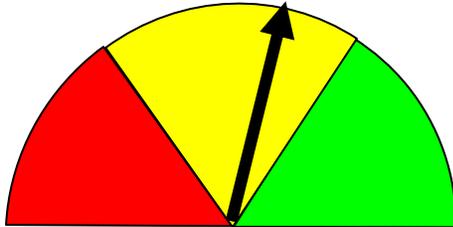
NORTHROP GRUMMAN

Agenda

- Service Delivery
- Transformation
- Customer Satisfaction
- Independent Verification & Validation

Service Delivery

Current Operations Dashboard



Central Metrics

	Nov	Dec
G	92.9%	100%
Y	7.1%	0%
R	0%	0%

Agency Metrics

	Nov	Dec
G	85.9%	90.0%
Y	3.8%	3.7%
R	10.3%	5.4%

Other Influencing Factors

Title	Description	Remedy
Unable to measure metrics against MOU SLOs	Measure and trend metrics	Include in Dec QoS Report (Closure: Mid Dec)
Cannot provide consistent superior service across the enterprise.	Combining agency IT departments resulted in non-standard systems/process	Standardization being pursued, but transformed systems required to provide consistent enterprise service.
Service Delivery must assimilate Transformed projects.	Transformation projects will be moved to Service Delivery incrementally.	Prepare plan for the incremental assimilation of transformed projects. (Closure: Mar 07)

Central IT Infrastructure Services

<u>Domain</u>	<u>Functional Area</u>	<u>December 2006</u>				<u>Post Transform</u>	<u>Coverage Action</u>
		<u>Prior Coverage</u>	<u>Current Coverage</u>	<u>Measures</u>	<u>Performance</u>	<u>SLAs</u>	
End User Services	Help Desk	36%	37%	5		19	Central actual 37% Field actual 24% Total actual 61% Enterprise goal 83%
	Messaging	21%	21%	2		10	Central actual 21% Field actual 51% Total actual 72% Enterprise goal 95%
	Desktop	13%	16%	3		14	Central actual 16% Field actual 59% Total actual 75% Enterprise goal 95%
Data Center Services	Server	6%	8%	2		21	Central actual 8% Field actual 70% Total actual 78% Enterprise goal 90%
	Mainframe	100%	100%	2		13	
Network Services	Data	90%	90%	1		25	
	Voice	0%	0%	0		19	VOIP coverage and Verizon metrics
Security Services	Security	100%	100%	1		9	

Central Operations Measures

Service Domain	Measure	MOU-SLO	M	J	J	A	S	O	N	D
End User Services	Average Speed to Answer	<30 sec	27	32	29	33	22	14	22	18
	Call Abandon Rate	< 5%	9.16%	5.41%	6.3%	6.1%	2.1%	.75%	2.0%	1.5%
	Email Response	<60 mins	14	15	15	15	16	18	16	16
	Voicemail Response	<30 mins	14	15	15	15	16	16	16	16
	First Call Resolution *	>70%	23%	21%	20%	20%	21%	61%	67%	73%
	VITA Messaging System Availability	>99.0%	100%	99.97%	99.98%	99.99%	100%	99.99%	100%	99.98%
	Shared Messaging System Availability	>99.0%	99.99%	99.80%	100%	100%	99.9%	100%	100%	99.98%
Data Center Services	IBM Mainframe Availability	>99.9%	99.98%	99.95%	100%	99.98%	100%	100%	100%	100%
	Unisys Mainframe Availability	>99.9%	100%	100%	100%	100%	99.9%	100%	100%	100%
	UNIX Server Availability	>99%	99.95%	99.87%	99.82%	99.82%	99.9%	99.8%	99.9%	99.9%
	Windows Server Availability	>99%	99.93%	99.88%	99.83%	99.96%	99.3%	100%	99.9%	99.4%
Network	Circuits Availability*	99.2%	99.5%	99.40%	99.2%	99.5%	99.4%	99.8%	99.7%	n/a
Security	ACF2 Logon Requests	95%					100%	99%	100%	100%
	Security Incident Reporting	95%					100%	100%	100%	100%

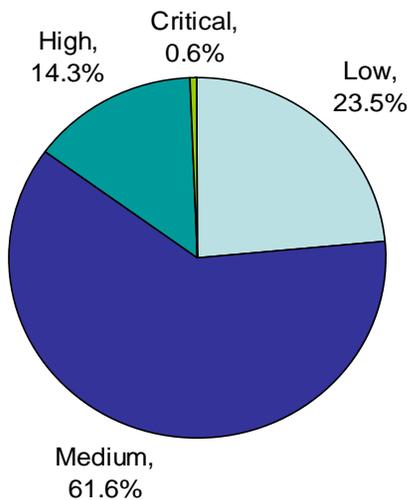
FCR – Start Oct measure is (Resolved on First Call/Can be Resolved on First Call. Previous measure was (Resolved on First Call/Total Calls)

Field IT Infrastructure Services

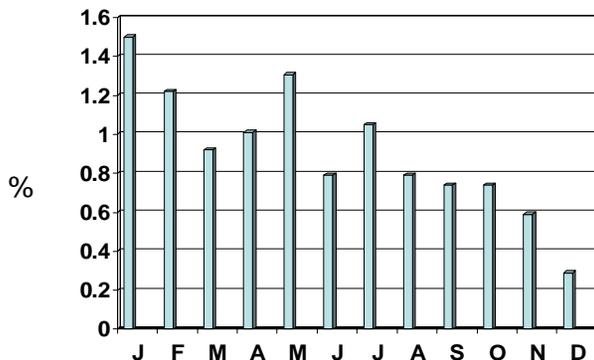
Domain	Functional Area	December 2006				Post Transform	Coverage Action	Performance Action
		Prior Coverage	Current Coverage	Measures	Performance G/Y/R	SLAs		
End User Services	Help Desk	0%	24%	7	31/1/2	19	Central actual 37% Field actual 24% Total actual 61% Enterprise goal 83%	Tax: Call Abandonment Rate at 6% for 3 months, Goal 5%
	Messaging	0%	51%	1	30/0/0	10	Central actual 21% Field actual 51% Total actual 72% Enterprise goal 95%	
	Desktop	0%	59%	3	72/9/14	14	Central actual 16% Field actual 59% Total actual 75% Enterprise goal 95%	Primary Issue DSS: High historic PC/Tech ratio (700/1), improving handoff from receipt of ticket to dispatch
Data Center Services	Server	0%	70%	6	139/1/0	21	Central actual 8% Field actual 70% Total actual 78% Enterprise goal 90%	DHRM: Single report Unix Server actual 98.8%, goal 99%
	Mainframe	N/A	N/A	N/A		13		
Network Services	Data	N/A	N/A	N/A		25		
	Voice	N/A	N/A	N/A		19		
Security Services	Security	N/A	N/A	N/A		9		

Service Delivery Incidents

Distribution of Incident Severity Since July 1, 2006



Percent Critical Tickets



- **Since July 1, 2006:**

- 18,377 incidents, 125 critical, 129 Incident Reports
- 60 Root Cause Analysis Opened; 46 Root Cause Analysis Closed

- **Significant Incidents in December:**

- 12/11,12/18, total 26 hours, DMV: Two outages on the same router caused slowdown in services at 33 CSCs, NG authorized replacement with transformation model due 1/31/07
- 12/11-12, total 25 hours, VDH: Two cable cut by nearby construction resulting in 90% of phones at Suffolk site down.
- 12/19, total 15 hours, DOA: Security certificate missing not allowing remote sites access to servers. Had to connect by 7am 12/20 to process payroll.

Transformation

Messaging Services



Enterprise Exchange/Outlook Email
Enterprise Collaboration Tools
Active Directory, DNS
\$25M Investment

Desktop



Mass Desktop Refresh Projects
Network Printer Consolidation and Refresh
Enterprise Desktop Management Systems
\$35M Investment

Help Desk



Enterprise Help Desk in Russell and Chesterfield
Field Based Agents and Technicians for Level 3
Enterprise Help Desk System (Peregrine)
\$10M Investment

Mainframe and Servers



New IBM and Unisys Mainframes
Consolidation and Refresh of Servers
Migration of servers to the Data Center
\$50M Investment

Transformation

People – Process – Tools
Reliable, High Performance,
Enterprise-Wide IT Infrastructure
\$270 Million Investment

Security



Enterprise Security Operations Center
Computer Security Incident Response Center
Secure Internet Gateway
\$10M Investment

Facilities Tier 3 and Tier 2



New Data Center/Office Building in Chesterfield
New Disaster Recovery Center and Help Desk
in Russell County
\$60M Investment

Network



New Commonwealth-wide MPLS Core WAN
LAN upgrades to Local Switches/Routers as Needed
Network Re-addressing of IP, DHCP
\$60M Investment

Voice / Video



Voice over IP Network Optimized for
Voice and Video Traffic
\$20M Investment

Transformation Rollout Overview

- Current rollout activities are centered around:
 - Desktop Refresh
 - Incident Management
 - GAL (Global Address List) updates
 - Network
 - Facilities
- Pilot Agencies have been contacted
- Kickoff for Service Delivery team Jan 5th
- Kickoff for Justice/Corrections Agencies Jan 9th
- Kickoff for Museum of Fine Arts Jan 11th
- “Communication Tracker” developed for transformation communication activities pending and executed at a program level

Schedule (Pilot)

Agency Name	Estimated Seat Count	Desktop Refresh		Incident Management		EMAIL GAL Synchron	
		Start	End	Start	End	Start	End
Veterans Services, Department of	125	Jan 07	Jan 07	Jan 07	Feb 07	complete	complete
Museum of Natural History, Virginia	65	Jan 07	Jan 07	Feb 07	Mar 07	complete	complete
Minority Business Enterprise, Department of	30	Jan 07	Jan 07	Mar 07	Mar 07	Jan 07	Feb 07
Criminal Justice Services, Department of	190	Jan 07	Jan 07	Feb 07	Mar 07	Feb 07	Mar 07

Schedule (Planned)

		Desktop Refresh		Incident Management		EMAIL GAL Synch	
Agency Name	Estimated Seat Count	Start	End	Start	End	Start	End
Virginia Museum of Fine Arts	249	Feb 07	Feb 07	Jan 07	Feb 07	Mar 07	Mar 07
Dept. of Correctional Education	1793	Feb 07	Mar 07	Mar 07	Mar 07	complete	complete
Dept. of Corrections	5719	Feb 07	May 07	Mar 07	Mar 07	complete	complete
Dept. of Juvenile Justice	1790	May 07	June 07	Mar 07	Apr 07	Feb 07	Mar 07

Schedule (Planned)

Agency Name	Estimated Seat Count	Desktop Refresh		Incident Management		EMAIL GAL Synch	
		Start	End	Start	End	Start	End
Dept. of Game and Inland Fisheries	314	May 07	Jun 07	Apr 07	Apr 07	Mar 07	Mar 07
Charitable Gaming Commission	51	Jun 07	Jun 07	Apr 07	May 07	Mar 07	Mar 07
Dept. Forestry	260	May 07	Jun 07	May 07	May 07	complete	complete
Dept. Labor & Industry	178	May 07	Jun 07	May 07	Jun 07	Mar 07	Mar 07
Dept. of Mental Health, Mental Ret. & Sub. Abuse Svcs.	4736	May 07	Jul 07	May 07	Jun 07	Jan 07	Jan 07

		2006					2007					2008					2009+						
months		J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A
Domains		Transformation Phase (36 Months to June 2009)																					
	General	Service Commencement Date 7/1/06 Procedures Manual (10/1/06) Procedures Manual Plan (8/1/06)					Process Cutover (Internal Apps)					ITIL Process Optimization Complete SCD+23 (6/1/08) DR Test at SWESC SCD+22 (5/1/08)											
	Help Desk	Incident Mgmt. Web Accessible (8/1/06)					Knowledge Mgt. System Operational 10/1/06					Production Incident Mgmt System / SPOC Help Desk (SWESC) SCD+24 (7/1/08)											
	Desktop						Desktop & asset mgmt system operational (1/1/07)					Begin Desktop Refresh (3/1/07)					Complete Desktop Refresh SCD+32 (3/1/09)						
EUS	Messaging	Single Statewide Address List SCD+9 (4/1/07)					DNS / WINS Infrastructure SCD+13 (8/1/07)					Enterprise messaging 90% complete SCD+ 35 (6/1/09)											
	Facilities						CESC Ready for Occupancy SCD+12 (7/1/07)					SWESC Ready For Occupancy SCD+16 (11/1/07)					RPB Migration Complete SCD+19 (2/1/08)						
DCS	Mainframe / Server	Infrastructure Ops Center (Interim) 11/1/06					Mainframe / server workload migration from RPB to CESC SCD+18 (1/1/08)					Server Consolidation 90% Complete SCD+35 (6/1/09)											
NWS	Data Network	Temp. NOC (11/1/06)					MPLS Core Complete SCD+14 (9/1/07)					Enterprise NOC SCD+16 (11/1/07)					Complete Agency LAN migration (90%) SCD+30 (1/1/09)						
	Voice						Arch Network Blueprint Addressing Plan (2/1/07)																
SS	Security	Interim Security Incident tracking and Mgmt System SCD+3 (10/1/06)					Enterprise Vulnerability Assessment Program Operational SCD+20 (3/1/08)					CSIRC Complete SCD+20 (3/1/08)					ESOC Complete SCD+23 (6/1/08)						

= Delivered
 = Delivered, awaiting final VITA acceptance
 = Delayed

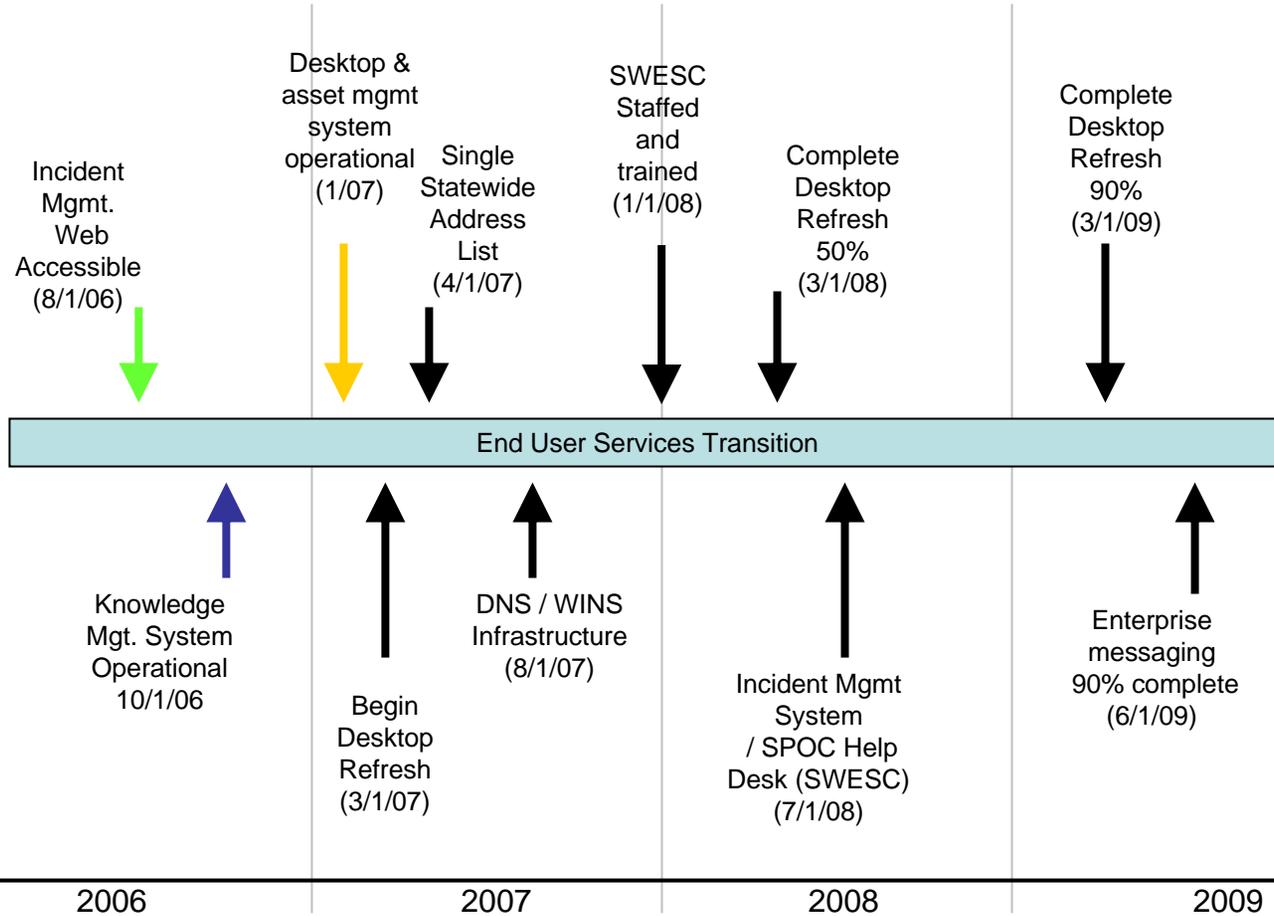
End User Services Transition

As Is

To Be

- 40+ separate help desks
- 20 incident management systems
- Limited call metrics
- Desk side agency support centric
- Multiple manufactures and support models
- 40+ email systems
- 40+ Global Address Lists
- Unsecured Messaging

- Enterprise help desk
- Single Incident management system
- Established call metrics
- Regionalized management services
- Standard systems, centralized software delivery, remote support
- Centralized messaging system
- Single Global address list
- Secure Messaging



Notes:

- SWESC – Southwest Enterprise Solutions Center, Russell County
- SPOC – Single Point of Contact Help Desk solution

▲ = Delivered / Complete

▲ = Delivered, awaiting final VITA acceptance

▲ = Delayed

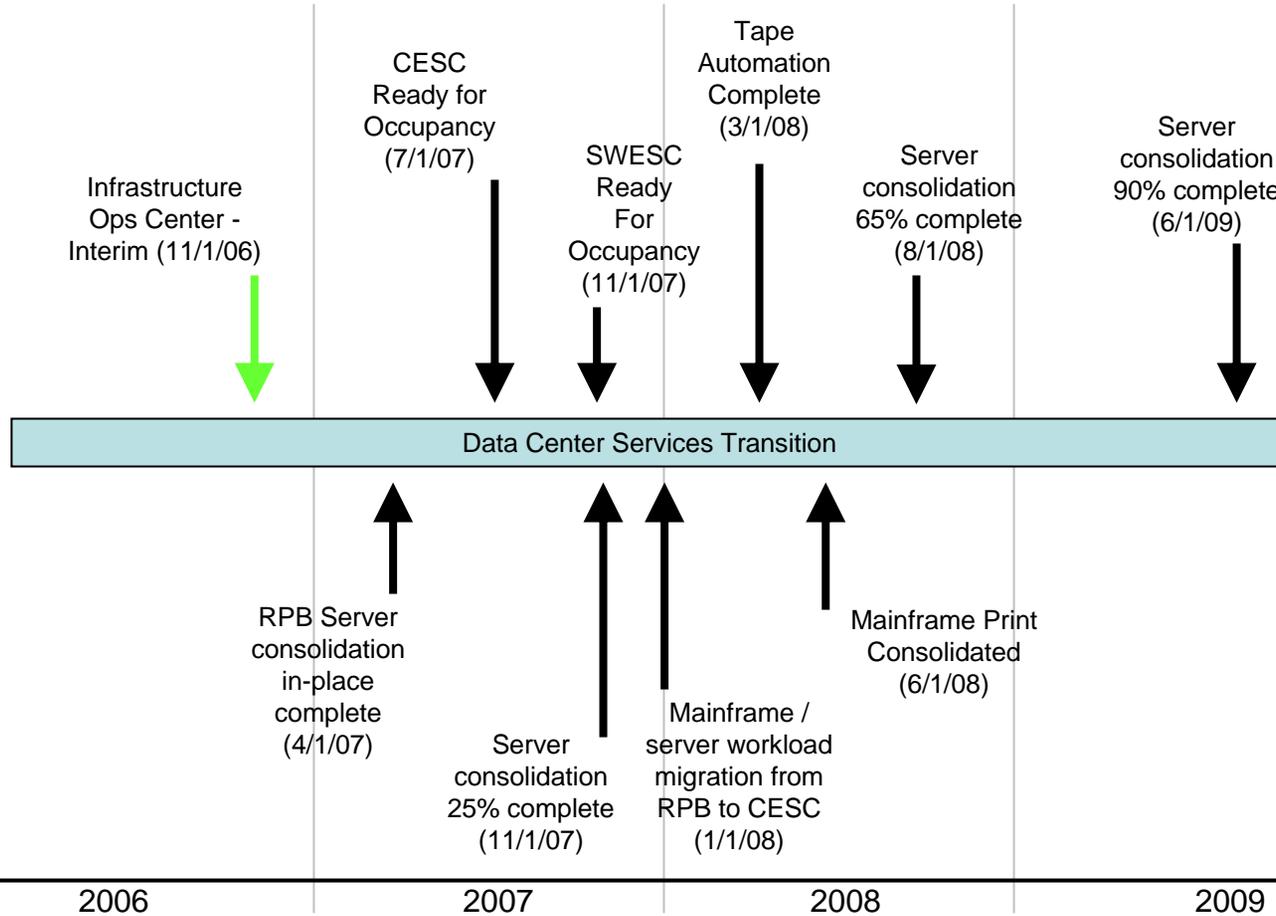
Data Center Services Transition

As Is

To Be

- 3000+ servers
75% distributed throughout agencies
- 3 mainframes located at RPB and VDACS
- Minimal performance monitoring
- Disaster recovery within 72 Hours
- No standard server tools or processes
- Multiple point storage solutions
- Remote high volume print operations
- Manual operations and tape management

- Consolidated storage servers and tape
- 75% centralized versus agency based server location
- Enterprise monitoring performance data
- 24 Hour disaster recovery
- Centralized operations and printing
- Automated tape processing and operations



Notes:

- CESC – Commonwealth Enterprise Solutions Center, Chesterfield County
- SWESC – Southwest Enterprise Solutions Center, Russell County
- RPB – Richmond Plaza Building Data Center

- ▲ = Delivered / Complete
- ▼ = Delivered, awaiting final VITA acceptance
- ▲ = Delayed

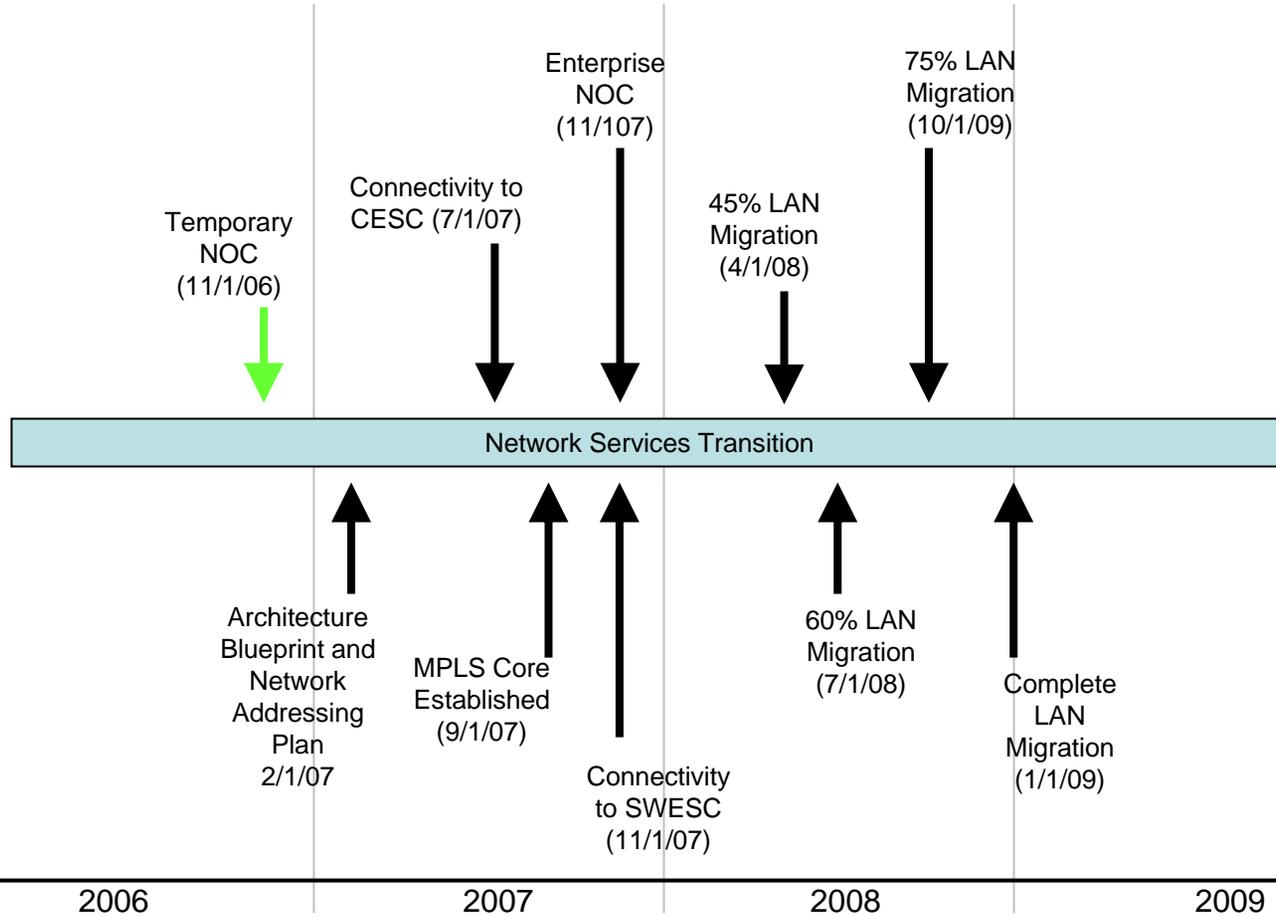
Network Services Transition

As Is

To Be

- Agency Centric Approach to Network Design, Management Operations
- Network Solution Not Scalable
- Varying Levels of Network Technology
- Multiple Connections (85+) to the Internet
- IP Address Duplication Across Agencies
- Frame Relay / ATM Network

- Enterprise-Managed Single Multi-Service Network
- Centralized Network Operations Center
- Reliable, Scalable and Secure Network Infrastructure
- Converged Communications (e.g., VoIP, QoS, MPLS / VPN)
- Increased Performance and SLAs
- Consolidated Internet Connections and WAN Links



Notes:

- NOC – Network Operations Center

▲ = Delivered / Complete

▼ = Delivered, awaiting final VITA acceptance

▲ = Delayed

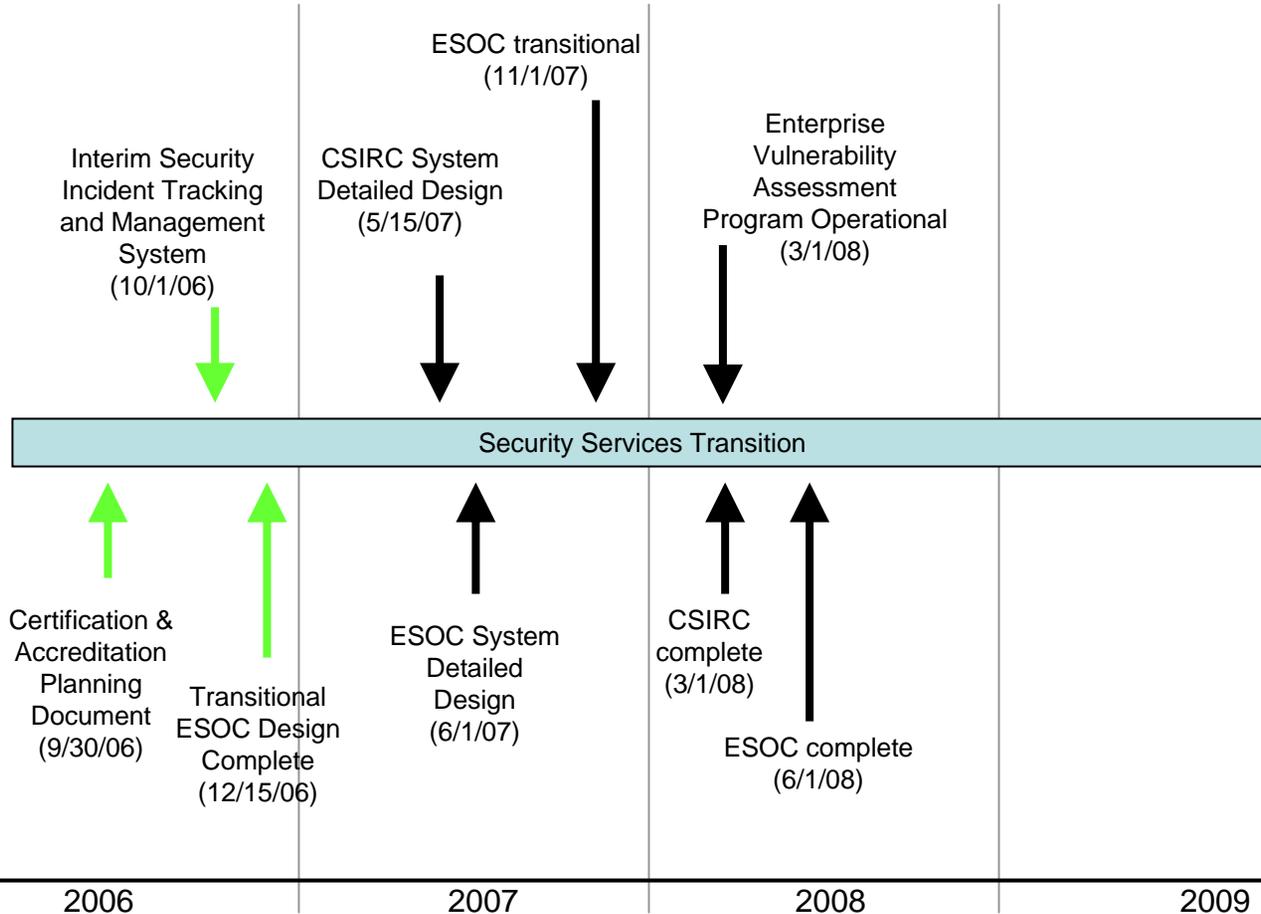
Security Services Transition

As Is

To Be

- 85 or More Internet Entrances to Defend to Varying Degrees, 40+ intrusion detection systems
- Various Levels of Security Monitoring
- Various Levels of Security incident Response
- No Enterprise Wide View of IT Security Status
- No Central Management of Enterprise Security Environment

- Two Internet Gateways, Strongly Defended
- 24x7 Enterprise Security Posture
- Centralized Highly Trained Incident Response Team
- Enterprise Security Dashboard Governance, Operational Control
- Centralized Management, Standardized Enterprise Security Protection



Notes:

- CSIRC – Computer Security Incident Response Center
- ESOC – Enterprise Security Operations Center

▼ = Delivered / Complete

▼ = Delivered, awaiting final VITA acceptance

▼ = Delayed

Customer Satisfaction

Improving Customer Satisfaction

- Customer satisfaction is a top priority
- VITA and Northrop Grumman are working together to develop and coordinate customer-focused strategies and initiatives
 - Improve customer satisfaction
 - Improve quality of services
 - Establish effective measurements (quantitative and qualitative) and feedback channels

Improving Customer Satisfaction

- Engaging our customers
 - Partnership Advisory Council
 - All AITR Meetings
 - Procurement Workgroup
 - Customer Account Teams
- Addressing top issues
 - Procure to Pay (P2P)
 - Request for Service (RFS)
 - Service Delivery

Procurement Work Group Initiatives

Based on customer feedback and involvement we have made or have planned improvements to the RFS and P2P process that have resulted in improvements. Some examples are:

Requests for Services

- Improved requirements gathering and processing
- Coordinated, frequent review of pending requests
- Communication and clarification of RFS versus P2P with stakeholders
- Define Service Level Objectives (2/07)
- Measure, monitor and report performance (3/07)
- Document processes in the Procedures Manual (4/07)

Procure to Pay

- Reduced procurement cycle time streamlining the review process, definition of scope and HW and SW standards and weekly review of PRs.
- Developed and implemented standard processes for Expiring Contracts, Urgent Procurements, Escalation of Issues and Procuring Assets with Federal Funds
- Implemented metrics to measure performance of processing purchase requests through the eVA system
- Continue to utilize the Procurement Working Group to identify issues and ways to improve the procurement process.
- Define Service Level Objectives (2/07)

Improving Service Delivery

- Engaging service delivery employees
 - Creating a mindset for excellent customer service and continuous improvement
 - Ongoing initiative to solicit and implement employee inputs
 - Identified 33 potential practices to improve customer experience
 - Measured enterprise wide compliance against 10 standard infrastructure practices (73% compliance) and establishing plans to upgrade remainder
- Developing targeted service-based surveys
 - Succinct, Web-based surveys to measure service delivery effectiveness
 - Help desk support (February)
 - Desktop support (March)
 - Enterprise Messaging (April)

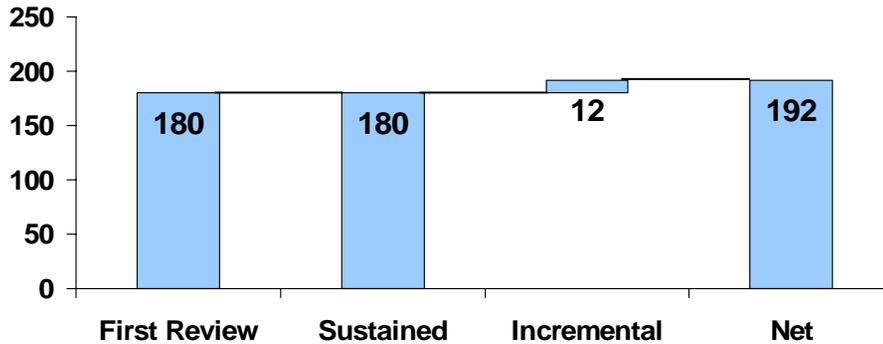
Service Delivery Improvements

- Central and Field Quality of Service Report issued monthly
- All critical tickets analyzed (129 reports) and root cause analysis accomplished on most significant critical tickets (60 opened, 49 closed)
- Service Delivery management notified of all critical tickets for immediate escalation of significant incidences
- More rapidly communicate incremental status information on vital service interruptions to stakeholders
- Hold weekly Telco issue review meetings and monthly management meetings with Verizon
- Improved Central Operations change control processes
- Measured enterprise wide servers against Center for Internet Security Configuration Standards and identifying improvements
- Evaluated our yearly mainframe patch process, consistent with best practices
- Drafted Emergency IT Operations Support Plan

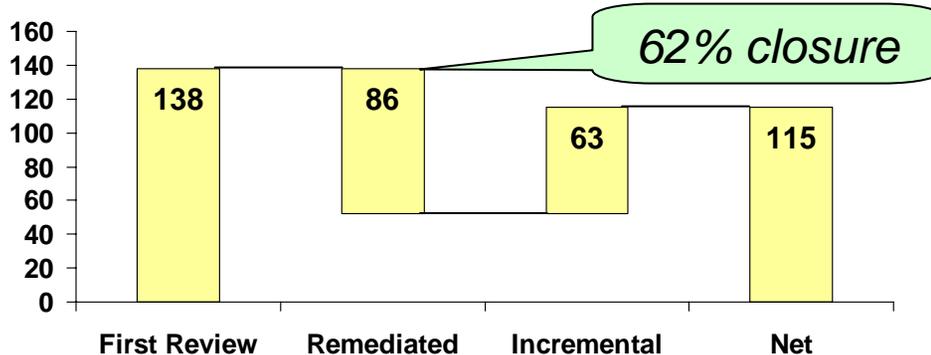
Independent Verification & Validation

Independent Verification and Validation (IV&V)

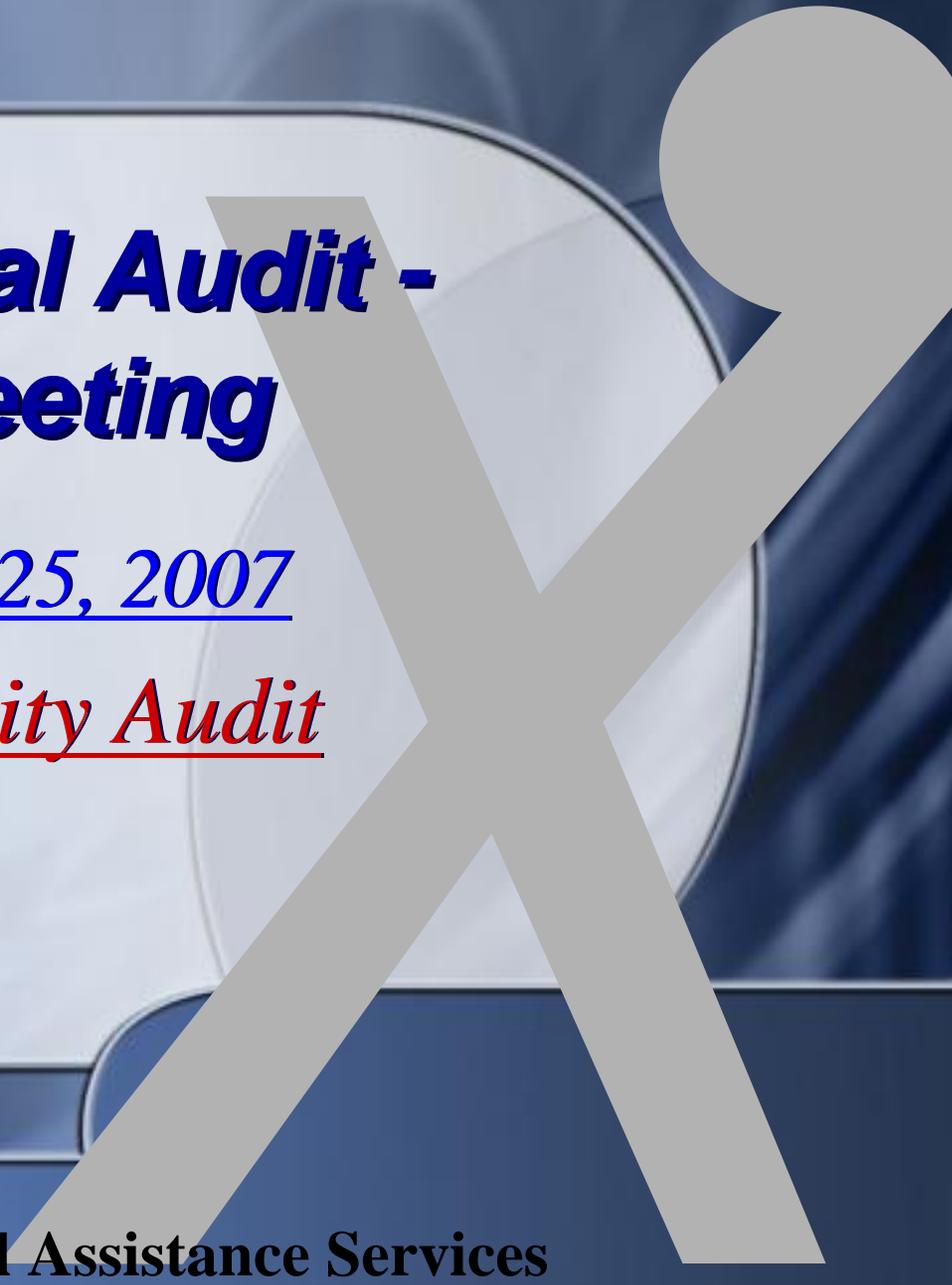
Positive IV&V Findings



Minor Negative IV&V Findings



- CACI conducted it's second, follow-up review Nov 27 – Dec 22
- Maturity level at 2+ (Repeatable)
 - No major negative findings
 - Significant progress on previous minor negative (62% closure)
 - Best practice cited regarding Committees, Forums and Workgroups
- Assessment expanding in two dimensions
 - Additional program theme of Stakeholder Management
 - Measured against next maturity level
 - Third review scheduled for April



***DMAS Internal Audit -
ISOAG Meeting***

Thursday, January 25, 2007

*Information Security Audit
Program*

ISOAG Meeting

--Medicaid is the largest health care system in Virginia (and the U.S).

--In FY 2005, the Virginia Medicaid Management Information System issued provider reimbursement to 55,000 active providers for the care of an average 691,000 recipients per month at a total cost of \$4.4 billion.

--In FY 2006, Medicaid claim payments increased to \$4.9 billion.

ISOAG Meeting

--Program costs are shared by the state and Federal government—the federal share is higher in states with lower per capita income.

--Eligibility Categories:

-Aged blind or disabled

-Member of a family with children

-Certain Medicare beneficiaries

ISOAG Meeting

--This immense claim and transaction volume can only be effectively audited using automated approaches to pre and post payment review.

--DMAS must pay quickly and, if we make a mistake, chase quickly, hence, the need for concurrent audit approaches.

-- In this environment information systems security audits are essential.

ISOAG Meeting

--DMAS is required by Federal law to perform a review of MMIS security at First Health Services Corporation (our Fiscal Agent) and of the DMAS information systems resources operating at our headquarters (600 East Broad Street in Richmond) every two years.

ISOAG Meeting

--The DMAS audit program we're discussing this morning covers the following Health Insurance Portability and Accountability Act of 1996 (HIPAA) security standards - 45 CFR - Parts 160, 162, and 164. The program was reviewed by the APA and found adequate for their reliance during their 2006 DMAS examination.

ISOAG Meeting

--The audit program divides the review into four categories:

-Organizational Requirements

-Administrative Safeguards

-Physical Safeguards

-Technical Safeguards

For example...

ISOAG Meeting

Organizational Requirements

- Policies, Procedures and Documentation Requirements, etc.

ISOAG Meeting

Administrative Safeguards

- Security Management Process Standard – Policy Making Process
- Security Management Process Standard – Risk Analysis – Risk Management, etc.

ISOAG Meeting

Physical Safeguards

- Facility Access Controls Standard – Contingency Operations
- Facility Access Controls Standard – Facility Security Plan, etc.

ISOAG Meeting

Technical Safeguards

- **Access Control Standard – Unique User Identifier**
- **Access Control Standard – Emergency Access Procedure, etc.**



Agency Encryption Requirements Survey

Don Kendrick
Senior Manager of Security Operations

January 25, 2007



NORTHROP GRUMMAN

Agency Encryption Requirements Survey

- As of January 10th:
 - 39 Agencies have responded.
 - Requirements:
 - 46% Encrypting email.
 - 33% Secure remote access.
 - 31% Secure internal or external web site traffic.
 - 29% Secure file transfer.
 - 27% Data at rest (laptops, USB, database)
 - 23% Wireless Security.

Agency Encryption Requirements Survey

- Next Steps:
 - Requirements have been distributed based on functional towers.
 - Teams forming to include NG Tower Lead, NG Security representative, and VITA SMO SLD manager.
 - Map “included” product sets to requirements, do gap analysis on remainder.
 - Bring recommended product set to Architecture team.
 - Distribute to this forum for comment.
 - Produce rates for add on services.



Virginia Information Technologies Agency

2007 General Assembly Session IT Legislation Update

Peggy Ward





HB1603

Multiline telephone systems; owner or operator thereof ability to identify location from 9-1-1 call.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB1603>

Multiline telephone systems. Requires owners or operators of multiline telephone systems serving residential facilities, hotels and motels, business locations, and educational institutions to ensure that a public safety answering point is able to identify the location from which a call to 9-1-1 is placed. *Patrons:* Rapp, O'Bannon and Orrock



HB 1885

Voice-over-Internet protocol service; revises definition.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB1885>

Voice-over-Internet protocol service. Revises the definition of Voice-over-Internet protocol service to eliminate references to the public switched telephone network and a requirement for the use of Internet protocol-compatible customer premises equipment. Providers of Voice-over-Internet protocol service are exempt from regulation by the State Corporation Commission. *Patron:* Marshall, R.G.



HB 2140/SB 1244

Identity theft; notification of breach of information system.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2140>

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1224>

Database breach notification. Requires an individual or a commercial entity that conducts business in Virginia and that owns or licenses computerized data that includes personal information to conduct in good faith a reasonable and prompt investigation when it becomes aware of a breach of the security of the system. If the investigation determines that misuse of information has or is reasonably likely to occur, the individual or commercial entity shall give notice to the Virginia resident as soon as possible. Notification must be made in good faith, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. The bill also contains alternative notification provisions. The Office of the Attorney General may bring an action in law or equity to address violations of this section and other appropriate relief. The provisions of this bill, as they apply to governmental entities, become effective July 1, 2008. *House Patron: Brink*
Senate Patron: Howell



HB 2196

Chief Information Officer; powers and duties.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2196>

Powers of the CIO. Gives the CIO of the Commonwealth the power to enter into contracts with one or more other public bodies, or public agencies or institutions or localities of the several states, of the United States or its territories, or the District of Columbia for the provision of information technology services. *Patron:* Nixon



HB 2198

HB 2198 Electronic health records; requires those purchased by state agency to adhere to accepted standard.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2198>

Electronic health records. Requires any electronic health records system or software purchased by a state agency to adhere to accepted standards for interoperability or to be certified by a recognized certification body. *Patron:* Nixon



HB 2306/SB 1342

Public institutions of higher education; operational authority.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2306>

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1342>

Public institutions of higher education; operational authority. Provides operational authority for public institutions of higher education in the areas of information technology and procurement pursuant to the Restructuring Act of 2005. *House Patron: Callahan Senate Patron: Houck*



HB 2870

Cellular telephones; encouraged to program with ICE numbers

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2870>

Programming cell phones with ICE numbers. Requires providers of commercial mobile telecommunications service to implement a program, in accordance with criteria developed by the Wireless E-911 Services Board, of encouraging its subscribers to program one or more ICE numbers into their mobile telephones. An ICE number is a telephone number that is programmed into a mobile telephone, and labeled ICE, which when called by a firefighter, paramedic, emergency medical technician, rescue worker, or ambulance when the subscriber is nonresponsive or impaired, will connect to the person who the subscriber desires to be contacted in case of an emergency. *Patron: McEachin*



HB 2496

Chief Information Officer; powers and duties.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2946>

Powers of the CIO; information technology recycling. Requires the CIO to contemporaneously account, to the greatest extent possible, for the recycling and disposal of information technology investments when developing policies and procedures for the procurement of such investments. *Patrons:* Plum and Nixon



HB 2973

Unsolicited bulk electronic messages; changes scope of State's spam law

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2973>

Unsolicited Bulk Electronic Messages; cell phone spam; penalty. Changes the scope of Virginia's spam law from electronic mail to electronic messages by defining electronic message as any text, image, or other communication transmitted to a computer. The bill also adds wireless communications devices to the type of devices defined as computers. The bill reduces the number of messages necessary for a person to meet the requirements of this section to 2,500 attempted recipients in any 24-hour period, 25,000 attempted recipients in any 30-day time period, or 250,000 attempted recipients in any one-year time period. Additionally a new provision would make sending unsolicited bulk electronic messages a Class 6 felony if a single recipient of an electronic message or multiple electronic messages incurs damages in excess of \$250 during any one year time period.

Patron: Bell



HB 3148

Compromised Data Disclosure Act; created

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB3148>

Compromised Data Disclosure Act. Creates the Compromised Data Disclosure Act, which requires state agencies to notify residents of Virginia when their personal information maintained by a state agency has been compromised through a breach of a security system or otherwise acquired by an unauthorized person. The bill requires the Virginia Information Technology Investment Board to establish policies and procedures to implement the provisions of the bill. The bill defines personal information. *Patron:* Bulova Sickles



SB 845

State agencies; Chief Information Officer to develop policies, etc. relating to security data.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB845>

Security of confidential state data. Requires the Chief Information Officer of the Commonwealth to develop policies, procedures, and standards relating to the security data maintained and used by state agencies. The policies, procedures, and standards must include requirements that a user be required to provide a password or other means of authentication to access a computer and to access a state-owned or operated computer network or database through the computer, and that a digital rights management system be used to control access to electronic records containing confidential information. *Patron:* Devoletes Davis



SB 1004

Telecommuting; use of personal computers.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1004>

Telecommuting; use of personal computers. Authorizes a state agency to allow employees to use computer equipment not owned or leased by the Commonwealth to telecommute, so long as such equipment is not used to access or store data made confidential by state or federal law. The bill contains an emergency clause.
Patron: Devolites Davis



SB 1029

Chief Information Officer; to incorporate computer security into 4-year strategic plan.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1029>

Powers of the Chief Information Officer (CIO); information security. Requires the CIO of the Commonwealth to monitor trends in information security and incorporate computer security into the four-year strategic plan for information technology.

Patron: O'Brien



SB 1111

Freedom of Information Act; closed meetings and security of public buildings.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1111>

Freedom of Information Act; closed meetings; security of public buildings. Adds a closed meeting exemption for the discussion of reports or plans related to the security of any governmental facility, building or structure, or the safety of persons using such facility, building or structure.

Patron: Houck

2007 INFORMATION RISK EXECUTIVE COUNCIL®

A Proven Resource for Addressing Your Urgent Priorities

AB Volvo • Abbott Laboratories • Abercrombie & Fitch Co. • ADC Telecommunications, Inc. • Adecco SA • Adobe Systems, Inc. • ADT Security Services, Inc. • Advance Auto Parts, Inc. • Advanced Micro Devices, Inc. • Aetna, Inc. • Aflac, Inc. • A.G. Edwards & Sons, Inc. • Agilent Technologies, Inc. • Agrilliance, LLC • AgStar Financial Services • AIG Private Bank • Air France • Airservices Australia • Alzco Nobel N.V. • Albany International Corp. • Albemarle Corporation • Albertsons, Inc. • Alcatel • Alcoa, Inc. • Allegis Group, Inc. • Allergan, Inc. • Alliance Data Systems Corporation • ALLTEL Corporation • ALSAC—St. Jude Children's Research Hospital • Altacor, Inc. • Altria Group, Inc. • Amazon.com, Inc. • Amcor Ltd. • American Airlines, Inc. • American Cancer Society, Inc. • American Crystal Sugar Company • American Eagle Federal Credit Union • American Greetings Corporation • AMERIGROUP Corporation • Amkor Technology, Inc. • Anheuser-Busch Companies, Inc. • Applebee's International, Inc. • Apple Computer, Inc. • ARAMARK Corporation • Arbitron Inc. • Archstone-Smith • Ariba, Inc. • Arizona Supreme Court • Arkansas Blue Cross and Blue Shield • Arkema, Inc. • Arrow International, Inc. • ASML Holding N.V. • Assurant, Inc. • Atlantic Lottery Corporation, Inc. • Australian Public Service Commission • Automobile Club of Southern California • Avaya, Inc. • Aviall, Inc. • Avon Products, Inc. • AXA UK plc • Axpo Holding AG • Babson College • Bacardi Ltd. • BAE Systems, Inc. • Balboa Insurance Group, Inc. • Ball Corporation • Bally International AG • Banco BPI • Banco de Crédito Inversiones • Banco Nacional de México • BancWest Corporation • BankBoston Argentina • Bank of America Corporation • Baptist Health South Florida • Barclays PLC • Barnes and Noble, Inc. • Basell B.V. • BASF Aktiengesellschaft • Baylor Health Care System • BB&T Corporation • BCD Travel B.V. • Bearing Point, Inc. • BEA Systems, Inc. • Belgacom SA • Bell Canada International, Inc. • Benjamin Moore & Co. • Best Buy Co., Inc. • Big Lots Stores, Inc. • Biovail Corporation • BJ's Wholesale Club, Inc. • The Black & Decker Corporation • Bloomberg L.P. • Blue Cross and Blue Shield of Louisiana • BMO Financial Group • BMW Manufacturing Co. • Boar's Head Provisions Co., Inc. • The Boeing Company • Boeing Integrated Defense Systems • Bombardier • Bonnier AB • Bose Corporation • The Boston Beer Company, Inc. • BP p.l.c. • Bridgestone Americas Holding, Inc. • Briggs & Stratton Corporation • Brightpoint, Inc. • Brinker International, Inc. • Bristol-Myers Squibb Company • British Airways Plc • British Sugar Plc • Britvic Soft Drinks Ltd. • Brown Brothers Harriman & Co. • BT Group plc • Burger King Corporation • Cabela's, Inc. • Cadbury Schweppes plc • CAE, Inc. • Caja Madrid • California State Lottery • Canadian Imperial Bank of Commerce • Canon, Inc. • The Capital Group Companies, Inc. • Career Education Corporation • CareFirst BlueCross BlueShield • Caremark Rx, Inc. • Cargill, Inc. • Carlsberg A/S • Carl Zeiss Meditec AG • Carnival Corporation • The Carphone Warehouse Group PLC • Caterpillar, Inc. • CBS Television • Celestica, Inc. • CEMEX, Inc. • Centers for Medicare & Medicaid Services • Centrica plc • Ceska sportelna a.s. • CheckFree Corporation • Chemoil • Chesapeake Corporation • Chick-fil-A, Inc. • Chico's Retail Services, Inc. • Chipotle Mexican Grill, Inc. • Chiquita Brands International, Inc. • Choice Hotels International • Chubu Electric Power Company, Inc. • Church & Dwight Co., Inc. • Church Pension Group • CIGNA Corporation • Citibank International • Citizens Gas and Coke Utility • City National Bank • Clark Construction Group, LLC • Clifford Chance LLP • ClubCorp • CNH Global N.V. • Coach, Inc. • The Coca-Cola Company • Coinstar, Inc. • Colgate-Palmolive Company • Comcast Corporation-Comcast Cable • Commonwealth of Virginia • CompUSA, Inc. • ConAgra Foods, Inc. • Conair Corporation • Condé Nast Publications, Inc. • ConocoPhillips • Consolidated Container Company • Constellation Energy Group, Inc. • Continental AG • Convergys Corporation • Cornell University • Corning, Inc. • Costco Wholesale Corporation • Countrywide Financial Corporation • Covance, Inc. • Crane Co. • Crate and Barrel • Crédit Agricole S.A. • Credit Union Central of Canada • Crosstex Energy Services • Crowe Chizek and Company LLC • CTT Correios de Portugal • CUNA Mutual Group • Cushman & Wakefield, Inc. • DaimlerChrysler AG • Dairy Farmers of America, Inc.

*Increasing the Effectiveness of
Executives and Their Enterprises*



25+

Years of Experience

The Corporate Executive Board is the world's premier network for leading executives to solve their most urgent shared challenges.

40+

Distinct Executive Programs

Members use the collective experience and insight of our network every day to improve their personal and corporate performance.

45+

Countries Represented in Our Network

Our shared-cost research model allows us to provide insight at the quality standard of the leading strategy consultants but at a fraction of the cost.

3,000+

Member Organizations Worldwide



EXBD on NASDAQ

OUR CORE VALUES

Force of Ideas

We believe that great ideas—acute insights rooted in microeconomics and informed by human behavior—can carry an organization forward more surely than can access to superior resources, market power, or sheer effort. Our corporate task is to discover these ideas wherever they arise, within and beyond the membership, and to teach them to the membership at large.

Spirit of Generosity

Our ambition is to forge relationships with our members that go beyond the merely commercial. This spirit is expressed in our business model, which directs that wherever possible we provide our services in unlimited amount. This aim beyond commerce also informs our personal relations; our goal is to serve members and each other beyond expectation and with appreciation, bringing honest joy to the opportunity to serve.

THE FIRM IN BRIEF

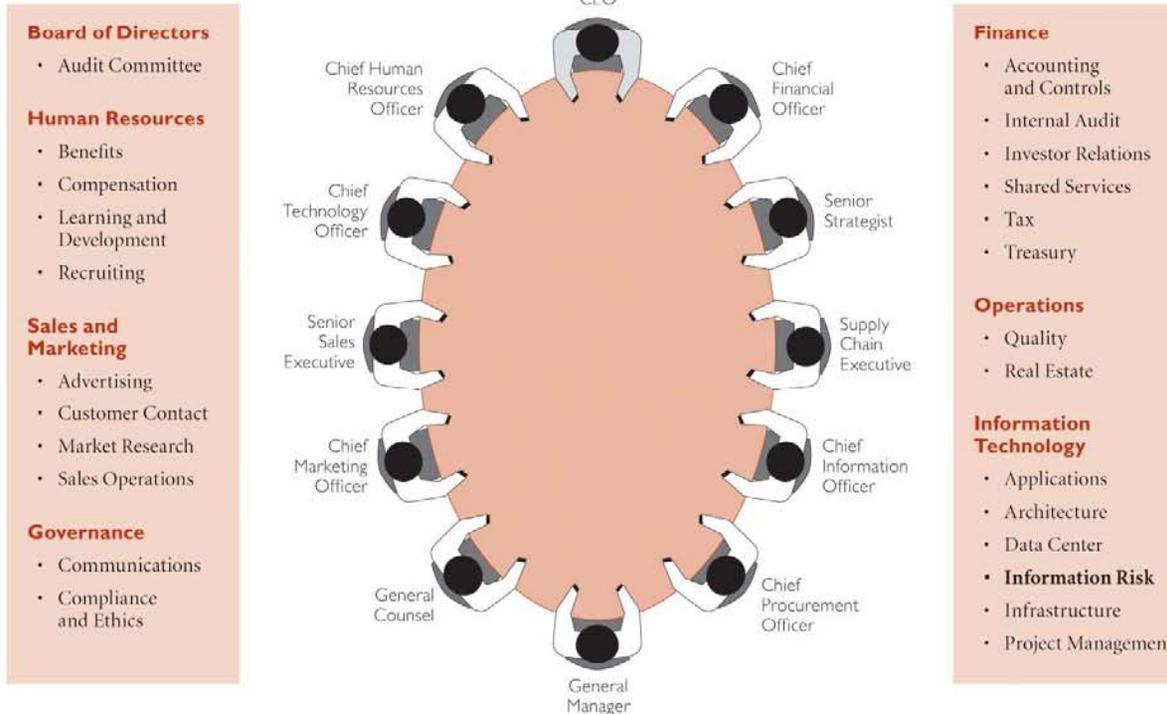
The Corporate Executive Board provides best practices research, decision-support tools, and executive education to a membership of the world's leading corporations and not-for-profit institutions. Our member network spans all major areas of functional management, general management, and organizational governance. Our work focuses on identifying practical solutions—strategies, frameworks, and time-saving tools—that will allow our members to avoid rework and duplication of effort in addressing their urgent priorities.

With more than 25 years of experience in managing high-quality executive memberships, more than 3,000 large corporate members around the world, and 2,400 staff in our Washington, D.C., London, and New Delhi offices, we are more excited than ever about the unique capability we offer our members and the opportunities that lie ahead to extend our impact on the executives and enterprises we serve.

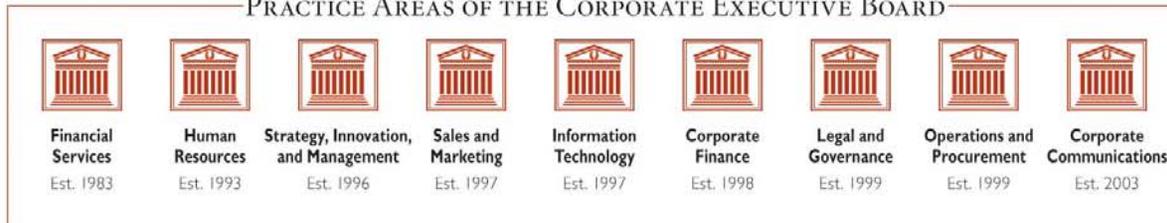
THE WORLD'S PREMIER EXECUTIVE NETWORK

Connecting Thought Leaders to Each Other and to New Ideas

Functions Served by Executive Board Memberships



PRACTICE AREAS OF THE CORPORATE EXECUTIVE BOARD



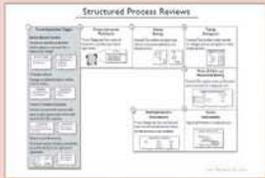
A PROVEN MODEL FOR CREATING VALUE

Delivering High-Quality Insights, Practitioner, Peer-Tested Resources—at Low Cost

	CEB IT Practice's Focus	Traditional IT Research Firms' Focus
Perspective	<ul style="list-style-type: none"> • Cross-functional, business-driven IT perspectives provided through programs established with senior executives across the enterprise 	<ul style="list-style-type: none"> • Siloed IT-centric perspective with memberships comprising senior and junior executives
Objectivity	<ul style="list-style-type: none"> • Annual membership contributions represent 100% of our revenue 	<ul style="list-style-type: none"> • Up to 40% of revenue from vendors • Follow-on consulting services
Agenda	<ul style="list-style-type: none"> • Research agenda set by members annually 	<ul style="list-style-type: none"> • Analyst-set research agenda
Methodology	<ul style="list-style-type: none"> • Step-by-step management guides based on proven practices from peer organizations • Focus on field-tested management practices and implementation tools • Peer-tested reviews of technologies and infrastructures 	<ul style="list-style-type: none"> • Analyst-based management recommendations unproven at real organizations • Focus on technology and vendor recommendations
Pricing	<ul style="list-style-type: none"> • Annual fixed contribution provides enterprise-wide, unmetered access • Unlimited event attendance, customized research projects, and research downloads across team 	<ul style="list-style-type: none"> • Incremental fees for “premium services” such as analyst calls and custom research • Seat-based charges for events and access to research

Emphasis on a Member-Centric Agenda Executed to Deliver Immediate Value

Step-by-Step Implementation Guides from Member Companies



Implementation Tools and Templates



Vendor-Free Member Events



Vendor Knowledge Exchange



Online inventory of peer-tested reviews and direct networking on technologies and infrastructures

INTRODUCING THE IT PRACTICE

Member-Directed Resources for Each Constituency

OUR PRACTICE DESIGN PRINCIPLES

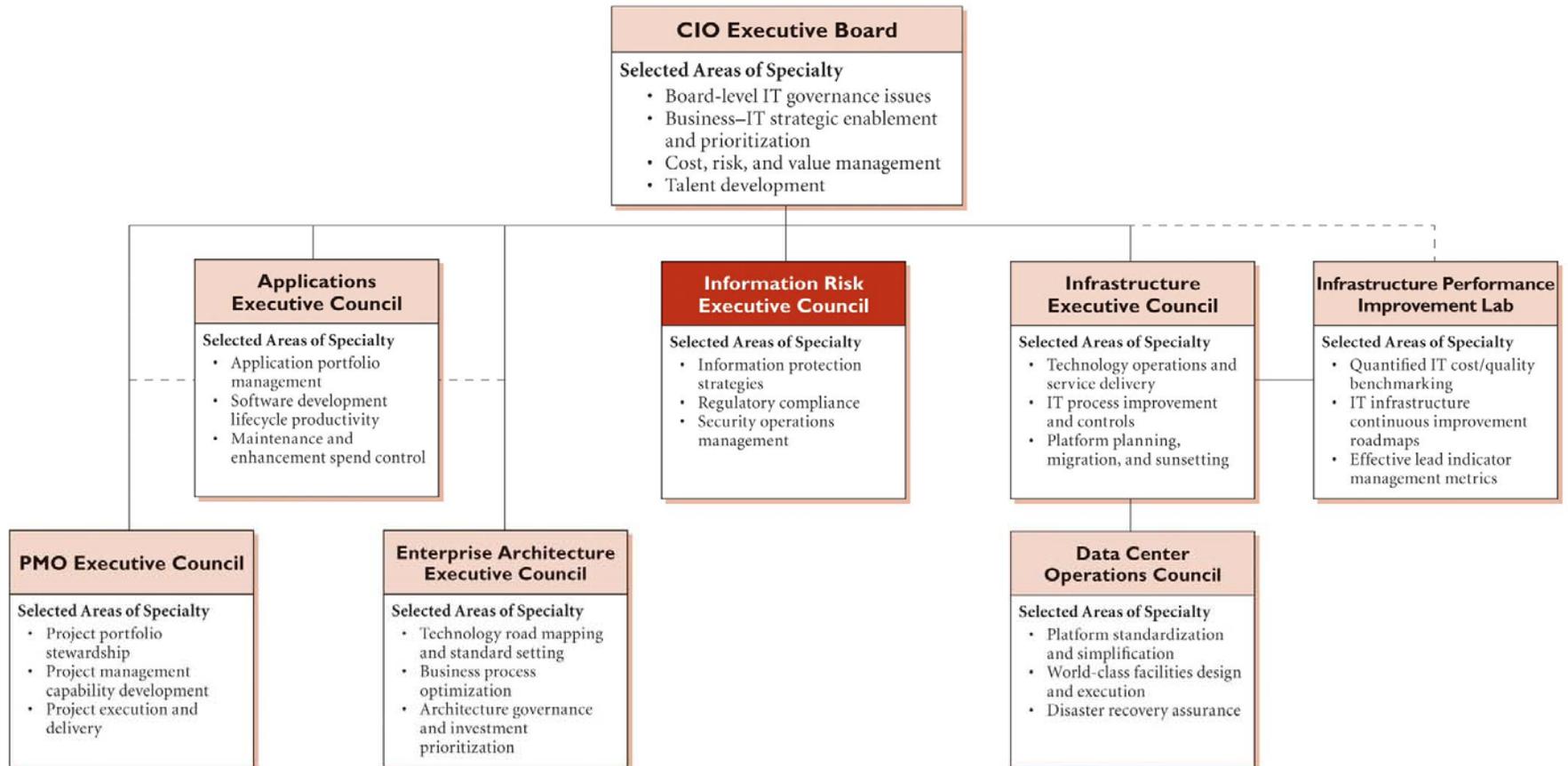
Members Choose Programs According to Their Needs

We invite members to opt-in to individual programs according to their specific needs and to assess the returns on their financial contribution for each membership; members prefer this approach to incorporating all of our service enhancements into one membership and raising the overall price.

Programs Receive Dedicated and Incremental Resources

Each new program we introduce represents an enlargement of our issue coverage and an added richness to the resources available to members; when urgent challenges are shared across functions, we will undertake independent inquiries and generate practices, data, and tools tailored to the needs and perspectives of each constituency.

Programs Within the Practice



IN SERVICE TO IT

Benefits to Participation Across Multiple Programs

Leadership Alignment at All Levels of IT

A common platform drives more effective leadership development and alignment of CIO strategic objectives with functional agendas.

- Increased integration and coordination across IT functions
- Developing business-skilled IT strategic objectives and functional agendas
- Faster, better decisions—staff have access to objective data and analysis
- Enhanced ability to communicate value that individual functions provide to the business

Execution Support Across the Full Lifecycle of Major Initiatives

While powerful individually, when deployed in tandem the collective resources of the IT practice ensure that high-priority member initiatives are supported by objective decision support at each stage.

Example: Enterprise Resource Planning (ERP)

- Architecting for business requirements
- Optimizing business processes
- Bullet-proofing global rollout
- Managing performance post-go-live
- Accelerating benefits capture

Integrated Relationship Management Approach

The responsibility for ensuring that member returns exceed their membership investments is a key KPI for our staff.

- *Tailored Service Plan*—This plan serves as our internal compass, documenting key objectives for our member companies.
- *Utilization Tracking*—We are pleased to provide team utilization reports to each of our members at any level of frequency.
- *Membership Commitment*—Each membership comes with an unequivocal satisfaction guarantee.

ACCELERATING RESPONSIVENESS OF THE IT FUNCTION

“I note that my direct reports are benefiting from the quality of advice and resources that are constituency-specific and empower them to drive their functional priorities. It has distinctly improved the overall capabilities of our IT team and enabled us to effectively plan and respond to shifts in business priorities.”

Chief Information Officer
Diversified Manufacturing

CHALLENGES OUR MEMBERS CURRENTLY FACE

Which of These Are Priority Issues for You?

Strategy and Governance

Representative Challenges

Strategic Planning

Developing a three-year strategic plan

Cross-Functional Alignment

Understanding priorities of key stakeholders

Organizational Design

Creating roles and responsibilities for effective information risk governance

Security Policy Management

Representative Challenges

Policy Design

Creating a standards-based security policy framework

Awareness and Training

Instilling secure behavior in end users

Monitoring

Monitoring compliance with security policies

Regulatory Compliance

Representative Challenges

Compliance Roadmap

Creating a unified view of regulatory compliance requirements

Data Privacy

Developing pragmatic strategies for protecting personally identifiable information

Audit Support

Educating and coordinating with the Audit function

Architecture and Technology

Representative Challenges

Identity Management

Implementing a business-appropriate identity management strategy

Perimeter Design

Creating a network security blueprint for the extended enterprise

Information Protection Technologies

Leveraging technology controls to protect sensitive intellectual property

Security Process Management

Representative Challenges

Security Operations

Improving the efficiency of security operations

Third-Party Risk Management

Assessing information risks associated with offshoring relationships

Application Security

Embedding security in the applications development lifecycle

Measurement and Reporting

Representative Challenges

Risk Assessment

Developing a comprehensive risk assessment framework

Maturity Benchmarking

Measuring organizational maturity and effectiveness

Performance Communication

Designing the Information Risk scorecard

MEMBERS USE OUR RESOURCES TO SOLVE SHARED CHALLENGES

Sample Research, Data, and Tools We've Recently Created

✓ Strategy and Governance

-  *Key Developments in the Information Risk Function*
-  Emerging Information Risk Organizational Models
-  Information Risk Budget and Spend Benchmarks
-  *From Enforcer to Collaborator*
-  *Cross-Functional Perspectives on Risk Across the Enterprise*

✓ Security Policy Management

-  Policy Resource Center
-  Compendium of Information Security Policies
-  *Inflecting End-User Awareness*
-  Awareness and Training Resource Center
-  Event-Log Correlation Tools

✓ Regulatory Compliance

-  *Strategies for Ongoing Regulatory Compliance*
-  Pragmatic Data Classification Strategies
-  Data Privacy Resource Center
-  PCI: A Practitioner's Primer
-  Strategies for Data Retention and Records Management

✓ Architecture and Technology

-  Identity Management Implementation Toolkit
-  Security Project Implementation Guide: Digital Rights Management
-  Security Project Implementation Guide: Laptop Encryption
-  Technology-Driven Controls: Leakage Protection
-  Vendor Knowledge Exchange

✓ Security Process Management

-  *Scaling Third-Party Risk Management*
-  Building Security into the SDLC
-  Security Incident Response Management
-  Selective Outsourcing of Information Security
-  Security Patch Management

✓ Measurement and Reporting

-  Risk Assessment Resource Center
-  Drivers of CISO Effectiveness
-  Information Risk Scorecard Builder
-  Compendium of Information Risk Scorecards
-  Key Attributes of Information Risk Management: Competency Diagnostic

YOUR ACCOUNT MANAGEMENT TEAM GUIDES YOU TO A WEALTH OF RESOURCES

OUR MEMBERSHIP PROPOSITION

- All-inclusive for one annual contribution
- Supported by an account management team
- Backed by a service guarantee

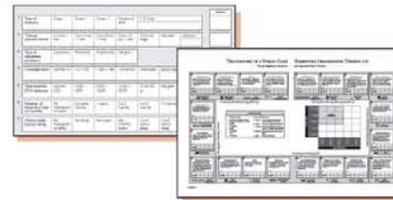
Research and Analysis

Identify Best Practices



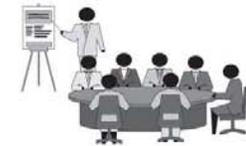
Benchmarking Data and Diagnostic Tools

Prioritize Investments



Execution Support

Save Time on Execution



OUR RELATIONSHIP MANAGEMENT APPROACH

- Installation call to develop a working partnership for the coming year
- Engagement call to key staff to stimulate immediate use of services
- Account management team to map your priorities to Council resources to drive value
- Regular check-in and future-year planning to reprioritize support

Best Demonstrated Practices

Exportable strategies and tactics from leading companies for overcoming major strategic challenges

Research Briefs

Synopses of key findings from primary or secondary research on emerging issues or specific tactical challenges

Vendor Knowledge Exchange

Unbiased peer-tested reviews and direct networking on technologies to assist in technology investment decisions

Budget and Organization Benchmarking

Detailed data on information risk management organizational models, governance structures, and resource allocation

CISO Effectiveness Benchmarking

Annual survey and quantitative analysis providing actionable insight into key management drivers of CISO effectiveness

Competency Diagnostic

Customized online exercise for calibrating expectations for information risk management against a world-class standard

Project Acceleration Toolkits

Online repositories of actionable, member-submitted tools and templates to assist in execution across all stages of the security project lifecycle

Security Project Implementation Guides

Terrain overviews, lessons learned, and detailed implementation tips on high-impact technology projects, featuring interviews with leading practitioners

Facilitated Networking

Ad hoc networking conversations or discussion groups based on shared implementation challenges

MULTIPLE CHANNELS MAKE IT EASY FOR YOU TO ENGAGE WITH THE MEMBER NETWORK

Senior Executive Engagement

Frame Thought and Stimulate Ideas



Annual Executive Retreats

Highly interactive meetings restricted to the seniormost information risk executive

Member-Hosted Forums

Highly interactive meetings hosted by a member for seniormost executives on a topic of particular interest

Executive Networking

Prewired introductions among members and executives at other organizations who possess relevant expertise or shared challenges

Meetings and Events for Key Staff

Develop New Skills



Staff Briefings

Broad gatherings designed to expose direct reports and high-potential staff to ideas and practices presented in seniormost forums

Practitioner Teleconferences

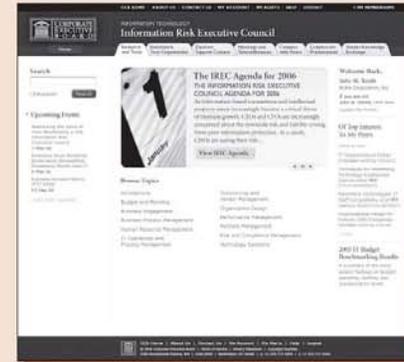
Succinct overviews of Council research, facilitated by member-practitioners, with the opportunity for attendees to ask questions and discuss implementation details

Emerging Issue Cohorts

Issue-based teleconferences and meetings, facilitated by the Council, revolving around critical, time-sensitive issues facing information risk executives across multiple industries

Members-Only Online Resources

Discover Proven Solutions Powered by Your Peers



Research and Tools

Browse or search for all best practices provided by the Information Risk Executive Council.

Benchmark Your Organization

Participate in Council surveys and diagnostics, benchmark your organization against others, and view aggregate results.

Decision Support Centers

Access all research, tools, and templates on a specific topic area.

Meetings and Teleconferences

View all executive and team events, register for a retreat or teleconference, and recommend events to your coworkers.

Connect with Peers

Network with peers at other organizations on a specific issue or challenge via our online listserv technology.

Graphics for Presentations

Reuse Council graphics available in a convenient PowerPoint format for your own internal presentations.

www.irec.executiveboard.com

THE BUSINESS CASE FOR MEMBERSHIP

Boosting IT Performance More Efficiently and Cost-Effectively

A Proven Model for Creating Value

Saves You Money

- All-inclusive, for one annual contribution
- Shared cost with hundreds of peer members
- Backed by a service guarantee

High-Quality Insight, Actionable Data, and Peer-Tested Tools and Tactics

Saves You Time and Reduces Risk

- Avoid rework and duplication of efforts
- Learn from peer successes and failures
- Test internal assumptions

A Dedicated Relationship Management Team

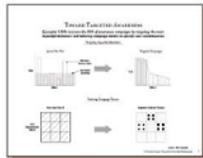
Ensures That You Maximize ROI

- Stimulates engagement of key staff
- Maps our research to your priorities
- Shoulders responsibility for value creation

How We Will Support Your Next Priority

Case in Point: Identity Management

Project Planning



Build the Business Case

IREC Identity Management ROI Calculator and Business Case Builder

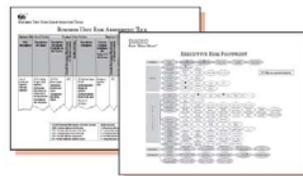
Define Scope and Sequence

Diagnostics to Decide Ideal Scope and Sequence

Avoid Reinventing the Wheel

Sample Business Requirements Documents from Peer Companies

Execution



Identify Best Practices

For Example, a Member Case Profile Illustrating a Frame-Breaking Approach to Role Definition

Leverage Implementation Toolkits

Compendium of Tools and Templates Shared by Members

Select Vendor(s)

Vendor Experience Database Featuring Unbiased Peer Opinions

Ongoing Support



Measure Performance

Metrics Scorecards and Performance Benchmarking

Make Course Corrections

Peer Feedback at Annual Executive Retreats

Return on Investment

- Minimize consulting fees and prevent overinvestment.
- Reduce rework caused by poor project scope and process definition.
- Negotiate better deals and hire the right vendors.
- Save staff time in creating better tools and templates.
- Avoid cost of third-party benchmarking and improve cost transparency.

OUR MAJOR INITIATIVES FOR 2007

The Context: Spurred by high-profile incidents and regulatory demands, security budgets saw approximately 10% increases across the past two years. This “honeymoon” is likely to end in 2007, with economic uncertainty and rising expectations of organizational maturity leading CFOs and CIOs to demand greater execution discipline from Information Risk.

The Imperative: Information risk organizations’ inability to articulate risks in business terms has hindered their ability to help the business make informed choices on risk mitigation. This has led to security being perceived as an obstacle to business execution, and has also impacted Information Risk’s ability to allocate investments optimally to drive better risk mitigation outcomes. Leading companies are therefore seeking, first, *a business-focused approach to risk prioritization*, and second, *an integrated, process-driven approach to risk mitigation*.

Council Value: The Council will help members by providing ready-to-use frameworks, tools, and templates shared by leading practitioners, thus *reducing consulting spend*, as well as providing best practices to streamline the project portfolio, tighten project scope, and avoid costly implementation errors, thus *reducing operational expenses*.

Reconfiguring Security for Business Enablement

- I. Articulating Security’s Value Proposition**
 - Quantifying risk exposure by tying risks to business value chains
 - Developing consistent risk assessment frameworks to ensure business buy-in
 - Planning security work programs based on enterprise/IT strategy

- II. Evaluating the Business Benefits of Converged Risk Management**
 - Integrating information risk “vertically” into enterprise-wide risk management efforts
 - Converging “horizontally” with adjacent risk groups to capture operational efficiencies

- ∞ **Member Impact**
 - Risk Evaluation Toolkit (process maps, valuation calculators, prioritization tools)
 - Risk Stakeholder Calibration Diagnostic
 - Information Risk ERM Integration Plan
 - Benefits Calculator for “Converged” Risk Management

Building an Integrated Information Protection Strategy

- III. Optimizing the Information Protection Solutions Portfolio**
 - Rationalizing security spending by coordinating investments across people, process, and technology dimensions
 - Encouraging secure behavior by weaving security into user workflows
 - Using transparent controls to secure mobile and auxiliary devices

- IV. Targeted Strategies for Closed-Loop Policy Enforcement**
 - Streamlining control requirements to facilitate policy compliance
 - Translating automated monitoring data into insight through correlation tools
 - Minimizing losses by developing cross-functional incident response protocols

- ∞ **Member Impact**
 - Employee Awareness Baselining Service
 - Security Project Portfolio Optimizer
 - Emerging Security Technology Watch
 - Automated Monitoring Deployment Blueprint

Other Initiatives Under Consideration

- | | | | |
|--|---|---|---|
| <ul style="list-style-type: none"> • Identity Management Implementation Toolkit | <ul style="list-style-type: none"> • Application Security Best Practices | <ul style="list-style-type: none"> • Global Regulatory Landscape Watch | <ul style="list-style-type: none"> • CISO Effectiveness Benchmarking Service |
|--|---|---|---|

2007 TIMELINE OF MEMBER EVENTS AND RESEARCH INITIATIVES

First Quarter 2007

-  **Online Resource Center**
Identity Management Implementation Toolkit
January
-  **Teleconference**
Key Enterprise Priorities for 2007: Review of Agenda
Survey Results
16 January
-  **Teleconference**
Key Developments in Information Risk: A Briefing for Heads
of Infrastructure
18 January
-  **Online Resource Center**
Compendium of Information Risk Organizational Structures
February
-  **Annual Executive Retreat**
Engaging the Enterprise
6 February, Washington, D.C.
-  **Teleconference**
Drivers of CISO Effectiveness
20 February
-  **Project Implementation Guide**
Managing Intrusion Prevention Systems
March
-  **Strategic Research**
Boosting CISO Personal Effectiveness
March
-  **Teleconference**
Identity Management: Principled Vendor Selection Strategies
20 March

Second Quarter 2007

-  **Implementation Tool**
Global Regulatory Landscape Watch
April
-  **Member-Hosted Forum**
Intellectual Property Protection
3 April, Motorola, Inc., Chicago
-  **Teleconference**
Business Workflow Risk Assessments
17 April
-  **Teleconference**
Maximizing Membership Value: Overview of Council Resources
24 April
-  **Project Implementation Guide**
Two-Factor Authentication Implementation and Management
May
-  **Strategic Research**
Business-Driven Risk Mitigation
May
-  **Teleconference**
Identity Management: Pragmatic Approaches
to Roles-Based Access
15 May
-  **Annual Executive Retreat**
2007 Meeting Series
14–15 June, Washington, D.C.
-  **Teleconference**
Third-Party Risk Assessments
19 June

THE COUNCIL IN ACTION

Helping EMC Design and Implement an Exception Handling Process

EMC²

- **Background:** EMC is a leading provider of computer storage technologies based in Hopkinton, Massachusetts. In 2005, EMC generated revenue of approximately US\$10 billion and employed more than 26,000 individuals.
- **Situation:** EMC finds that business unit compliance with policies mandating the mitigation of significant risks is lower than desired. Due to a widespread perception that the processes are not only burdensome, but also are designed without regard to imposed cost, business units often fail to comply, leading to unacceptably high risk exposure and/or friction with the security group.

From Insight to Impact

Council Analysis



- IREC Annual Executive Retreat presents best practices in eliciting cooperation from business stakeholders.
- Teradyne's approach to exception handling shows how business and security concerns can be reconciled through formal negotiation and escalation procedures.
- EMC's Director of Global Security implements the Teradyne exception handling approach using presentation materials and ideas surfaced during peer discussion.

Result

Exception Requests Denied Upon Review



EMC's new exception handling process results in significantly improved business engagement, as evidenced by the decrease in the number of exception requests denied after appropriate review and escalation.

FROM INSIGHT TO ACTION

“While I had long recognized the need for a more business-friendly approach to risk mitigation, the Teradyne case study and ensuing discussion helped crystallize the issue for me. The soundness and actionability of the profiled approach made implementation such a no-brainer that I e-mailed my team during the meeting itself, asking them to start work on it right away.”

Roland Cloutier
Director of Global Security

IMPACT ACROSS THE NETWORK

Members Share How the Network Has Created Value for Them

CHARTING A COURSE FOR THE FUTURE



“The field of information risk management is undergoing a dramatic transformation and IREC, for want of a better phrase, ‘gets it.’ Their research does a good job of articulating the challenges inherent in this transformation and suggesting promising approaches. In particular, IREC’s innovative quantitative work on the drivers of CISO effectiveness provided me with much food for thought—and action.”

Bill Boni
Corporate Information Security Officer

UNMATCHED PEER LEARNING



“The Annual Executive Retreat I attended was an excellent use of my time. The topics were perfectly aligned with my strategic agenda. The presentations and peer discussions validated key elements of my approach to information risk management while providing an abundance of fruitful ideas for the future. I look forward to working with IREC as I put some of these ideas into practice.”

Jaap Halfweg
Chief Information Security Officer

NOT REINVENTING THE WHEEL



“Needing to quickly build out our secure software development policies, I reached out to my account director at the Council, who shared with me an applications security policy template originally developed by another member company. I used this template as the basis for our own policy, and needless to say, it saved me a ton of time and effort. As a firm believer in not reinventing the wheel, I shared my version of the document with the Council so that others could benefit in turn from my efforts.”

Steve Christensen
Global Director of Information Security

INFORMATION RISK EXECUTIVE COUNCIL

Washington, D.C. • London • New Delhi

www.irec.executiveboard.com

Dallas/Fort Worth International Airport • Danish Crown AmbA • Danske Bank A/S • David Jones Ltd. • Dawn Food Products, Inc. • Deere & Company • Del Monte Foods Company • Denny's, Inc. • Denso International America, Inc. • Desjardins Group • Deutsche Post AG • Dex Media, Inc. • DHL Holdings (USA), Inc. • Diageo plc • The Diamond Trading Company • Dick's Sporting Goods, Inc. • Diebold, Inc. • Discovery Communications, Inc. • Dollar Tree Stores, Inc. • Dominion Resources, Inc. • Domino's Pizza, Inc. • Dover Electronics, Inc. • The Dow Chemical Company • Dow Corning Corporation • Dow Jones & Company, Inc. • DreamWorks SKG • Dreyer's Grand Ice Cream Holdings, Inc. • Duchossois Industries, Inc. • Dunkin' Brands, Inc. • Dynege, Inc. • Eastman Kodak Company • eBay, Inc. • Eddie Bauer Holdings, Inc. • Edison International • Educational Testing Service • Electrolabel S.A. • Electronic Arts, Inc. • Eli Lilly and Company • El Paso Corporation • Emap Plc • EMCOR Group, Inc. • Emerson Electric Co. • EMI Group plc • Energen Corporation • EnergyAustralia • ENMAX Corporation • ENSCO International, Inc. • Enterprise Ireland • Ernst & Young • ESPN, Inc. • E*TRADE Financial Corp. • Expedia, Inc. • Exxon Mobil Corporation • Fairmont Hotels & Resorts, Inc. • Fannie Mae • Federal Aviation Administration • FedEx Corporation • F5 Networks, Inc. • Finland Post Group • First Charter • FirstGroup plc • First Niagara Financial Group, Inc. • Fisher-Price, Inc. • Flowers Foods, Inc. • Ford Motor Company • Franklin Covey Co. • Freddie Mac • Fremont General Corporation • Frito-Lay, Inc. • Fromageries Bel S.A. • Fuji Photo Film U.S.A., Inc. • Gallaher Group Plc • Gambro Renal Products • GE Energy • GEICO • Genentech, Inc. • General Mills, Inc. • General Motors Corporation • Getronics • Getty Images, Inc. • Girl Scouts of the United States of America • GlaxoSmithKline plc • Global Knowledge Training LLC • GN ReSound • Goodrich Corporation • Goodwill Industries International, Inc. • Graham Packaging Company, LP • Granite Construction, Inc. • Grant Prideco, Inc. • Grant Thornton LLP • Great Plains Energy, Inc. • Greif, Inc. • GroupM • Grundfos Management A/S • Grupo Televisa, S.A. • Grupo Uralita • Guardian Industries Corp. • Halliburton • Hallmark Cards, Inc. • H & R Block, Inc. • Hannaford Bros. Co. • Hanson PLC • Harrah's Entertainment, Inc. • Harri Teeter, Inc. • Harsco Corporation • Hawaiian Electric Company, Inc. • HealthMarkets • Heineken N.V. • Hennepin County, Minnesota • Hercules, Inc. • Hershey Foods Corporation • Hess Corporation • Hibernian Group • Hilton Hotel Corporation • H.J. Heinz Company Ltd. • Honeywell International, Inc. • Horizon Lines, Inc. • Houghton Mifflin Company • HP Hood LLC • HSBC Bank Australia Ltd. • Hubbell, Inc. • Humana, Inc. • Huntsman Corporation • ICMA Retirement Corporation • IDACORP, Inc. • InBev NV/SA • Indigo Books & Music, Inc. • ING Direct • Ingersoll-Rand Company Ltd. • Integral Energy Australia • Inter IKEA Systems B.V. • Intermetics General Corporation • International Paper Company • Interstate Bakeries Corporation • Intuit, Inc. • Invensys plc • IPSCO, Inc. • Itron, Inc. • Jabil Circuit, Inc. • Jackson National Life Insurance Company • Jafrá Cosmetics International • Jardine Matheson Holdings Ltd. • J. Crew Group, Inc. • Johnson & Johnson • John Wiley & Sons, Inc. • The Jones Financial Companies, L.L.L.P. • Jostens, Inc. • JPMorgan Chase & Co. • JT International S.A. • Kaiser Permanente • KB Toys, Inc. • Keane, Inc. • Kellogg Company • KeySpan Corporation • Kirkland & Ellis LLP • Knight Ridder, Inc. • Kohler Co. • Kohl's Corporation • Komerční banka, a.s. • Koninklijke Philips Electronics N.V. • Kraft Foods, Inc. • Labatt Brewing Company Ltd. • Lafarge S.A. • Land O'Lakes, Inc. • La Poste • LaSalle Bank • LeapFrog Enterprises, Inc. •



CORPORATE EXECUTIVE BOARD
 Washington, D.C. • London • New Delhi
www.irec.executiveboard.com
 IREC16KXIIIL

Legg Mason, Inc. • Lehman Brothers, Inc. • Level 3 Communications, Inc. • Levi Strauss & Company • LexisNexis Group • Liberty Media Corporation • Lion Nathan Ltd. • Lockheed Martin Corporation • Lonmin Plc • L'Oreal SA • Lowe's Companies Inc. • Lyondell Chemical Company • Malt-O-Meal Company • M&T Bank Corporation • Man Group plc • Manpower, Inc. • Maple Leaf Foods, Inc. • Markel Corporation • Marks & Spencer Group p.l.c. • Marriott International, Inc. • Marsh, Inc. • Mars, Inc. • Mary Kay, Inc. • Mattel, Inc. • Mayo Foundation for Medical Education and Research • MBI, Inc. • MBNA America Bank • McDermott International, Inc. • McDonald's Corporation • The McGraw-Hill Companies, Inc. • McKee Foods Corp. • McKesson Corporation • McKinsey & Company • MDS Pharma Services • MeadWestvaco Corporation • Mentor Graphics Corporation • Merck & Co., Inc. • Mervyns LLC • METRO AG • Metso Corporation • Michelin Group • MidFirst Bank • Millennium Pharmaceuticals, Inc. • Miller Brewing Company • Millipore Corporation • Misy's plc • Mittal Steel Company N.V. • Mobistar S.A. • Momentum Life • Morgan Stanley • Morton's Restaurant Group, Inc. • MTV Networks • Mueller Industries, Inc. • The Murugappa Group • Musgrave Ltd. • National Basketball Association • National Football League, Inc. • Nationwide Mutual Insurance Company • Navy Federal Credit Union • NEC Corporation • Nestlé Purina PetCare Company • New Balance Athletic Shoe, Inc. • The New York Times Company • NIBC N.V. • NIKE, Inc. • Nintendo of America, Inc. • Nissan North America, Inc. • Nokia Corporation • Norsk Hydro ASA • Nortel Networks Corporation • Northrop Grumman Corporation • Northwest Airlines, Inc. • Northwestern Mutual • Novartis AG • Novation, LLC • NSTAR • NTL Group Ltd. • Nutreco Holding N.V. • Oakley, Inc. • Oakwood Worldwide • O'Charley's, Inc. • OfficeMax, Inc. • Ohio Savings Bank • Old National Bancorp • Omnicom Group, Inc. • Omni Hotels Corporation • OneSteel Ltd. • Orkla ASA • Owens & Minor, Inc. • Owens Corning • Pacer International, Inc. • Pacific Gas and Electric Company • PacifiCorp • Panasonic Corporation of North America • Panda Restaurant Group, Inc. • P&H Mining Equipment, Inc. • Parex banka • Parmalat Canada Ltd. • Payless ShoeSource, Inc. • Pegasus Solutions, Inc. • Penske Truck Leasing • PepsiAmericas, Inc. • The Pepsi Bottling Group, Inc. • Perdue • Petco Animal Supplies, Inc. • Petróleos de Venezuela S.A. • PETSMART, Inc. • P.F. Chang's China Bistro, Inc. • Pfizer, Inc. • PG&E Corporation • The Philadelphia Gas Works • Philip Morris International, Inc. • Piggly Wiggly Carolina Co. • Pitney Bowes, Inc. • Plum Creek Timber Company, Inc. • Polo Ralph Lauren Corporation • Posten Norge As • PricewaterhouseCoopers • The Procter & Gamble Company • Progressive Casualty Insurance Company • Prudential plc • Publix Super Markets, Inc. • Purolator Courier Ltd. • Qantas Airways Ltd. • QUALCOMM, Inc. • QVC, Inc. • RadioShack Corporation • Random House, Inc. • REI/Recreational Equipment, Inc. • Rent-A-Center, Inc. • Reyes Holdings, L.L.C. • R-G Financial Corporation • Rinker Group Ltd. • Rio Tinto plc • Riverside National Bank of Florida • Rockland Trust Company • Rockwell Collins, Inc. • Rohm and Haas Company • Rolls-Royce plc • Rosetta Resources, Inc. • Royal Mail Group plc • R.R. Donnelley & Sons Company • Rush Enterprises, Inc. • Ryder System, Inc. • Safeco Corporation • Safety-Kleen Holdco, Inc. • Salzgitter AG • Samsonite Corporation • San Diego Gas & Electric Company • Santee Cooper • Sara Lee Food & Beverage • Scandinavian Airlines System • Schering-Plough Corporation • Scholastic, Inc. • Schwarz Pharma AG • Scotiabank • Scottish Power plc • Scottrade, Inc. • Sealed Air Corporation • Sears Holdings Corporation • Sempra Energy • Sequa Corporation • Serologicals Corporation • 7-Eleven, Inc. • Severn Trent Water Ltd. • Shell International BV • The Sherwin-Williams Company • Shire plc • Shoppers Drug Mart, Inc. • Siemens AG • SigmaTel, Inc. • Sikorsky Aircraft Corporation • Silgan Holdings, Inc. • Simon Fraser University • SingTel Optus Pty Ltd. • Skanska AB • SkyWest, Inc. • SLM Corporation • Smith Barney's Private Client Group • Smithfield Foods, Inc. • Social Security Administration • Société Générale • Solo Cup Company • Solvay S.A. • Sony Electronics, Inc. • South African Airways (Proprietary) Ltd. • Sovereign Bancorp, Inc. • SPARTA, Inc. • Spectris plc • SPL WorldGroup, Inc. • The Sports Authority, Inc. • SSA Global Technologies, Inc. • Standard Motor Products, Inc. • Staples, Inc. • Starbuck's Corporation • Starz Entertainment, LLC • Sterling Chemicals, Inc. • St. Jude Medical, Inc. • St. Luke's Episcopal Health System • Sulzer Ltd. • Suncor Energy, Inc. • Sun Life Financial, Inc. • Sunoco, Inc. • SVB Financial Group • Swedbank AB • Swift Newspapers, Inc. • Swisscom AG • Symantec Corporation • Syngenta AG • Tata Group • Taylor Nelson Sofres plc • TD Waterhouse Canada, Inc. • Teekay Shipping Corporation • Tektronix, Inc. • Telcordia Technologies, Inc. • Telenor ASA • TellaSonera AB • Telstra Corporation Ltd. • Tennessee Valley Authority • Terra Industries, Inc. • Tesco PLC • Tetra Tech, Inc. • Texas Instruments, Inc. • Thomas & Betts Corporation • 3Com Corporation • TIAA-CREF • Tiffany & Co. • The Timken Company • Time Warner, Inc. • TiVo, Inc. • T-Mobile International AG & Co. KG • TNT N.V. • Tommy Hilfifer Corporation • TomTom International B.V. • Toronto Stock Exchange • TransUnion LLC • TransCanada Pipelines Ltd. • Transportation Security Administration • Tribune Company • Trinity Health • TriQuint Semiconductor, Inc. • Truilent Federal Credit Union • Tupperware Worldwide • Türkiye Garanti Bankası, A.S. • Tyco International Ltd. • Tyson Foods, Inc. • UAP Holding Corp. • UGS Corp. • UNICEF • United Nations • United Parcel Service, Inc. • United States Postal Service • Unitrin, Inc. • Universal Studios • UnumProvident Corporation • UPM-Kymmene Corporation • USA TODAY • U.S. Cellular • Vail Resorts, Inc. • Valassis Communications, Inc. • Vattenfall AB • Veolia Environnement • Verizon Communications, Inc. • Verizon Wireless • Verco • Viacom, Inc. • Virgin Mobile Telecoms Ltd. • Visa USA • Vodafone Group Plc • Volkswagen Financial Services (UK) Ltd. • Vulcan Materials Company • VWR International • Wachovia Corporation • Wal-Mart Stores, Inc. • Wartsilä • The Washington Post Company • Wawa, Inc. • WCI Communities, Inc. • Weight Watchers International, Inc. • WellCare • Wellmark Blue Cross and Blue Shield • Wells' Dairy, Inc. • Wendy's International, Inc. • Westfield Group Australia • WestLB AG • Whirlpool Corporation • White Castle System, Inc. • Wild Oats Markets, Inc. • Winterthur-Versicherungen • Winn-Dixie Stores Inc. • Wisconsin Energy Corporation • Wm. Wrigley Jr. Company • Wolverine World Wide, Inc. • Woolworths Pty. Ltd. • World Bank Group • Worthington Industries, Inc. • W.W. Grainger, Inc. • Xerox Corporation • XM Satellite Radio • Yahoo!, Inc. • The Yankee Candle Company, Inc. • Yapi ve Kredi Bankasi A.S. • Yorkshire Building Society • Yum! Brands, Inc. • Zebra Technologies Corporation • Zimmer Holdings, Inc. • Zions Bancorporation • ZLB Behring L.L.C. • Zürcher Kantonalbank



IREC Summary

- Cost: \$20,000
- Includes access for all state employees
- <https://www.irec.executiveboard.com/Public/Register.aspx>
- If you have problems contact:
 - Jason Dolan
 - (202) 587-3626
- Respond to let us know if you are or are not interested by January 30, to: VITASecurityServices@VITA.VIRGINIA.GOV

If you have questions call Cathie Brown at (804) 786-2467



Virginia Information Technologies Agency

Other Business





IT Security Audit Standard

1. Does it cover standalone systems/databases?
YES if it contains sensitive data
2. Should Internal Audit or IT staff develop the IT Security audit plan?
Either as the agency sees fit. VITA is having Internal Audit prepare the plan.
3. My agency already has audits conducted of every sensitive system. Do we have to have additional audits?
No. Simply submit your IT Security Audit Plan.



IT Security Audit Standard

4. My agency cannot have the plan submitted by Feb. 1 because..... What do I do?

The Agency should submit an except request stating why & when it will be done (Form on-line).

5. My agency completed IS templates for VITA identifying 35 systems as being sensitive with unique security requirements but I only have 5 sensitive systems on my IT Security Audit Plan. What should I do?

Provide an explanation to VITA of the discrepancy or only the systems on the IT Security audit plan will be considered as needing unique security controls.



UPCOMING EVENTS!

ISOAG MEETING DATES

Thursday, February 15, 2007 9:00 -12:00

Tentative Agenda

Encryption Solution Ordering Specifics

SJR 51 Action Plan

VITA COOP/IT DR

MOAT (Security Awareness)

Information Security Assurance Plan

IT Legislation

Thursday, March 22, 2007 1:00 - 4:00

Agenda TBD



Upcoming Events

Virginia Digital Government Summit

March 15, 2007 Richmond Marriott

<http://www.govtech.net/events/index.php/VirginiaDGS2007>



ADJOURN

**THANK YOU FOR
YOUR TIME AND
THOUGHTS**

!!!