

AT&T Security Evaluation Program

Rebecca Finnin

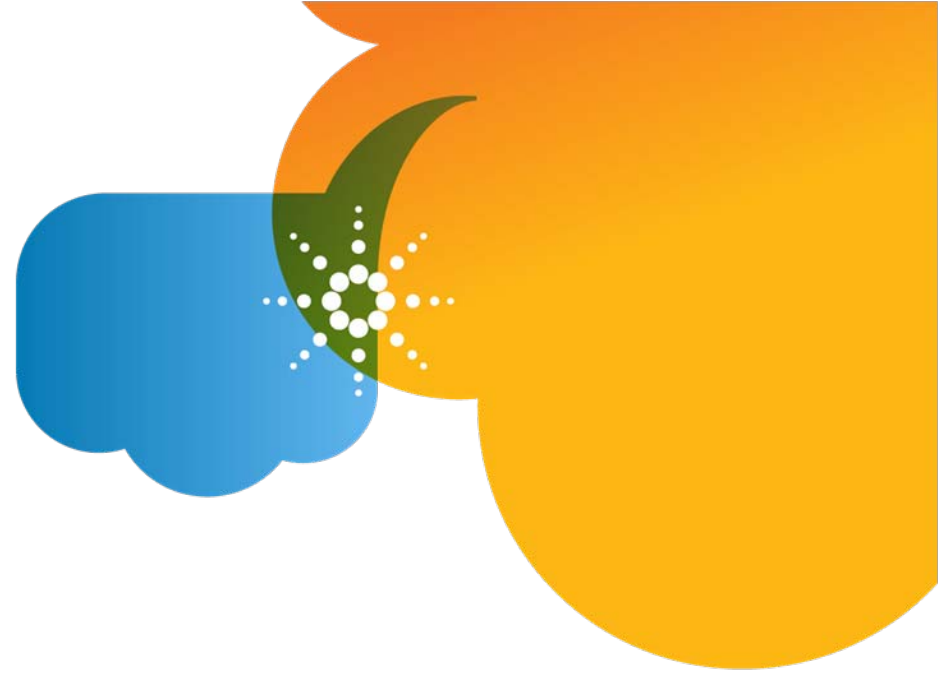
Director, AT&T Chief Security Office



Agenda

- AT&T Enterprise Security
- Compliance Management
 - Security Evaluation Program (SEP)
- Security Evaluation Programs
 - Websites
 - Applications/Databases
 - Servers
 - PCs
 - Modems
 - Routers/Switches
 - Firewalls
- Archer Automation





AT&T Enterprise Security





Enterprise Security

AT&T Security Policy, Standards and Awareness

- Develop and maintain security policies that enable the business and protect AT&T's world wide assets and data

Risk Management

- Maintain risk management processes that help to ensure appropriate approval, tracking and remediation for instances of non-compliance with AT&T security policies

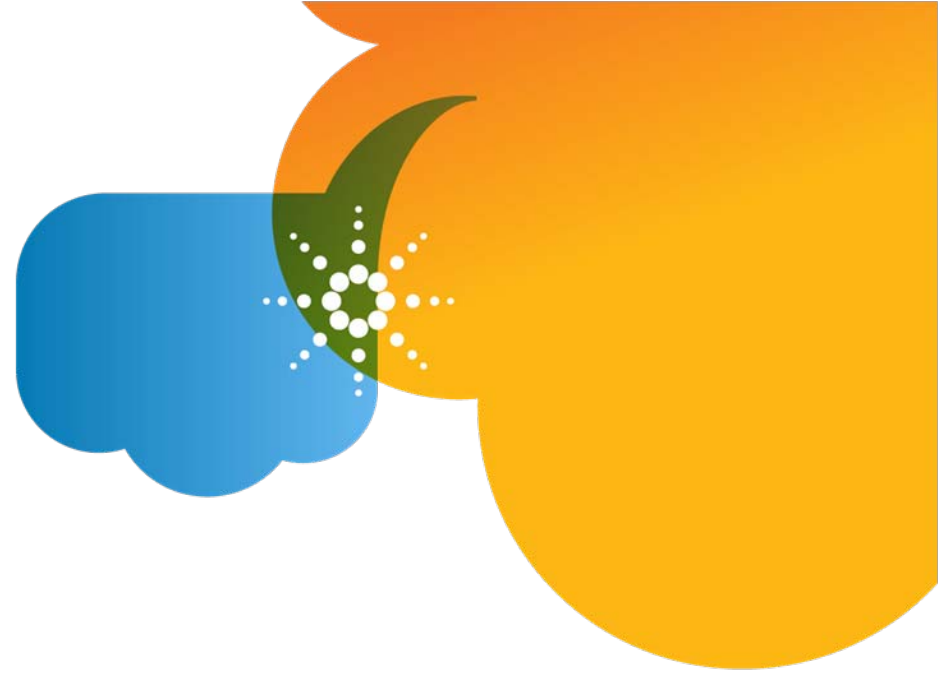
Compliance Management

- Review projects, applications and infrastructure to detect and remediate security vulnerabilities and instances of non-compliance with policy
- Maintain contract and review processes that extend AT&T security controls to vendors that process AT&T data

Audit Support

- Develop and support processes that help to ensure compliance with legal, regulatory, and customer requirements, including PCI, SOX, HIPAA, SAS 70, and customer contracts



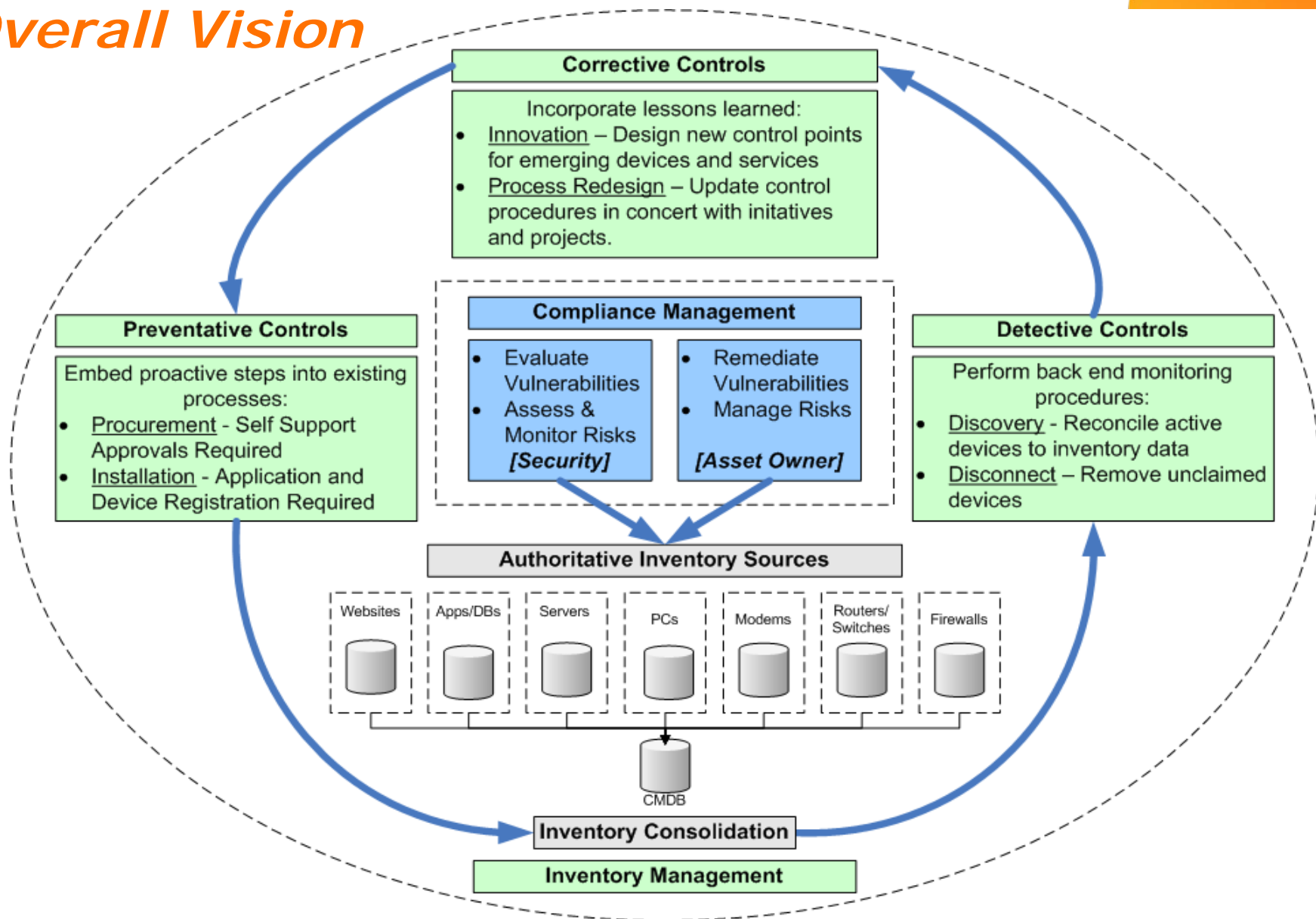


Compliance Management

Security Evaluation Program (SEP)



Security Evaluation Program: Overall Vision



Security Evaluation Program: *Methodologies & Tools*

Websites & Applications

Application Security Checklist

Threat Modeling

Static Code Review
(Fortify Source Code Analyzer)

Manual Code Review

Web Application Scanning
(Hewlett-Packard QAIInspect)

Database Scanning
(Application Security DBProtect)

Manual Penetration Testing

Servers & PCs

Operating System Checklist

Trust Level 1 Certification

Server Configuration Checks
(Symantec Enterprise Security Manager)

Server Port Scanning
(McAfee Vulnerability Manager)

Server/PC Virus Management
(McAfee Enterprise Policy Orchestrator)

PC Host Intrusion Protection
(McAfee Enterprise Policy Orchestrator)

PC Encryption
(Checkpoint PointSec)

Network Devices

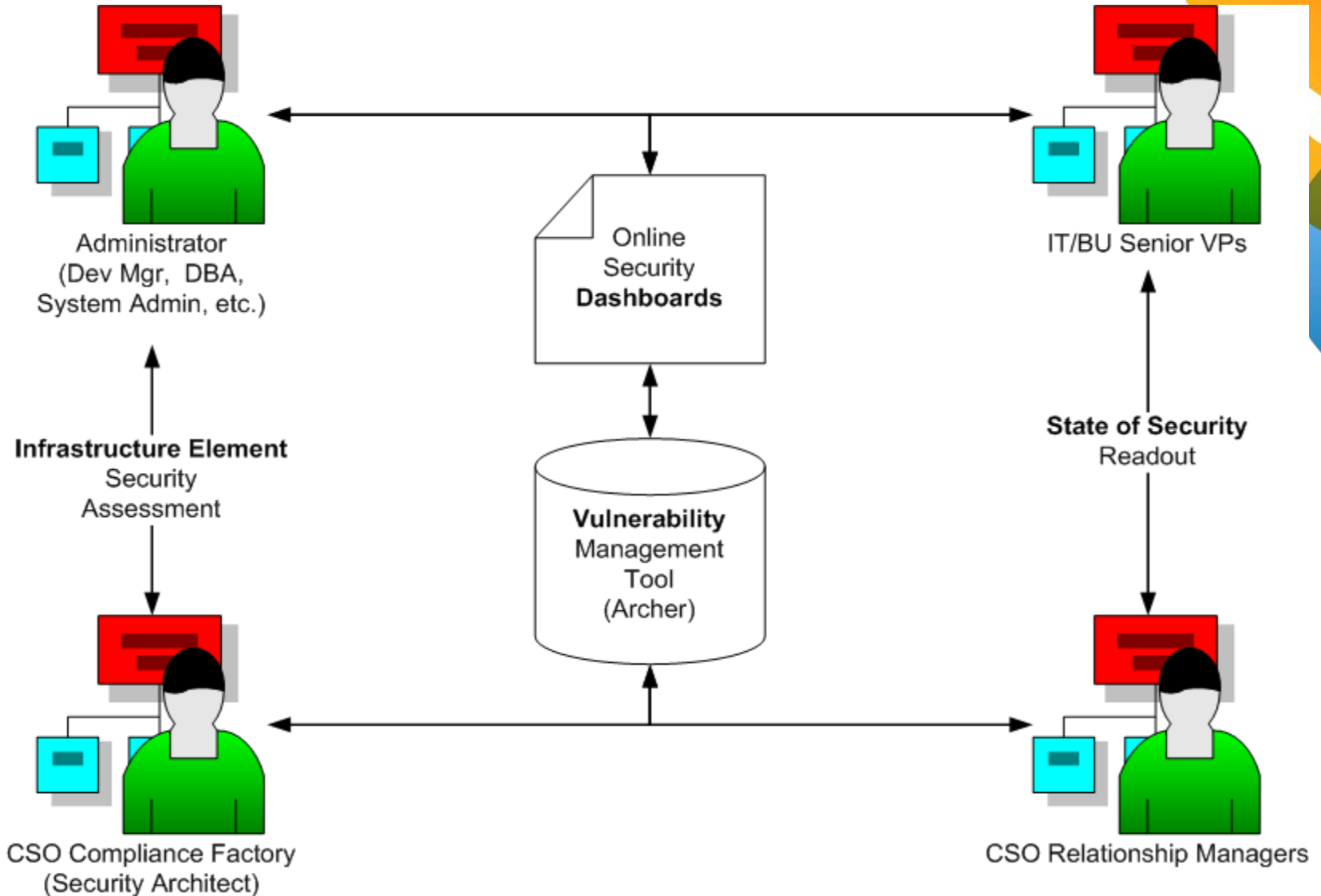
Router/Switch Assessments
(Alterpoint Network Authority)

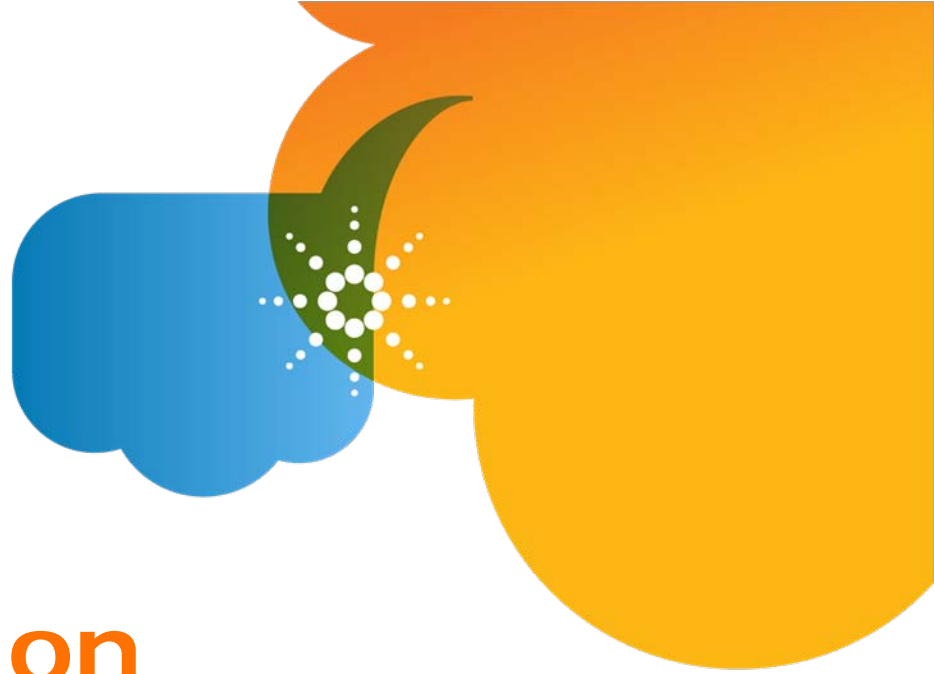
Modem War Dialing
(Sandstorm Phonesweep)

Firewall Assessments



Security Evaluation Program: *Roles & Responsibilities*





Security Evaluation Programs



SEP: Website Compliance Program

Program Component		
Scope of Coverage	Externally-Facing Websites	Externally-facing websites, which are not associated with application in corporate portfolio, hosted within AT&T owned IP space (ongoing)
Inventory Source	Web Site Inventory (WSI)	Homegrown tool developed and supported by security
Control Points	8 Security Frames (based on OWASP Top Ten)	Authentication, Authorization, User and Session Management, Data Protection, Data Validation, Error and Exception Handling, Auditing and Logging, Configuration Management
Tests Performed	Automated and Manual	Source Code Scan (Fortify), Web App Scan (QAIInspect), DB Scan (DBProtect), Manual Penetration Testing
Support Organizations	IT Towers and Business Unit Development Teams	After assessment are requested to register in Corporate Portfolio
Frequency of Assessments	One Time	



SEP: Application Compliance Program

Program Component		
Scope of Coverage	All AT&T Owned or Supported Applications	All applications registered in corporate portfolio (MOTS) with focus on PCI and other critical applications
Inventory Source	Mechanized Operations Tracking System	<u>PCI Application List</u> derived from PCI Indicator in corporate portfolio
Control Points	8 Security Frames <i>(based on OWASP Top Ten)</i>	Authentication, Authorization, User and Session Management, Data Protection, Data Validation, Error and Exception Handling, Auditing and Logging, Configuration Management
Tests Performed	Automated and Manual	Threat Model, Source Code Review (Automated via Fortify SCA), Dynamic Web App Scan (HP AMP/WebInspect), DB Scan (Application Security DBProtect), Manual Penetration Testing
Support Organizations	IT Towers and Business Unit Development Teams	Coordinated via CIO Compliance Team for IT Towers
Frequency of Assessments	3x Annually	As part of standing release schedules or 1x/year if no code modifications



SEP: Server Compliance Program

Program Component		
Scope of Coverage	All Servers on the AT&T Network	Pre-Production: new servers and high risk connection requests (ongoing) Production: all servers within AT&T network boundaries
Inventory Source	Unix, Wintel, Self Supported Inventories	Future inventory source will be IT Configuration Management Database (CMDB), made up of Unix, Wintel and Self supported server inventories
Control Points	8 Security Controls – <i>(based on SANS Top 20 Controls)</i>	Configuration Hardware, Monitor Logs, Control Admin Privileges, Control Access, Vulnerability Assessment and Remediation, Account Monitoring and Ctrl, Malware Defense, and Network Ports and Services
Tests Performed	Automated	Tests performed using McAfee Vulnerability Management port scanning tool and Symantec Enterprise Security Manager
Support Organizations	IT and Business Unit System Administrators	
Frequency of Assessments	Daily <i>(Pre-Prod)</i> Monthly <i>(Prod)</i>	Pre-Production: Daily as part of project or request. Production: Monthly as part of network-wide scans



SEP: PC Compliance Program

Program Component		
Scope of Coverage	All PCs on AT&T Network	PCs on AT&T network with brand assigned by IT (ongoing) Includes PCs managed by IT and approved vendors or self-support groups
Inventory Source	Desktop Reporting System (DRS)	Desktop Reporting System (internally developed application)
Control Points	5 Key Controls <i>(Based on Internal Audit Corrective Action)</i>	Patching, Anti-Virus, Disk Encryption, Host Intrusion Protection, and Disk Wiping
Tests Performed	Automated and Manual	Tests performed using McAfee ePolicy Orchestrator, Checkpoint Encryption and manual inputs
Support Organizations	IT (IBM), Amdocs, Business Unit Self-Support Groups	
Frequency of Assessments	Quarterly	



SEP: Modem Compliance Program

Program Component		
Scope of Coverage	All Modems on AT&T Network	Includes all modems identified within AT&T network (ongoing)
Inventory Source	Corporate Telecommunications Services	Supplemented with findings from war dialing efforts
Control Points	Vendor Default Tests	Developing AT&T compliance framework to drive testing
Tests Performed	Automated	Phonesweep scans conducted
Support Organizations	Business Units	
Frequency of Assessments	Annually	



SEP: Router/Switch Compliance Program

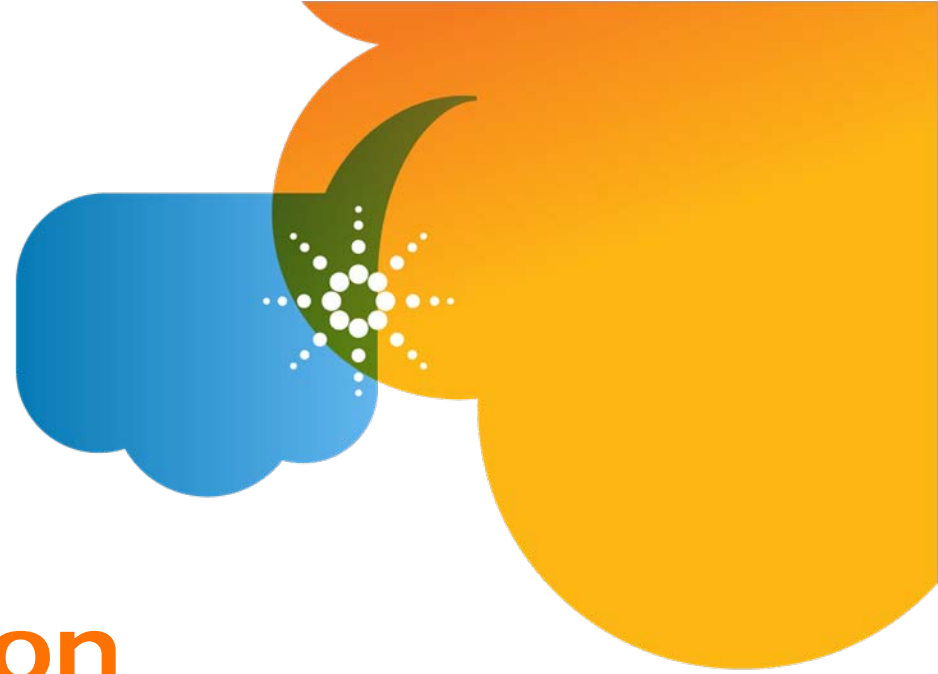
Program Component		
Scope of Coverage	Routers/Switches within AT&T Network	Includes all routers/switches identified within AT&T network (ongoing)
Inventory Source	Network Element Inventory Tool (SMARTS)	Homegrown tool developed and supported by IT Network Services (Supplemented by CSO rouge device discovery process)
Control Points	Vendor Default Tests	Drafting AT&T compliance framework to drive testing
Tests Performed	Automated	Using Alterpoint Network Authority Tool
Support Organizations	IT Network Services	
Frequency of Assessments	Quarterly	



SEP: Firewall Compliance Program

Program Component		
Scope of Coverage	All Firewalls within AT&T Network	New access requests: as they are provisioned Existing firewall rulesets: as identified as over risk threshold
Inventory Source	Firewall System (NOVA)	Homegrown tool developed and supported by security (Supplemented by non-CSO managed firewall discovery process)
Control Points	Firewall Access Risk Vectors	Traffic Source, Traffic Destination, Service / Protocol, Directionality, Size & Scope
Tests Performed	Automated	Risk evaluation rules built into provisioning system (eFORC) and connections rated: Low / Medium / High
Support Organizations	Security Access Control Team	
Frequency of Assessments	Real-Time <i>(new firewall access requests)</i> Annually <i>(existing firewall rulesets)</i>	

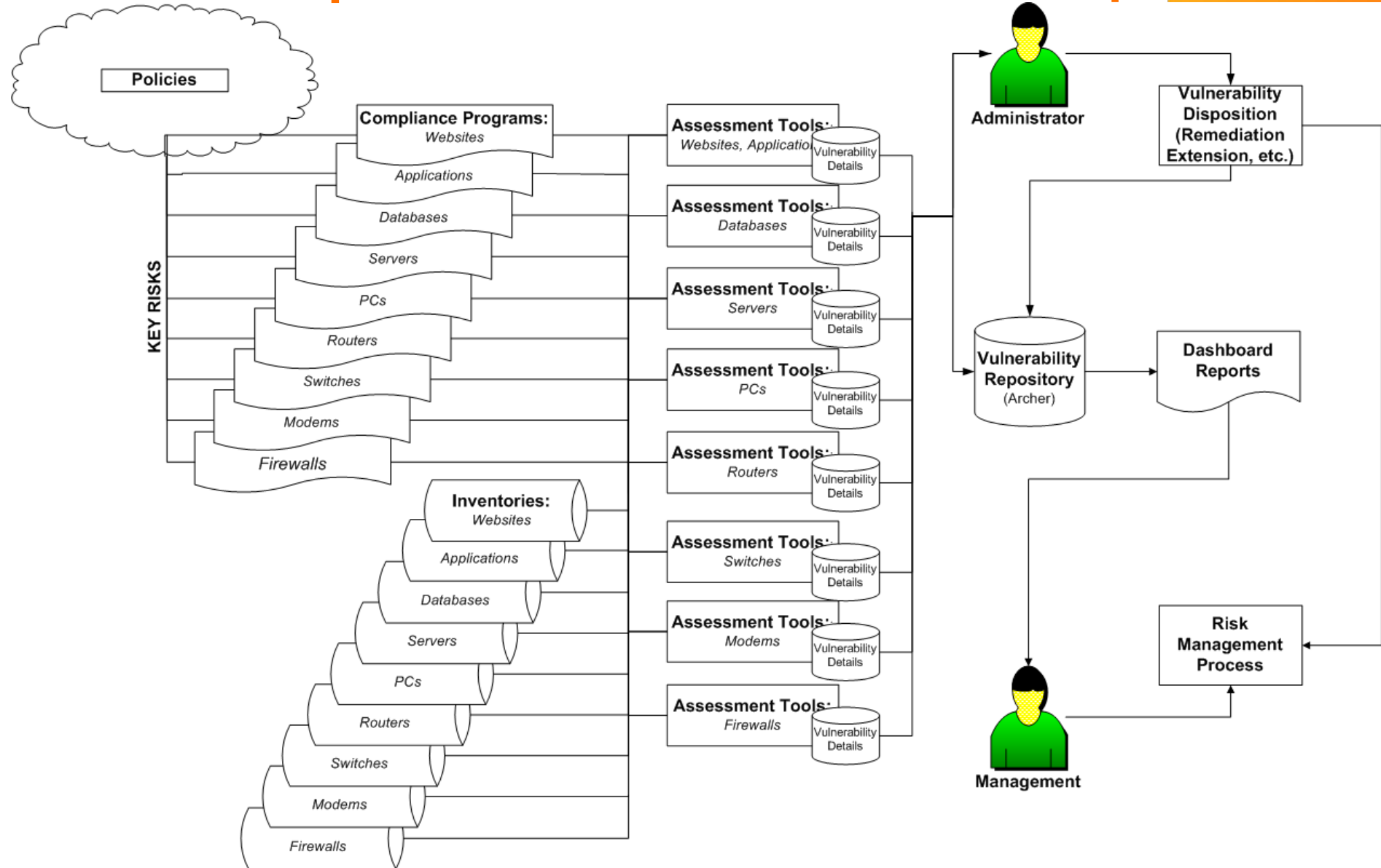




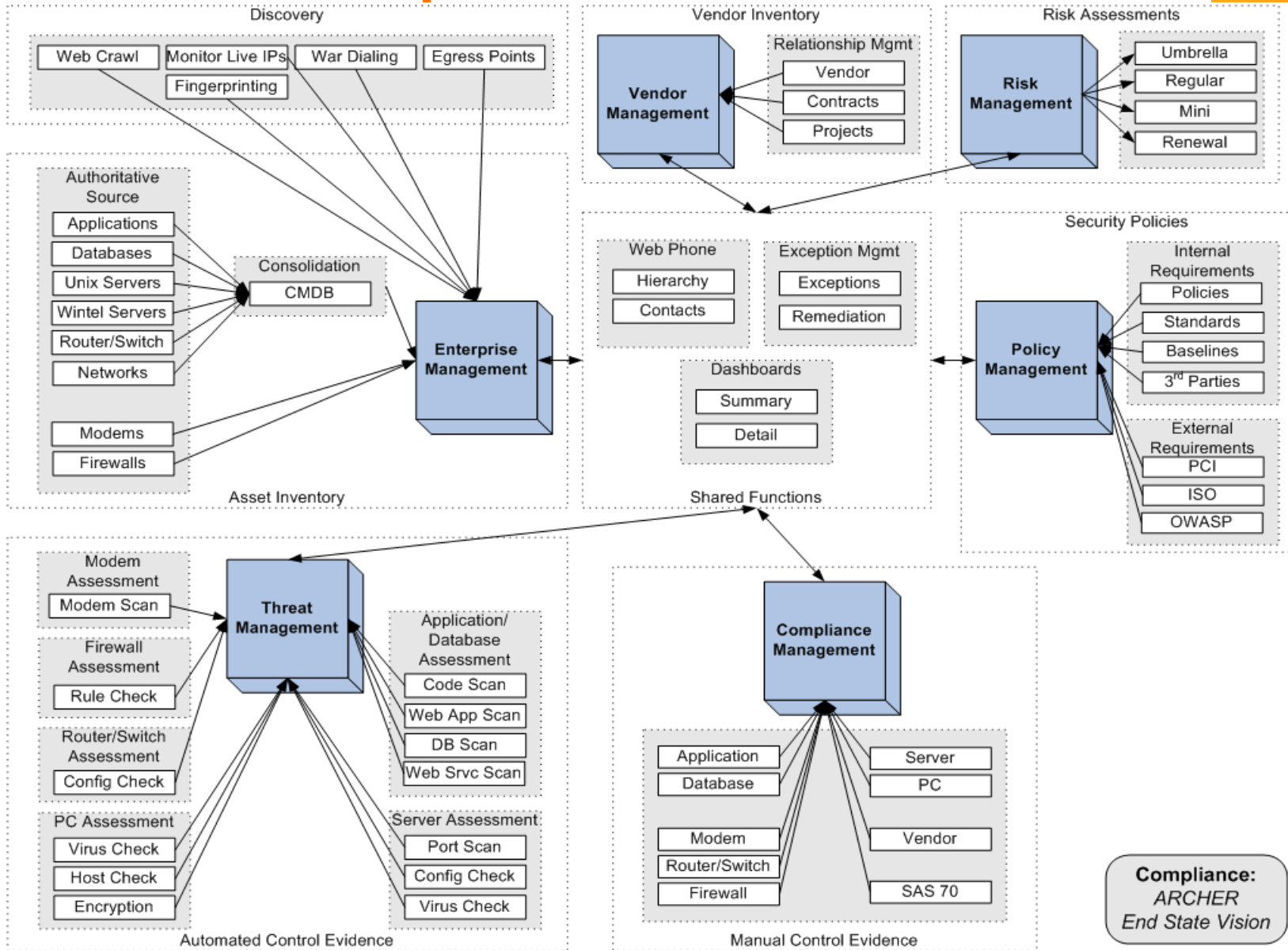
Archer Automation



CSO Compliance: Short Term Roadmap



Archer: Compliance Vision



Compliance:
ARCHER
End State Vision

