



Commonwealth Information Security Advisory Group (ISOAG) Meeting

October 31, 2006

expect the best



ISOAG October 2006 Agenda

- | | |
|--|--|
| I. Welcome | Peggy Ward, VITA |
| II. Partnership Update | Fred Duball, VITA |
| III. Standard Infrastructure Practices | Fred Duball, VITA |
| IV. Security Initiatives | Linda Smith, VITA/NG
Stephen King, VTIA/NG
Jason Sewell, VITA/NG |
| V. ITIL Overview | David Turner, VITA/NG |
| VI. Risk Management Guideline | Cathie Brown, VITA |
| VII. Other Business | Peggy Ward, VITA |



Virginia Information Technologies Agency



Welcome!!!

**National Cyber Security Awareness Month
October 2006**



IMPORTANT CHANGE TO THE VIRGINIA PUBLIC RECORDS ACT, 2006

Reference: Code of Virginia, §42.1-86.1 (A), effective July 1, 2006; §18.2-186.3

Applies to: Disposition of public records created after July 1, 2006 by state agencies, localities and political subdivisions

Discussion: Changes made during the 2006 regular session amended the Virginia Public Records Act (VPRA) through Senate Bill 461. The text below was added to §42.1-86.1, Disposition of public records:

B. Each agency shall ensure that records created after July 1, 2006 and authorized to be destroyed or discarded in accordance with subsection A, are destroyed or discarded in a timely manner in accordance with the provisions of this chapter; provided, however, such records that contain identifying information as defined in clauses (iii) through (ix), or clause (xii) of subsection C of §18.2-186.3 shall be destroyed within six months of the expiration of the records retention period.

expect the best



Partnership Update

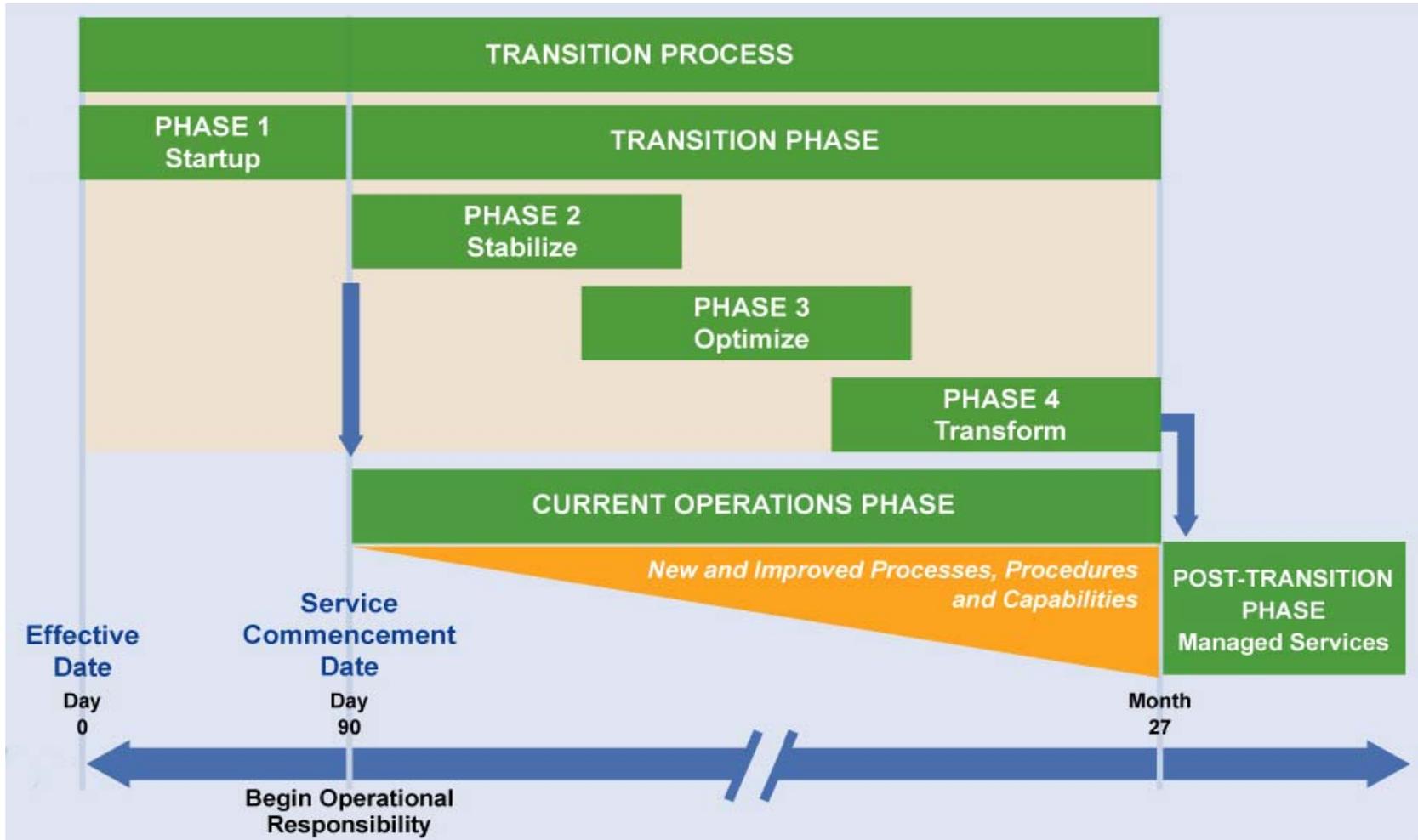
Fred Duball, VITA

October 31, 2006



NORTHROP GRUMMAN

The IT Infrastructure Partnership Program is a multi-year, multi-phase effort to stabilize, optimize and transform the people, processes and technologies for IT infrastructure services that support citizen services



Stabilize

- Completed

- Established the Operations Working Group
- Built Root Cause Analysis (RCA) process, completed 28 RCAs
- Bolstered operations organization with project, communications, and change management personnel
- Held four in-scope manager Q&A calls
- Disseminated and implemented 10 standard infrastructure practices
- Published Central Operations Quality of Service (QoS) Report
- Started collection of customer agency facing metrics
- Implemented fixes to correct central operations Yellow and Red metrics

- Planned

- 10/16 -11/8 - 10 regional NG new employee training meetings
- 10/31 – Complete evaluation of infrastructure against CIS Configuration Standards
- 11/15 - In-scope manager off-site – management team alignment
- 11/30 – Build process for flowing information on vital service interruptions
- 11/30 - Build Emergency Operations IT support plan
- 12/15 – Include all customer agency facing metrics in the QoS Report
- Early 2007 – Consolidate service support contracts

Transition Challenges

- **Move Operations from primarily distributed/agency-focused model to centrally-focused model**
 - Description
 - Effort now primarily performed in agency buildings and focused on agency support
 - Eventually move help desk, break/fix, server, network, security monitoring, e-mail to the Commonwealth Enterprise Solutions Center (CESC) and the Southwest Enterprise Solutions Center (SWESC) and focus on enterprise support
 - Near-term efforts
 - Moved East and West regions to geographic model, Capital region will move in early 2007
 - Accelerating interim help desk consolidation
 - Accelerating move of customer agencies to interim, existing single e-mail
- **Gain better understanding customer satisfaction at the agency level**
 - Description
 - Currently getting informal, ad hoc comments
 - No overall view of agency satisfaction
 - Near-term efforts
 - Started collection of agency facing metrics, first report December 2006
 - Customer Account Managers (CAMs) providing agency satisfaction assessment
 - Customer agency survey planned for early 2007

Initial, Notional Order for Help Desk and Desktop Transformation

Agency	Secretariat	Number of Sites	Workstation Count (as of 5/10/06)	Cumulative Workstation Count
Veterans Services, Department of	Public Safety	26	106	106
Museum of Natural History, Virginia	NR	1	45	151
Minority Business Enterprise, Department of	C & T	4	27	178
Criminal Justice Services, Department of	Public Safety	2	194	372
Museum of Fine Arts, Virginia	Educ	4	250	622
Correctional Education, Department of	Public Safety	58	2971	3593
Corrections, Department of	Public Safety	115	6984	10577
Juvenile Justice, Department of	Public Safety	142	1509	12086
Game and Inland Fisheries, Dept. of	NR	21	656	12742
Charitable Gaming Commission	Admin	1	55	12797
Forestry, Department of	C & T	74	408	13205
Labor & Industry, Department of	C & T	13	396	13601
Mental Health, Mental Ret. & Sub. Abuse Svcs., Dept. of	HHR	15	4907	18508

IT Infrastructure Services

Domain	Functional Area	September 2006				Post Transform	Coverage Action	Performance Action
		Prior Coverage	Current Coverage	Measures	Performance	SLAs		
End User Services	Help Desk	36%	36%	5		19	1/07 - 37% 4/07 - 42% 7/07 - 47%	Addressed Aug ASA and CAR - Reassigned HD staff to peak hours Red FCR correcting definition
	Messaging	18%	21%	2		10	Nominal increase	
	Desktop	3%	13%	3		14	1/07 - 18% 4/07 - 28% 7/07 - 38%	
Data Center Services	Server	6%	6%	2		21	1/07 - 70%	
	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	60%	100%	1		9	Initial reporting of security incidents	

Central Operations Measures

Service Domain	Measure	MOU-SLO	J	F	M	A	M	J	J	A	S
End User Services	Average Speed to Answer	<30 sec	17	15	13	15	27	32	29	33	22
	Call Abandon Rate	< 5%	6.08%	4.92%	4.53%	5.63%	9.16%	5.41%	6.3%	6.1%	2.1%
	Email Response	<60 mins			17	16	14	15	15	15	16
	Voicemail Response	<30 mins			17	16	14	15	15	15	16
	First Call Resolution*	>70%	12%	14%	14%	18%	23%	21%	20%	20%	21%
	VITA Messaging System Availability	>99.0%	99.99%	99.79%	99.88%	99.79%	100%	99.97%	99.98%	99.99%	100%
	Shared Messaging System Availability	>99.0%	100%	99.98%	99.89%	99.79%	99.99%	99.80%	100%	100%	99.9%
Data Center Services	IBM Mainframe Availability	>99.9%	100%	100%	100%	100%	99.98%	99.95%	100%	99.98%	100%
	Unisys Mainframe Availability	>99.9%	99.95%	100%	100%	100%	100%	100%	100%	100%	99.9%
	UNIX Server Availability	>99%	99.61%	99.69%	99.64%	99.84%	99.95%	99.87%	99.82%	99.82%	99.9%
	Windows Server Availability	>99%	99.79%	99.56%	99.64%	99.84%	99.93%	99.88%	99.83%	99.96%	99.3%
Network	Circuits Availability*	99.2%	99.2%	99.5%	99.2%	99.3%	99.5%	99.40%	99.2%	99.5%	n/a

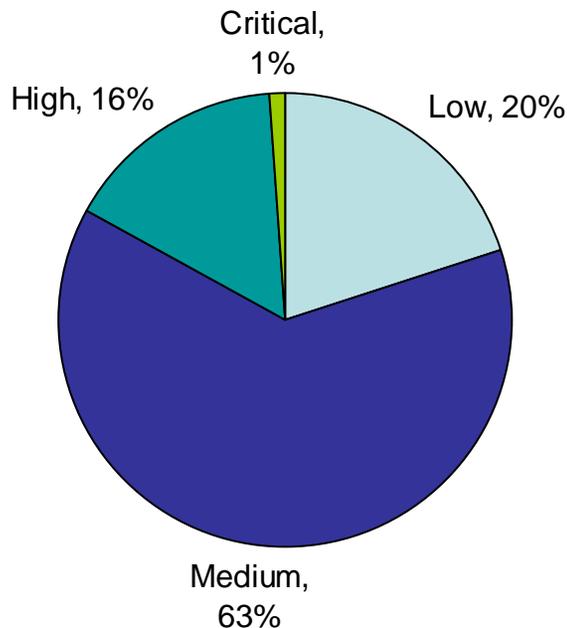
* Current measure assumes all initial calls can be resolved immediately; beginning Oct 06 and per industry standard, basis will consider resolvable versus all calls

Baseline Agency Measures (Sep 06)

Service Domain	Functional Area	Measure	MOU-SLO	DEQ	SBE	DSS	VDH	DMHMRSAS	DGIF	DOE
End User Services	Help Desk	Average Speed to Answer	100%							
		Call Abandonment Rate	5%							
		Email Response rate	100%							
		Voicemail response rate	100%							
		First Call Resolution	70%	44.8%	42.2%			85.2%		
		Average time on-hold	100%							
		Help Desk Password resets	90%	18.0%				100%		
		Service via incident ticket	78%	84.0%	95.2%	62.8%	100%	100%	100%	58.3%
		Service via service request	80%	78.8%		91.4%	100%	88.2%		42.9%
	Incident Repair	80%	85.7%	100%	78.8%	99.7%			87.5%	
	Messaging	Messaging Service Availability	99%	100%	100%	100%	100%	100%	99.9%	100%
Data Center Services	Server	Windows Mission Critical servers	99%	100%		100%	99.0%		100%	
		RISC/Unix Mission Critical servers	99%	100%	100%	100%	99.0%	100%	100%	
		Windows other server	90%	100%	100%	100%	99.0%	100%	100%	
		RISC/Unix other servers	90%	100%	100%	100%	99.0%	100%		
		QA/Test Systems and Servers	90%	100%	100%	100%	97.0%	100%		100%
		Development Servers	90%	100%	100%	100%	95.0%	100%	99.9%	100%
Network Services	Voice	Voice	99.6%	100%	100%	100%	100%	100%		
	Data	Video	99.8%			100%	100%			
		Internet Access	99.8%	99.5%	100%	100%	100%	100%		

Incidents

Distribution of Incident Severity for July - Sept 2006



- Since service commencement:
 - 8,674 total incidents, 74 critical
 - 28 RCAs prepared and corrective action identified
- Significant incidents for period:
 - 7/6, 12 Hours, VDOT: Poorly written script caused all employees to not be able to access applications
 - 7/9, 7 Hours, VDOT: Improper Raid Array configuration caused VDOT website to go down when a drive failed
 - 7/23, 32 Hours, VEC: Improper server restart after maintenance caused the VEC website to go down
 - 7/25, 6 Hours, VDEM: Antivirus software upgrade caused external e-mails to not be passed to VDEM
 - 8/8, DSS, DMV, VRS: A file storage parameter was improperly changed in Jan 06 causing permanent file deletion after 180 days
 - 9/2, 80 Hours, DGIF: Verizon circuit failure caused DGIF website to be unavailable to the public

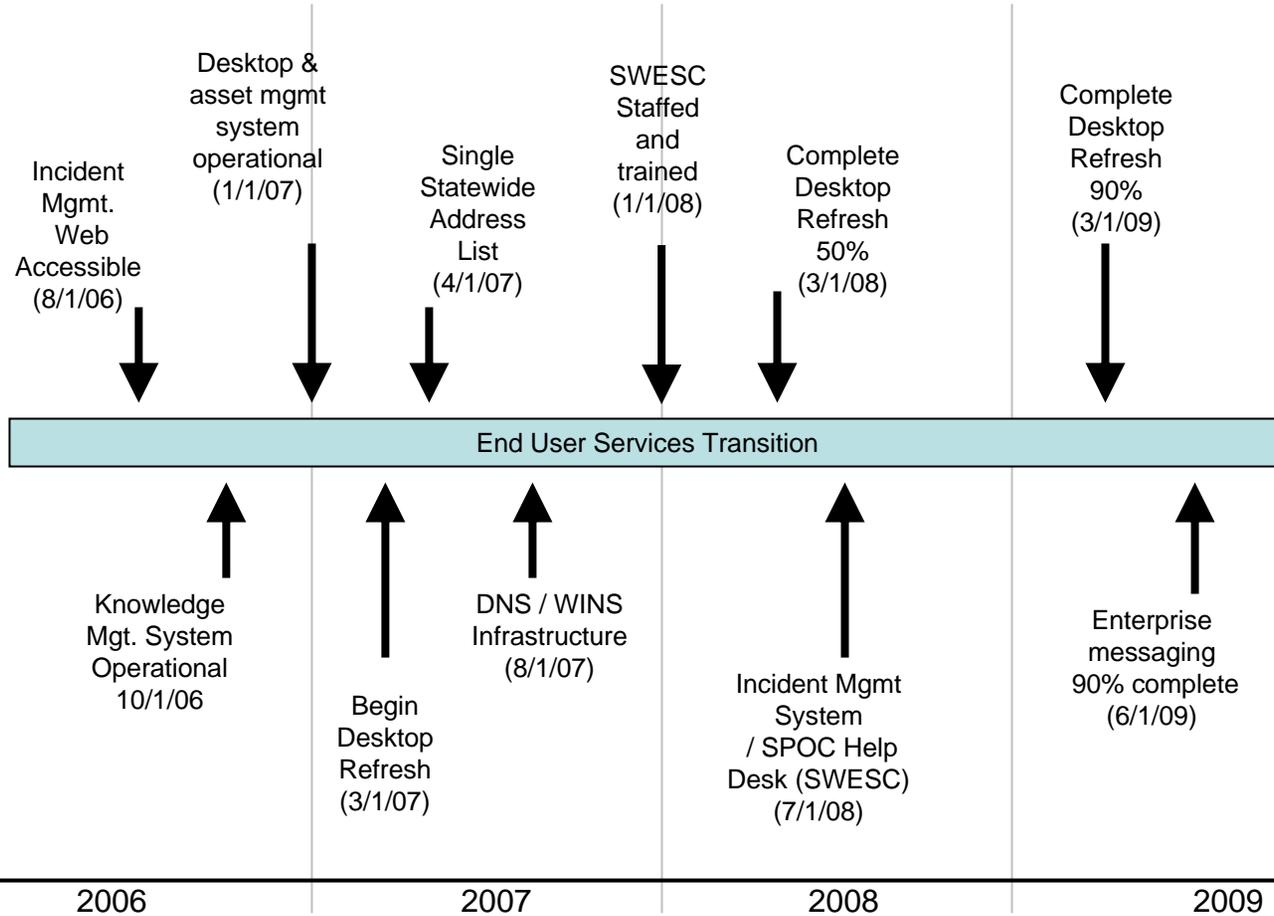
End User Services Transition

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

End User Services Status and Progress

<u>Quarter</u>	<u>Milestone</u>	<u>Due</u>	<u>Status</u>
Q3 2006	Incident Management Web Accessible	8/1	Complete
	Altiris backend system pre-configured	9/30	Complete
Q4 2006	Knowledge Management System Operational	10/1	Delivered – Preparing for Post Live Testing
	Desktop & Laptop Selection	11/1	On Schedule
	Desktop Core Image Design Complete	11/30	On Schedule
Q1 2007	Desktop & asset mgmt system operational	1/1	On Schedule
	Begin Desktop Rollout	3/3	On Schedule

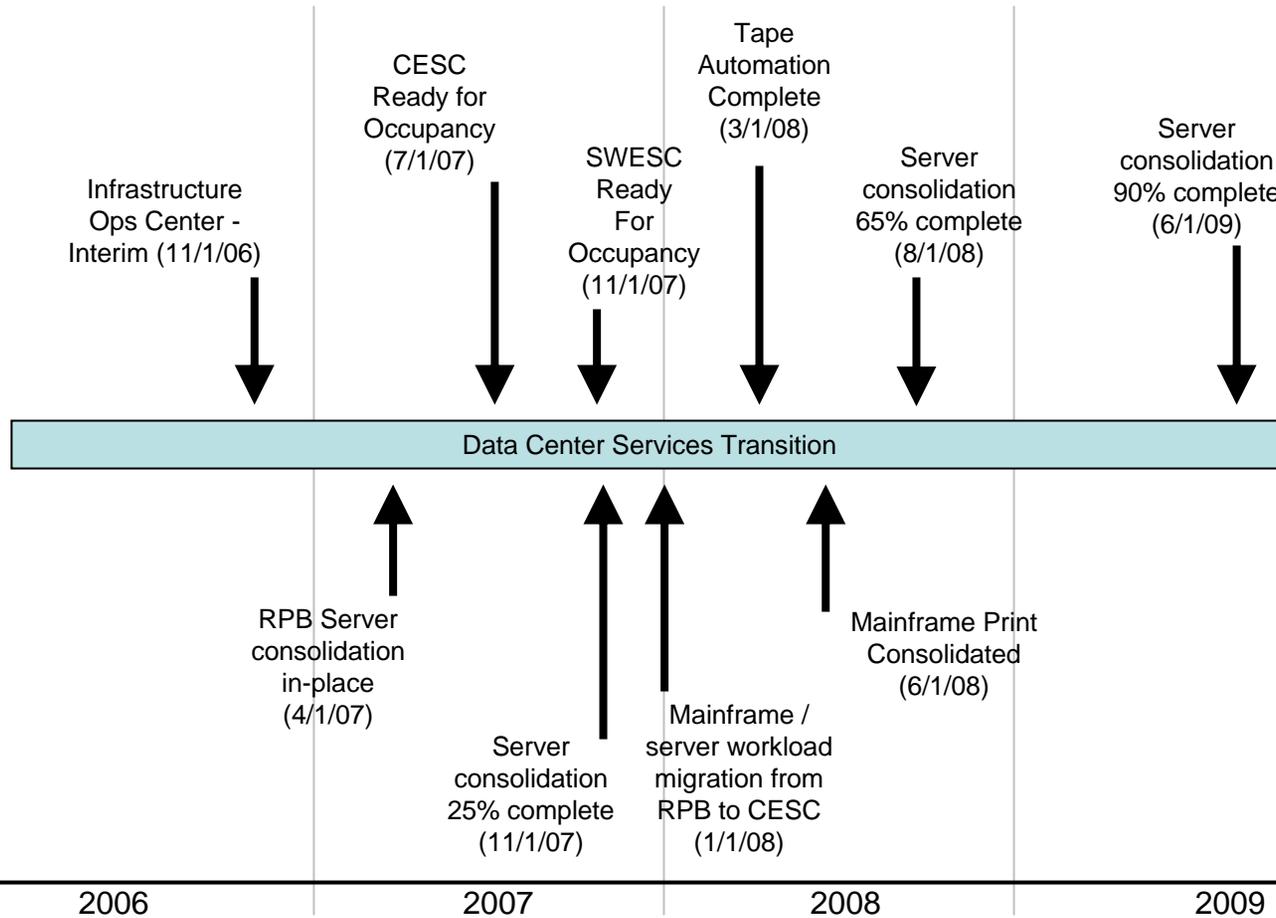
Data Center Services Transition

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

Data Center Services Status and Progress

<u>Quarter</u>	<u>Milestone</u>	<u>Due</u>	<u>Status</u>
Q3 2006	HP Open View Lab Hardware	9/15	Complete
	Complete Data Center Precast Walls	9/30	Complete
Q4 2006	SWESC Groundbreaking	10/27	On Schedule
	Begin Mainframe Print Consolidation Project	10/30	On Schedule
	Infrastructure Ops Center (Interim)	11/1	On Schedule
Q1 2007	Begin RPB Server Consolidation in Place	1/15	On Schedule
	RPB Server consolidation in-place complete	4/1	On Schedule

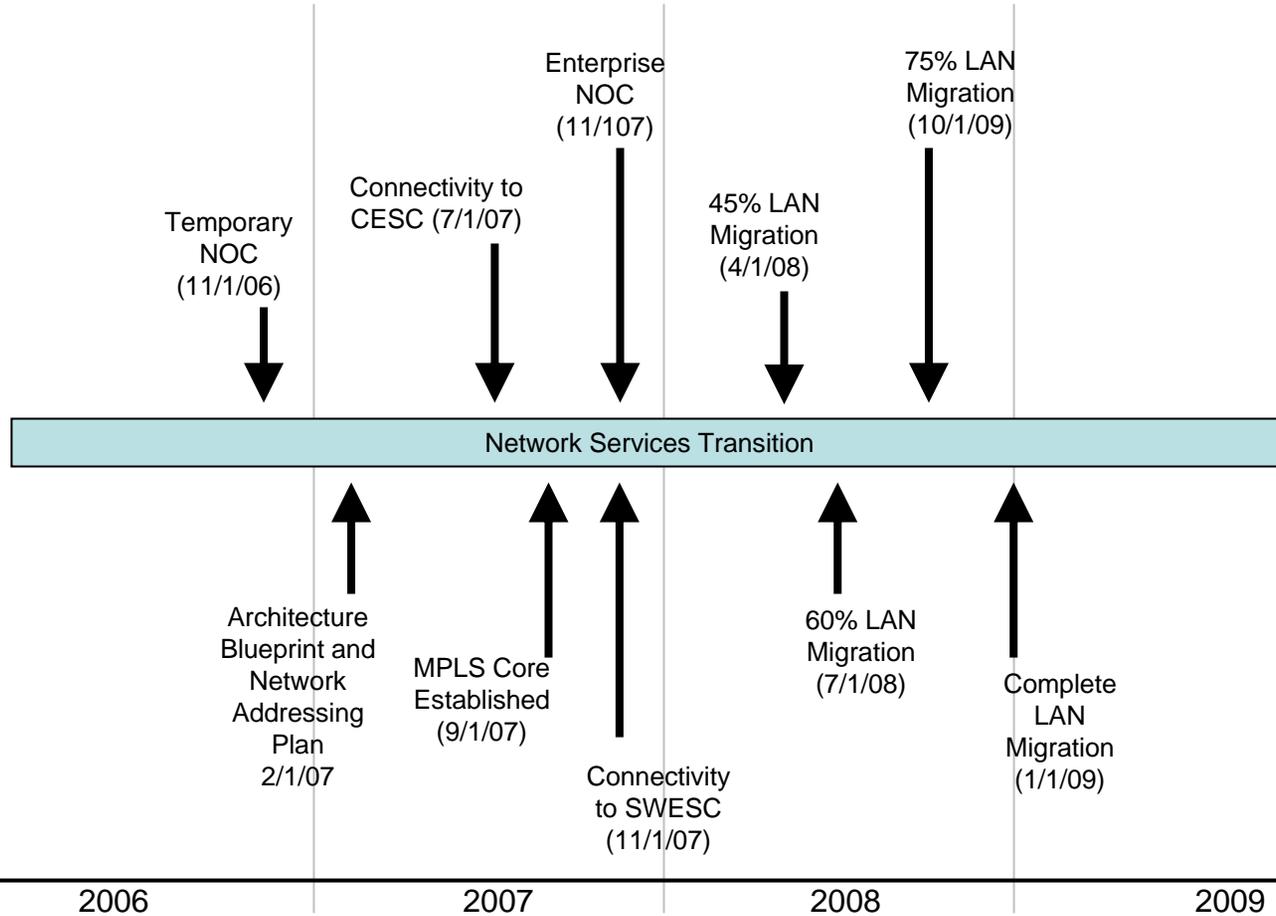
Network Services Transition

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

Network Services Status and Progress

<u>Quarter</u>	<u>Milestone</u>	<u>Due</u>	<u>Status</u>
Q3 2006	Complete Temporary NOC Requirements	9/15	Complete
	Draft Network Deployment Order Plan	9/30	Complete
Q4 2006	System Requirements	10/20	On Schedule
	Deploy Temporary NOC	11/1	On Schedule
	Initial MPLS Network High Level Design	12/1	On Schedule
Q1 2007	Architecture Blueprint & Network Addressing Plan	2/1	On Schedule
	MPLS Detailed Design	3/1	On Schedule
	Richmond MAN Detailed Design	3/31	On Schedule

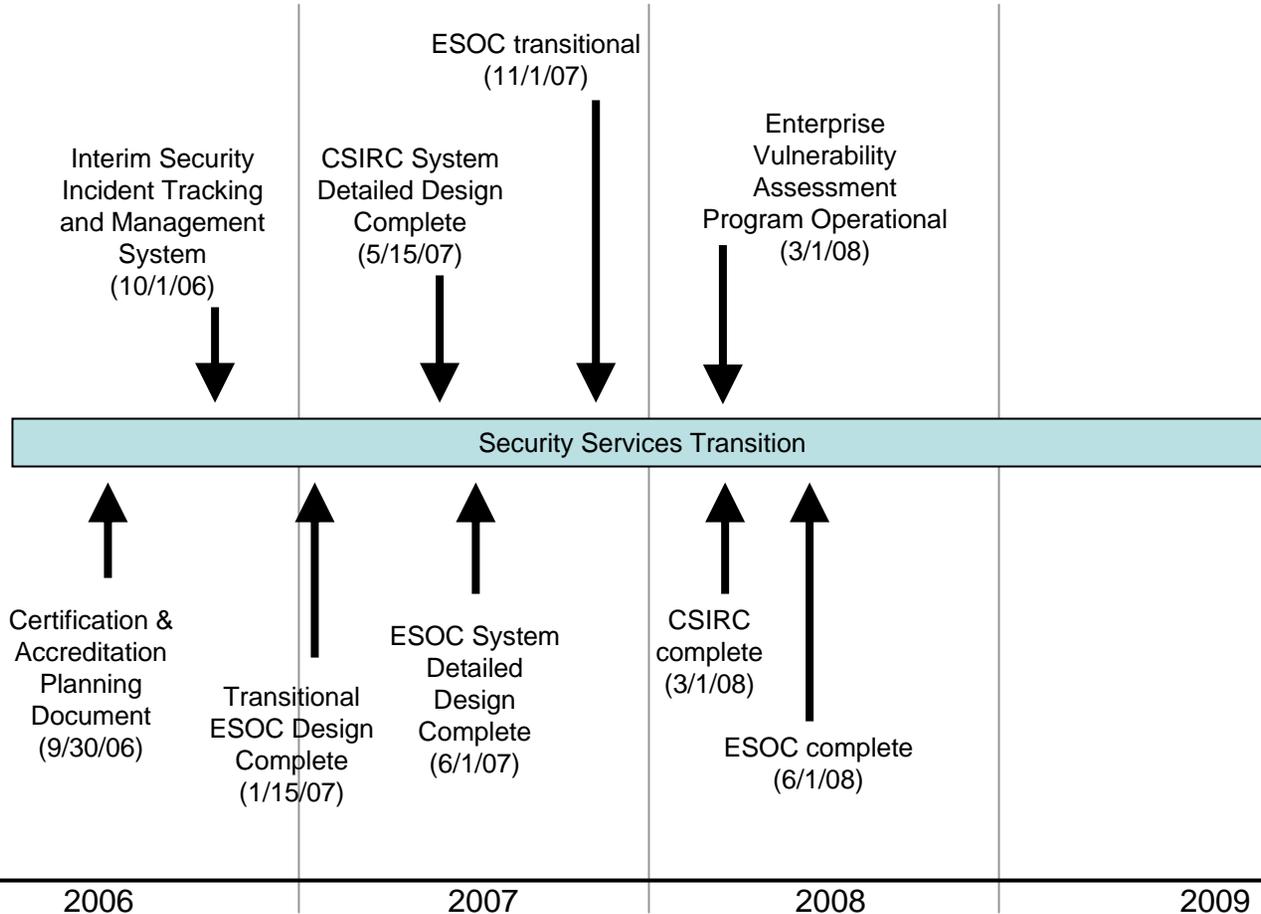
Security Services Transition

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

Security Services Status and Progress

<u>Quarter</u>	<u>Milestone</u>	<u>Due</u>	<u>Status</u>
Q3 2006	Begin ISG Design	9/1	Complete
	Security Certification/ Accreditation Planning Document	9/30	Complete
Q4 2006	Operational Interim Security Incident Tracking System	10/1	Delivered for Acceptance
	Internet Secure Gateway High Level Design Complete	11/01	On Schedule
	Transitional ESOC Design	12/15	On Schedule
Q1 2007	Internet Secure Gateway Detailed Design Complete	1/15	On Schedule
	Acquire/Receive Transitional ESOC Equipment	2/28	On Schedule

IV&V

- CACI concluded its initial review and delivered its formal report 8/31 – assessed ITP as maturity level 2 (Repeatable)
- ITP could be expected to achieve level 3 (Defined) in next 8-12 months
- 180 positive findings, 138 minor negative
- ITP action plan to sustain positive findings and address minor negative findings:
 - Evolve senior management teams, committees and forums with respective charters and prioritized processes
 - Document and communicate those prioritized processes
 - Establish consistent work methods producing artifacts and evidence of the processes and their outputs
- First follow-up review by CACI scheduled Nov 27 – Dec 14



Standard Infrastructure Practices

Fred Duball, VITA

October 31, 2006



NORTHROP GRUMMAN

Standard infrastructure practices

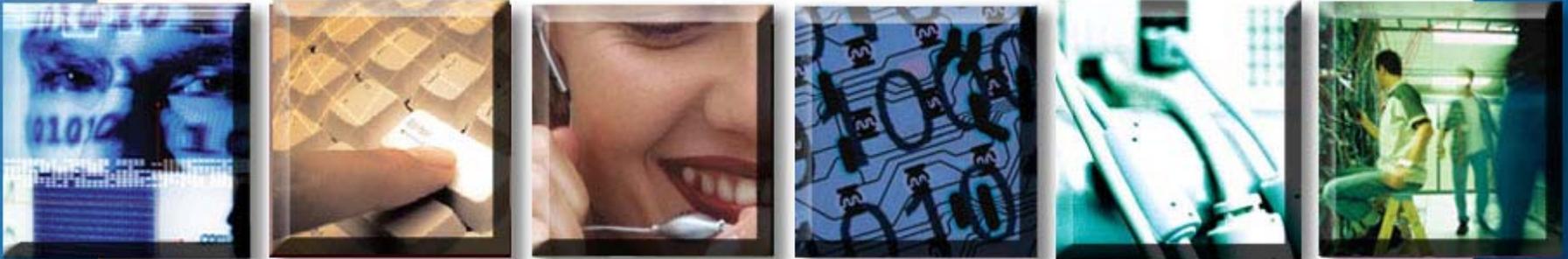
- **Purpose: Ensure basic infrastructure practices are being followed enterprise wide**
- Detailed description of Practices sent out to the field through Management Chain - Sept 21
- Compliance Tracking sheet will be sent back up through Management Chain – Tracking sheet consists of checkboxes for compliance, working on compliance, exceptions.
- Response due Oct 27
- Have allowed exceptions, will address those exceptions to determine if we can assist agencies reach compliance.

Standard infrastructure practices

1. Production server backup daily
2. Rotate backup tapes
3. Change user passwords every 90 days
4. Admin passwords restrictions
5. Load OS patches monthly or as directed
6. Distribute virus patches daily
7. Test 2 server restores yearly
8. Default passwords removed from network monitoring accounts
9. Document RAID configuration
10. Firewall on laptop - recommended

NORTHROP GRUMMAN

DEFINING THE FUTURE



ISOAG

Transformation Security Solution Briefing

Linda Smith, Stephen King, Jason Sewell, VITA/NG

October 31, 2006



SLIDES INTENTIONALLY OMMITTED



Bringing IT All Together

David Turner, VITA/NG

October 31, 2006

Virginia Information Technologies Agency



NORTHROP GRUMMAN

Agenda

- What is Information Technology Infrastructure Library (ITIL)
- What is IT Service Management (ITSM)
- The ITIL Framework
- Transformation Realization (How to get there)

What is Information Technology Infrastructure Library (ITIL)

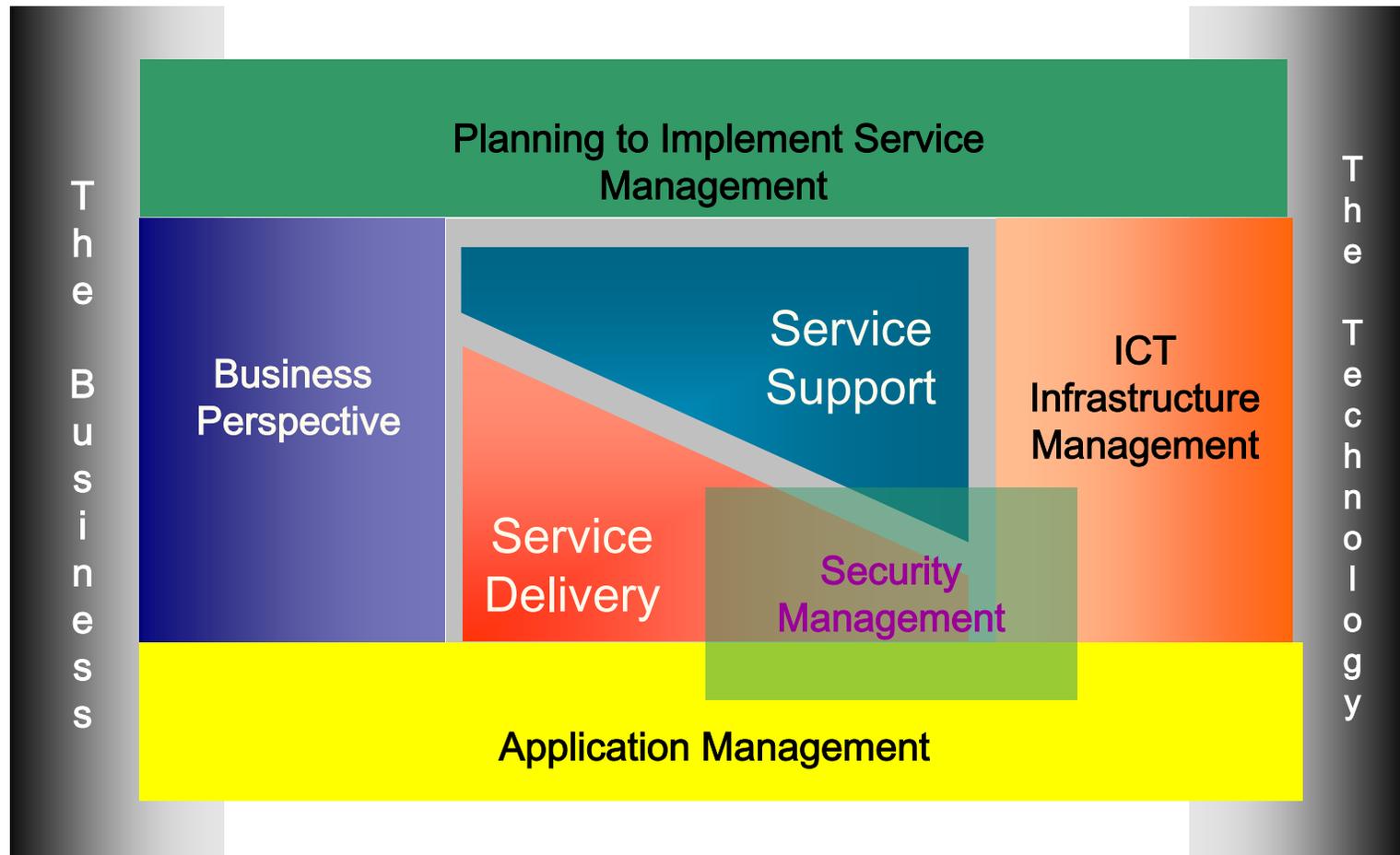


What is ITIL?

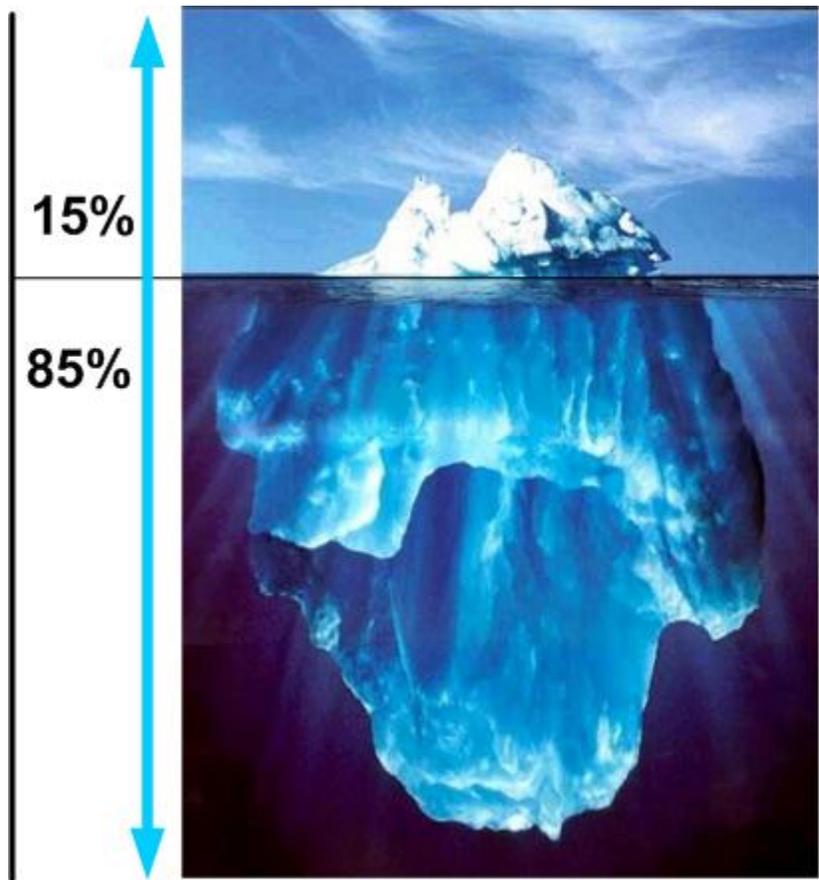
- ITIL stands for the **I**nformation **T**echnology **I**nfrasturcture **L**ibrary
- ITIL is a Series of reference books based on what the industry recognizes as “Best Practices”
- Originally established in the late 1980s by the UK government Central
- Computer and Telecommunications Agency (CCTA) - now OGC
- ITIL Processes are **GUIDELINES** not Methodologies.
- Based on practical experience, not vague or theoretical ideas.
- It is **NOT** a set of rules or procedures.

It has become the global standard in Service Management
ISO20000/BS15000

The IT Infrastructure Library



Technology Is Not A Silver Bullet



Technology: Tools and Infrastructure

Process: Definition/Design, Compliance and Continuous Improvement

People: Roles, Responsibilities, Management

Culture: Values, Unspoken norms, Often experienced and not seen

The ITIL Business Case

- More than 70% of technology budgets can be spent on Operating & Managing IT Infrastructure
- Increase efficiency and flexibility through well-defined and measurable IT processes
- Eliminates organizational “silos”
- Creates competitive advantage via the promotion of consistent and cost-effective services.
- Increase staff proficiency through comprehensive training and common direction
- Common processes with proven framework (*ISO20000*)
- Manage services to customers, NOT technology to users!

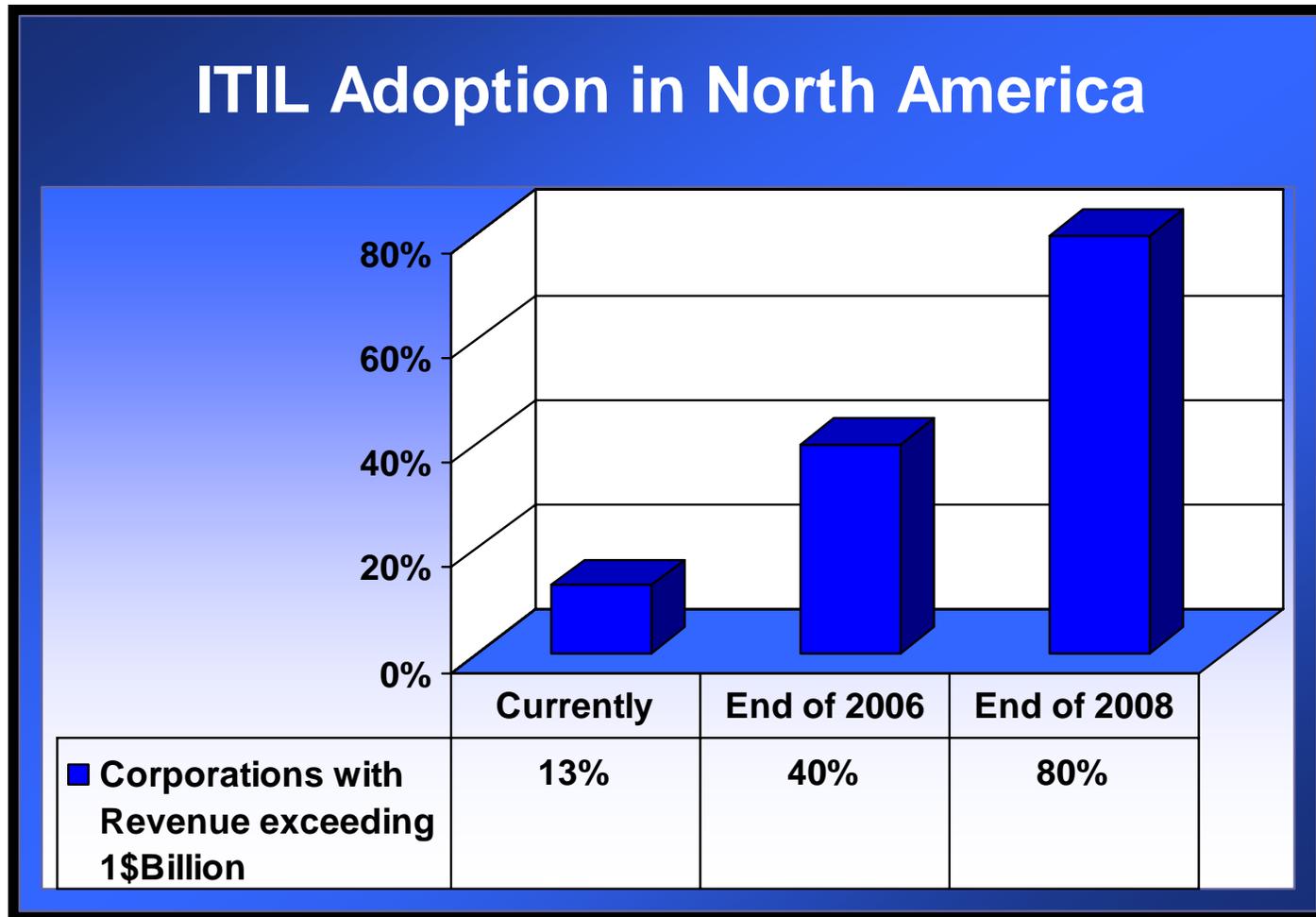
"If you've got best practices in place for a well-managed environment, you can reduce your total cost of ownership by as much as 25% to 30%."

*Michael Gartenberg
Gartner Group, Inc.*

ITIL Popularity Around the Globe

- 500,000+ ITIL/ITSM certifications to IT staff have been given globally to date.
- More than 6,000 companies in the public, private, and government sectors are in the middle of adoption and demanding core knowledge on resumes.
- IBM, HP, Microsoft, Oracle, CA and others have recognized ITIL as the framework of choice for managing their client's IT operations and likewise started building their own versions.
- The Northrop Grumman consolidated data center standard is ITIL based ISO 20000
- 60+ tool vendors claim their structure is based on ITIL as a framework (e.g. Peregrine, Remedy, CA, Mercury, OpenView, etc)
- Standard: BS15000 has become ISO 20000
- UK IT employees must have ITIL Foundations certification for Employment
- Gartner, IDC, MetaGroup, and Forrester recognize ITIL as "Best Practices in Change, Problem, and Service Level Management.

ITIL Popularity Around in the US



FORRESTER

How will ITIL impact the VITA Partnership

- **ITIL Optimization Project will effect the NG/VITA Partnership by delivering overarching governance for all aspects of the IT organization by:**
 - **Providing a common framework and terminology for communication between IT and the business**
 - **Providing standard policies, procedures and processes**
 - **Providing integration and communication across processes and functional areas**
 - **Providing management and control over entire managed services environment**
 - **Providing a programmatic approach to service execution and continuous service improvement**
 - **Aligning to business needs and requirements**

Why Service Management (within VITA)?

- ✓ ROI for NG/Commonwealth
 - ✓ Better, Faster, Cheaper
- ✓ Stronger Focus and Strengthening of IT controls
 - ✓ Agencies are more dependent on IT
 - ✓ Agencies are demanding more for less
 - ✓ Transformation Projects = Increase Change
- ✓ Customer satisfaction and expectation levels
 - ✓ SLA
 - ✓ KPI
 - ✓ Metrics/Reporting
 - ✓ Compliance with Regulations and Standards
 - ✓ SAS70 Type II, HIPPA, etc.
 - ✓ ISO 20000, ISO 27001, etc.

What is IT Service Management (ITSM)



What is an IT Service?

An **IT Service** is a set of related functions provided by IT systems in support of the business and perceived by the customer/user as a coherent and self-contained entity.

Key Phase: **'end-to-end' service**

Service ✓

E-mail

Billing System

Order Process System

Service ✗

Wide Area Network

Unix Server

Oracle Database

The ITIL Framework



Capacity Management

Service Delivery

IT Service Continuity Management

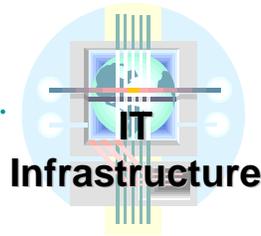
Availability Management

Financial Management for IT Services

Service Level Management



Service Desk



IT Infrastructure



Security Management

Incident Management

Configuration Management

Problem Management

Service Support

Change Management

Release Management

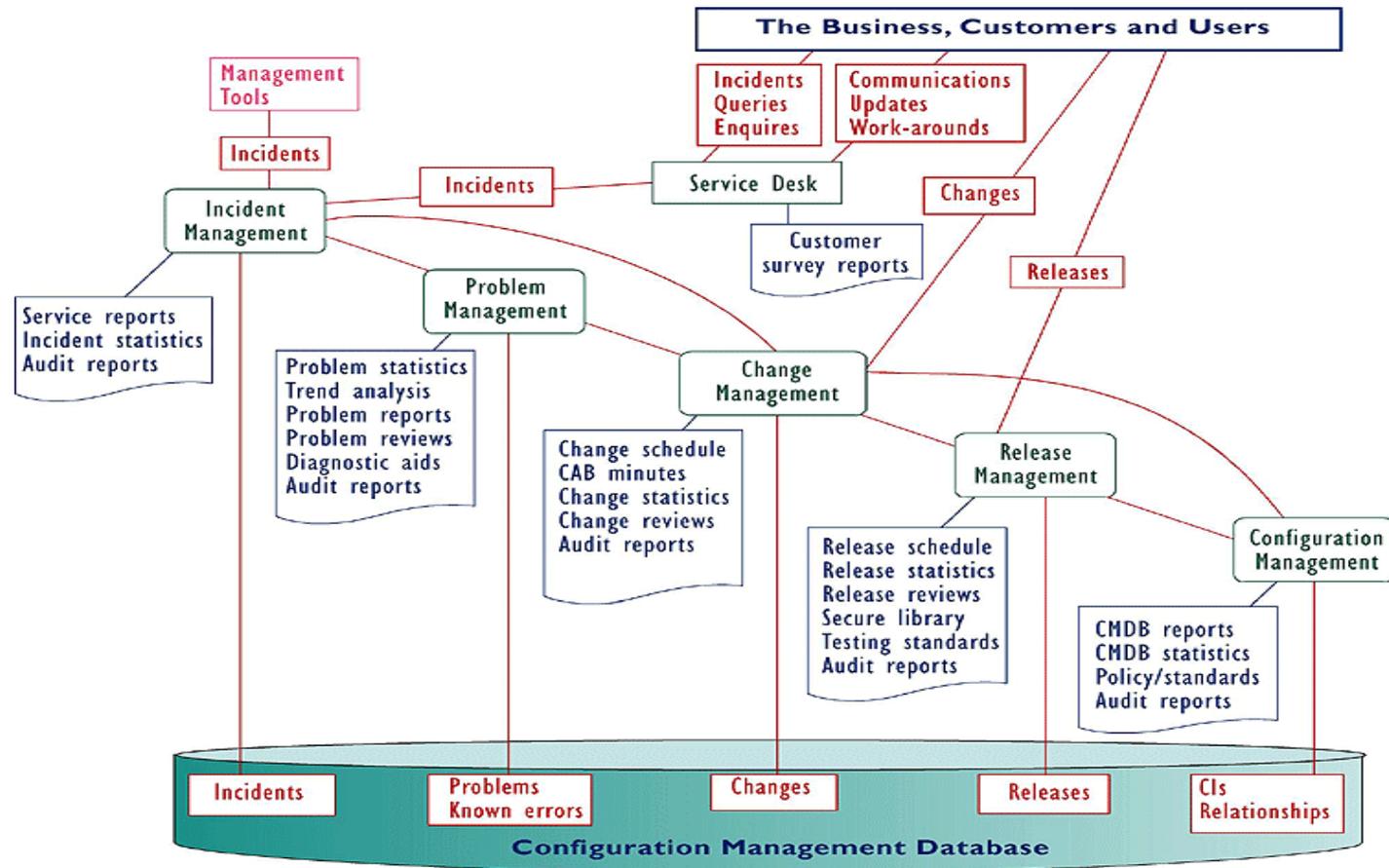
ITIL Framework

Overview of the ITIL Service Management

	Service Support	Service Delivery
Focus	Day to day	Planning/Longer term
S.P.O.C	Service Desk	Service Level Mgmt
Who Affected?	User	'Paying' Customer
Main Focus	Service Quality	Value for Money
ITIL Function	Service Desk (verses Help Desk)	Data Center
ITIL Processes	Incident Mgmt Problem Mgmt Change Mgmt Release Mgmt Configuration Mgmt	Service Level Mgmt Availability Mgmt Capacity Mgmt Service Continuity Mgmt Financial Mgmt

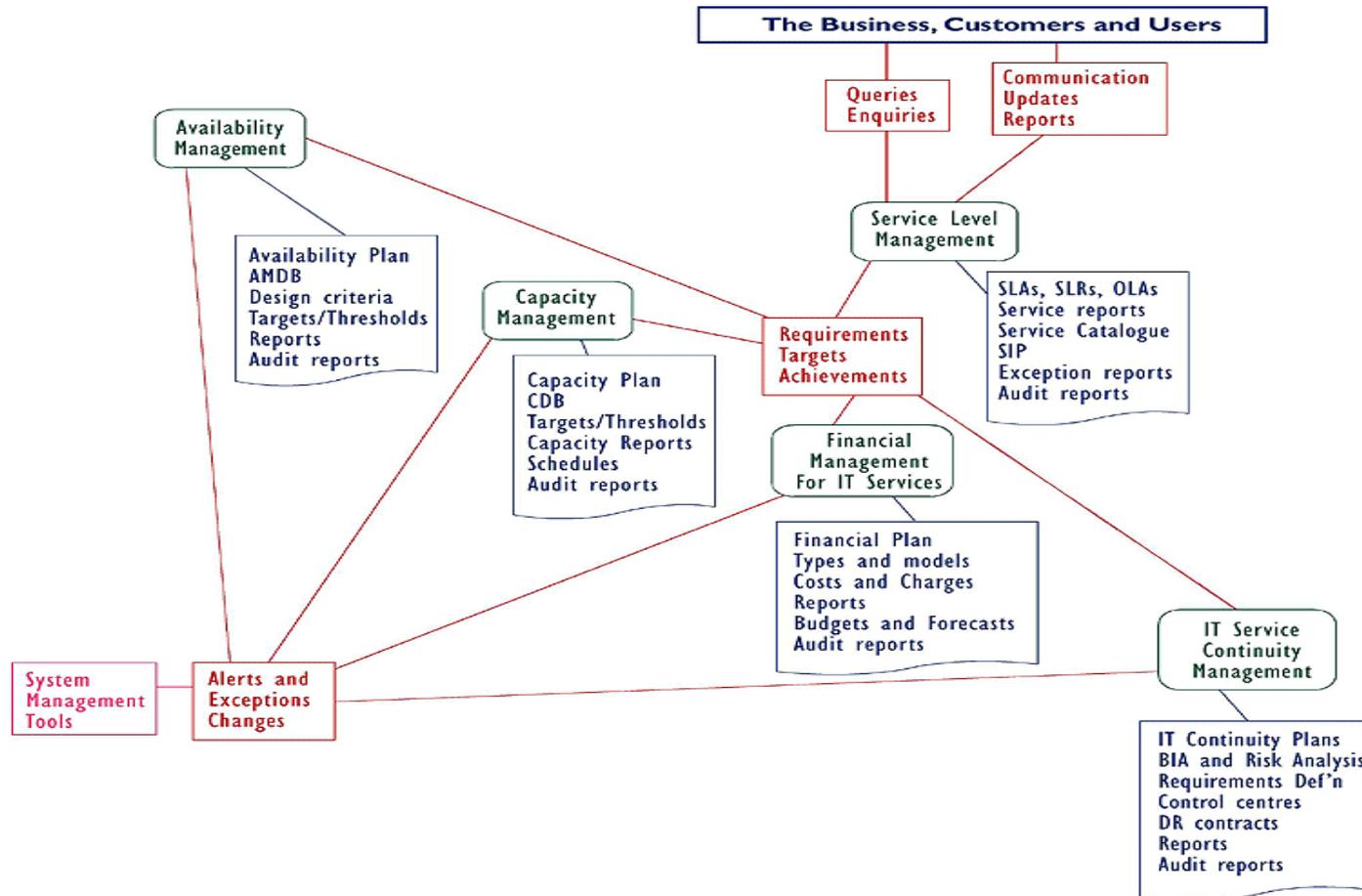
ITIL Framework

Service Support Coverage

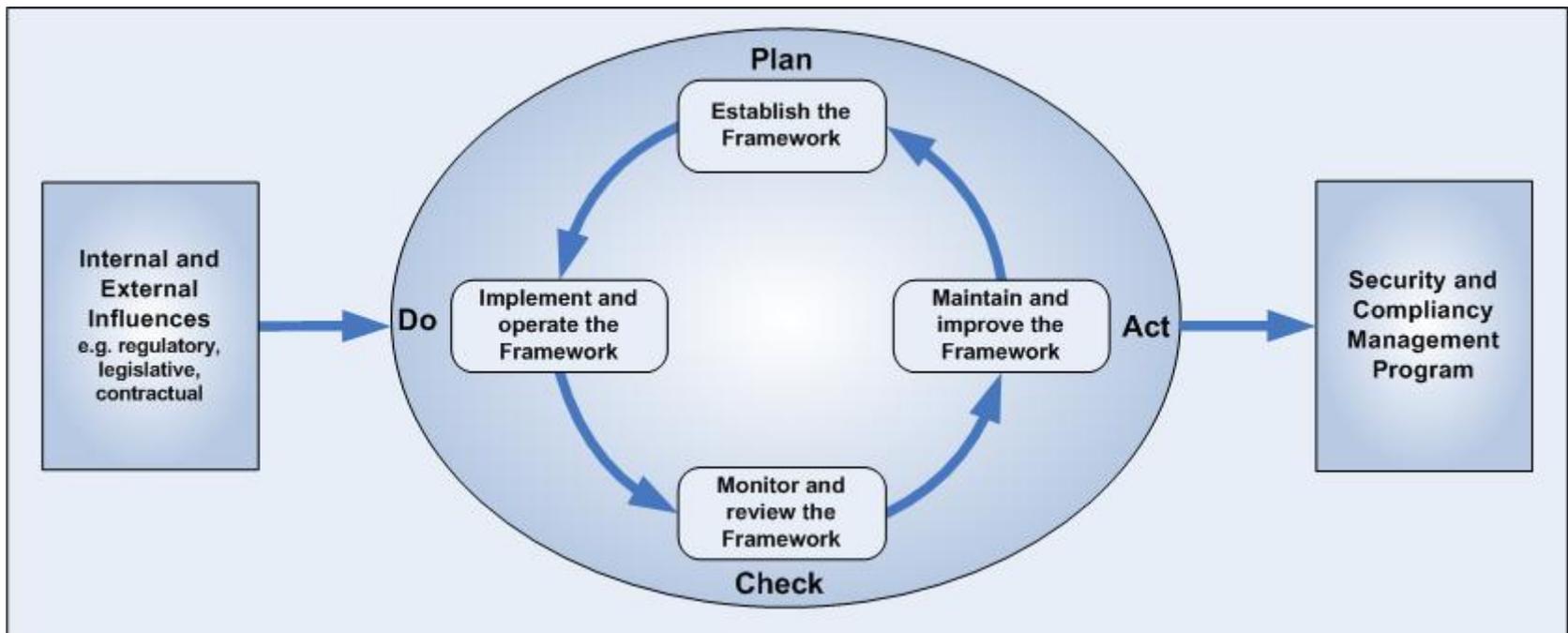


ITIL Framework

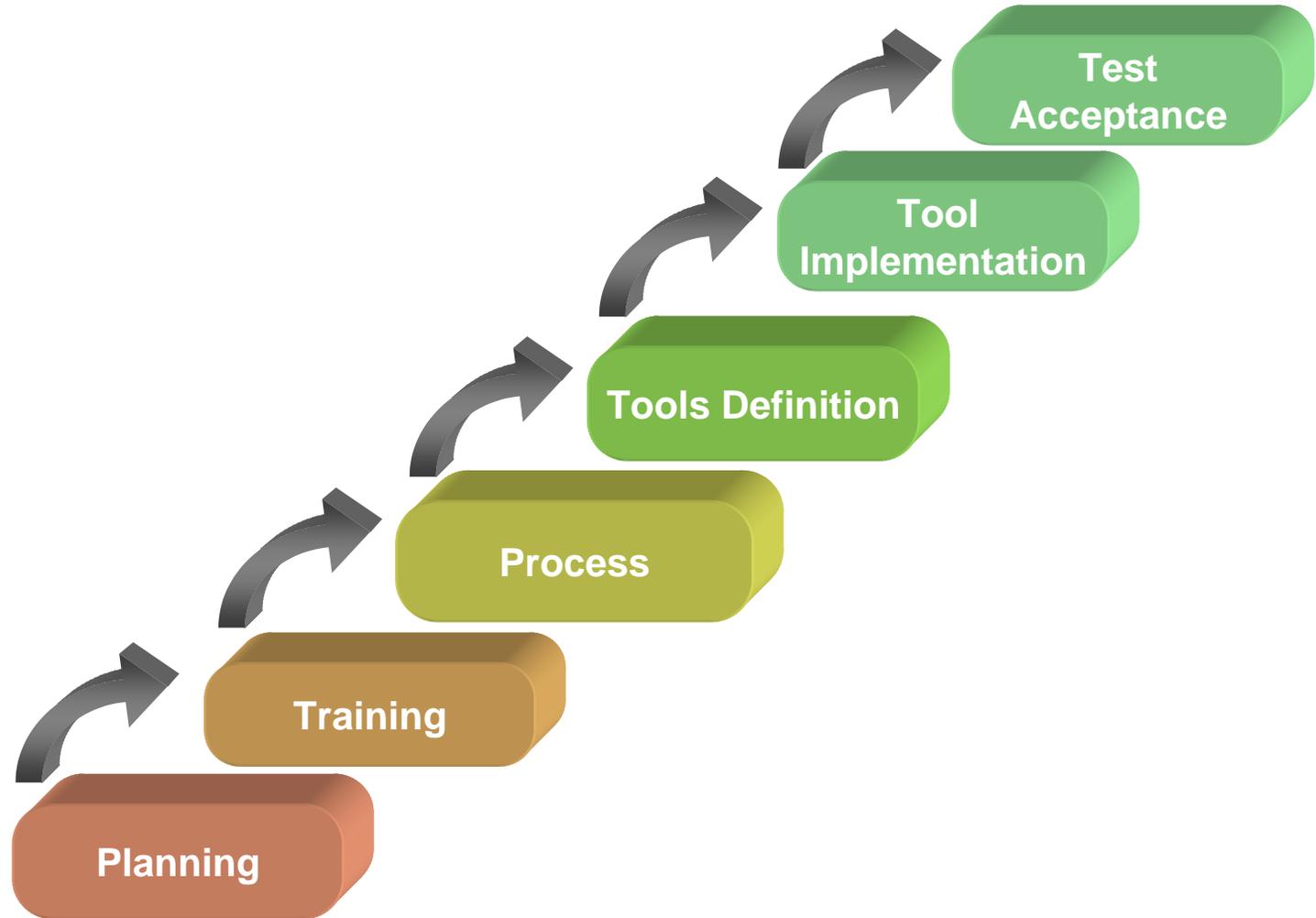
Service Delivery Coverage



Security, Compliance and Governance Management Programs based on ISO27001:2005



Process Implementation Cycle



Program Approach to ITIL

- Cultural Awareness, Education and Formal Training
- itDNA® Maturity Assessments for one or more itDNA® Disciplines or Elements
- Process Design including Roles & Responsibilities, Standards, Policies and Procedures, Industry Best Practices
- Technology Enabler Integration – Integration of the supporting tools which include Peregrine, Altiris and HP OpenView.
- Security and Compliance Management Framework design and implementation
- Audits and/or remediation of gaps against Standards such as ISO 20000 and ISO 27001 (not in contract)

ITIL Process Implementation Phases

- Phase 1 – Incident Management Process Assistance for TR047
 - Peregrine configuration for TR047 requirements
- Phase 2 – Change, Configurations, Release
 - Peregrine configuration for TR053 requirements
- Phase 3 – Incident, Service Request, Problem, Capacity, Availability
 - Peregrine configuration for Incident (enhance), Service Request, Problem
- Phase 4 – Security, Continuity, Service Catalog, SLM
- Phase 5 – Financial, Relationship (non-contract)

Questions?



JIC



Major Milestones for CCR & Incident (Phase 1)

Assume facilities are available

- Incident Management (Phase 1) Workshops— 8/22 and 8/23
- Master Communications Plan complete 9/1/06
- Complete Leadership Awareness & Assignments – 9/11
- Change/Configuration/Release (CCR) Process Kick Off – 9/25 – 10/5
- Begin ITIL Foundations & Practitioner Training – 10/9
- CCR Peregrine System Design (SDD) & Interface Design (IDD) Complete – 12/21/06
- Change/Configuration/Release Processes Accepted 2/11/07
- CCR Peregrine Configuration & Integration Complete – 2/22/07
- CCR Peregrine Pilot Complete 3/30/07

Major Milestones for Incident (Phase 2), Problem, Capacity & Availability (IPCA)

- Begin to Identify Workshop Participants – 1/8/07
- Begin Design Workshops for IPCA – 2/1/07
- IPCA Processes Accepted – 6/29/07
- Peregrine Configuration for Incident (P2) and Problem Complete – 10/24/07
- Pilot Test Complete 12/4/07

Major Milestones for Security, Continuity, SLM

- Begin Identify Workshop Participants – 5/21/07
- Begin Security, Continuity Design Workshops – 6/18/07
- Service Catalog Design Begins -- 6/18/07
- Service Catalog Accepted – 10/17/07
- Service Level Management Process Design Begins – 10/3/07
- Security & Continuity Processes Accepted – 11/15/07
- Service Level Management Process Accepted -- 3/7/08
- ITIL Consistency, Conformity & Performance 11/1/07 – 3/21/08
- Process Integration Validation – 3/24/08 – 5/27/08
- ITIL Process Optimization Complete – 6/1/08



Virginia Information Technologies Agency

Risk Management

Cathie Brown, VITA

ISOAG Meeting

Date October 31, 2006

expect the best



Risk Management

Purpose: to delineate the steps necessary to identify, analyze, prioritize, and mitigate risks that could compromise COV IT systems. (ITRM Standard SEC501-01)

Includes requirements in the following areas:

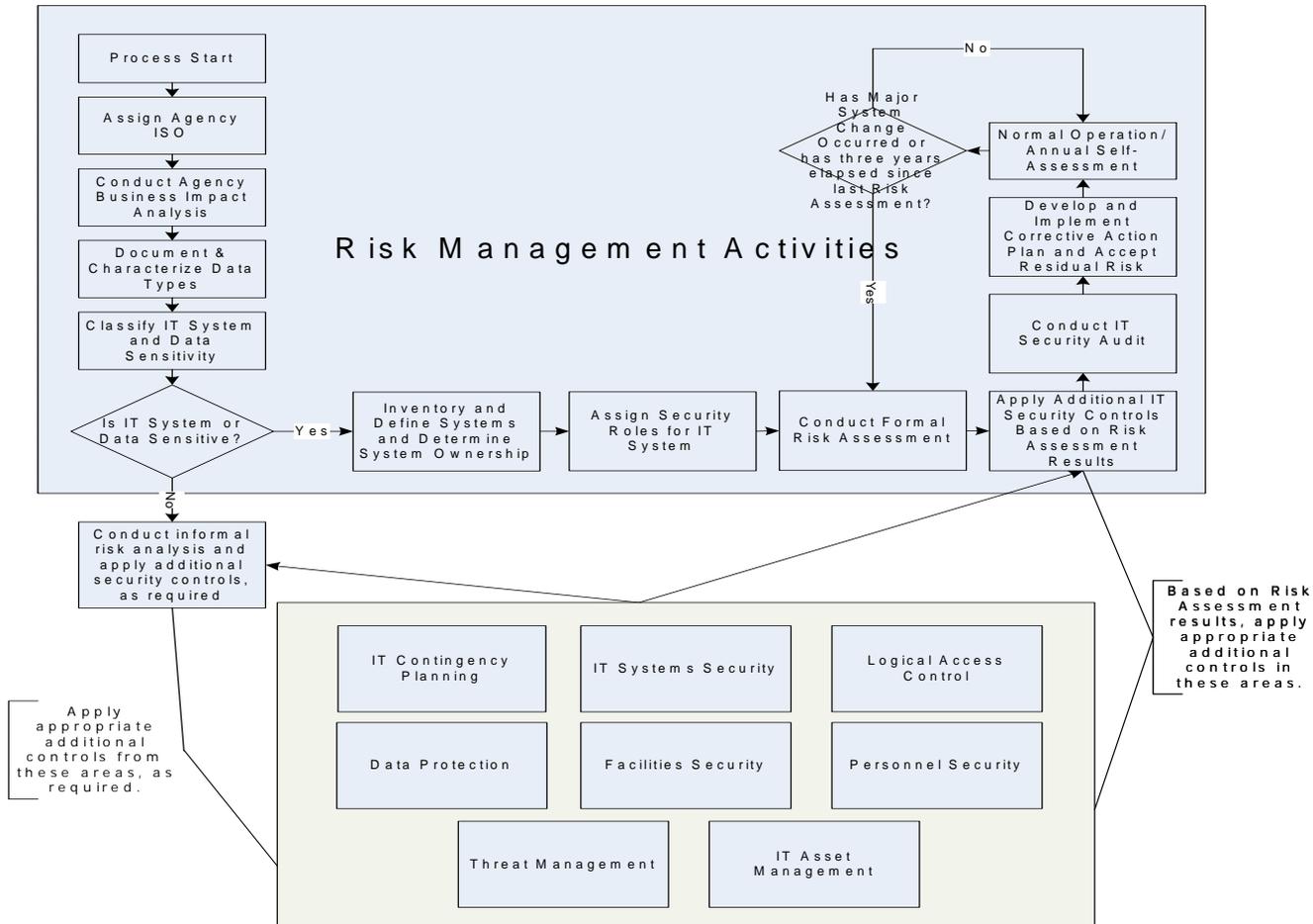
- IT Roles and Responsibilities
- Business Impact Analysis
- IT Systems and Data Sensitivity Classification
- IT System Inventory and Definition
- Risk Assessment
- IT Security Audits



Risk Management

- Risk Management Guideline (ITRM Guideline SEC506-01) – ORCA
- Methodology for IT Security Risk Management suitable for supporting the requirements of COV Policy and Standards (SEC500-02, SEC501-01, SEC502-00)
- Provides a guideline and templates for conducting Risk Management activities

IT Security Risk Management Process





IT Security Roles & Responsibilities

IT System Name, Acronym, and designation				
Role	Responsibility	Name	Reports to (Name and Title)	Assignment Date
Agency Head	Oversee Agency IT Security Program			
Information Security Officer	Overall security of Agency IT systems and liaison to the CISO of the Commonwealth.			
Privacy Officer	Provide guidance on privacy laws.			
System Owner	Responsible for the overall security of the IT system. Accountable to the Agency Head.			
Data Owner	Spread IT security awareness to data users. Develop any additional local requirements, guidelines and procedures needed to protect the data.			
System Administrator	Day-to-day administration of the IT system. Implements requirements of the IT Security Management Program.			
Data Custodian	Protect data from unauthorized access, alteration, destruction, or usage and in a manner consistent with COV IT security policies and standards			
IT System Users	Read/comply with Agency IT security requirements			

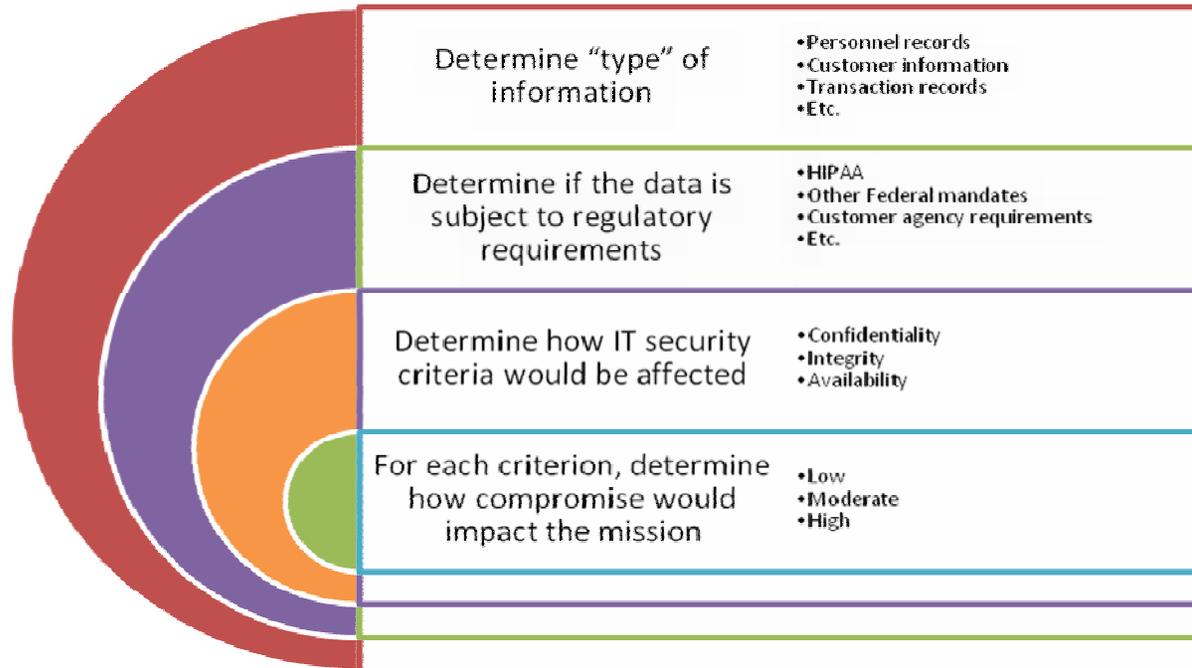


Business Impact Analysis

- The role of the BIA in IT Security Risk Management is to identify the IT systems that support critical business functions
- Refer to *The VDEM COOP Planning Manual* for instructions and worksheets

System & Data Sensitivity Classification

- Classify the sensitivity of IT systems and data





IT System Inventory & Definition

IT System Inventory and Definition Document			
I. IT System Identification and Ownership			
IT System ID		IT System Common Name	
Owned By			
Physical Location			
Major Business Function			
System Owner Phone Number		System Administrator(s) Phone Number	
Data Owner(s) Phone Number(s)		Data Custodian(s) Phone Number(s)	
Other Relevant Information			
II. IT System Boundary and Components			
IT System Description and Components			
IT System Interfaces			
IT System Boundary			



IT System Inventory & Definition

III. IT System Operability and Agreements				
Agency or Organization	IT System Name	IT System ID	IT System Owner	Interoperability Security Agreement Summary
IV. IT System and Data Sensitivity				
Type of Data	Sensitivity Ratings Include Rationale for each Rating			
	Confidentiality	Integrity	Availability	
Overall IT System Sensitivity Rating and Classification	Overall IT System Sensitivity Rating Must be "high" if sensitivity of any data type is rated "high" on any of the criteria			
	High	Moderate	Low	
	IT System Classification Must be "Sensitive" if overall sensitivity is "high"; consider as "Sensitive" if overall sensitivity is "moderate"			
	Sensitive		Non-Sensitive	



Interoperability Security Agreement

Memorandum of Understanding

This Memorandum of Understanding comprises an Interoperability Security Agreement (ISA) between the System Owners of the _____ “owned” by the _____ and the _____ “owned” by the _____. The interoperability between _____ and _____ provides _____.

The table below outlines the nature of the sensitive data shared between the systems

Type of Data	Sensitivity Ratings		
	Confidentiality	Integrity	Availability



Interoperability Security Agreement

The System Owners of the two IT systems agree to the following:

- To maintain the security of their respective IT systems in accord with the controls specified by the most current risk assessment for each IT system. This requires each System Owner to share the applicable security requirements of their respective IT systems with each other.
- To inform the other of any changes to the risk profile of their respective IT systems. This includes any major configuration changes as defined by ITRM Standard SEC501-01.
- To inform the other, in a timely and deliberate manner, of any security breaches to their respective IT systems.

(include additional Agency-specific requirements here).

This ISA shall remain in force until _____ unless jointly re-accomplished by the ISOs.

Sign and date by both parties.



Risk Assessment

- Risk Assessment instructions and templates are provided in a separate document (ITRM Instructions SEC506-01)



IT Security Audit Plan

This Plan coordinates the execution of security audits for the IT systems supporting government databases (as defined by ITRM Standard SEC502-00).

Agency Name and Acronym	IT Security Audit Plan				
	Date Submitted	Submitted By			Areas for Special Emphasis and Additional Audit Requirements ¹
		Name & Title	Phone Number	E-mail Address	
IT System Name, Acronym, and Designation	Expected Auditor	Next Three Planned Audit Dates Fiscal Years			Areas for Special Emphasis and Additional Audit Requirements ¹
		2008	2009	2010	



Corrective Action Plan

IT Security Audit Quarterly Summary

Audit Name: _____

Audit Finding No. & Agency Concurrence	Short Title	Summary	Risk	Responsible Person(s) and Due Date	Status*	Status Date	Concurs: Planned Action & Status Does Not Concur: Mitigating Controls & Risk Acceptance

* Status Legend: NS = Not Started; U = Underway; C = Completed



QUESTIONS

????



Security Questions

Question

- We are processing a security survey from APA and VITA ran a security scan on the network. When I replied to APA that we were going to follow VITA security policy, they stated that each agency has to have its own separate written policies and procedures. This appears to be some what of a duplication of effort and is VITA available (without charging the agency) to assist in writing these documents for each individual agency?



Security

Answer

- Each agency is responsible for developing their own unique policies relative to their own business processes, sensitivity of data and risk tolerance
- According to COV ITRM Policy 500-02 Information Technology Security Policy, each Agency Head is responsible for
 - Security of the Agency's data
 - Taking appropriate steps to secure Agency IT systems and data through the development of an Agency IT security program
- Each Agency is responsible for having their own Information Security Policies related to how they utilize technology
 - Security awareness training
 - Protection of data
 - Back-up and recovery
 - Continuity of operations planning (COOP)
- VITA is developing guidance documents to assist you in implementing the security policies and standards



OTHER BUSINESS

Any Items for
Discussion??



ADJOURN

**THANK YOU FOR
YOUR TIME AND
THOUGHTS**

!!!