

# AT&T Application Security Program

*Ron Bolin, Lead Member  
Technical Staff*

*Rebecca Finnin, Director*

*Ron Williams, Lead Member  
Technical Staff*

Rethink Possible 



# Agenda

- Compliance Management
  - Security Evaluation Program (SEP)
- Application Security Program
- Test Steps
  - Threat Modeling
  - Static Analysis (Automated or Manual Code Review)
  - Dynamic Analysis (Automated Scanning)
  - Manual Penetration Testing

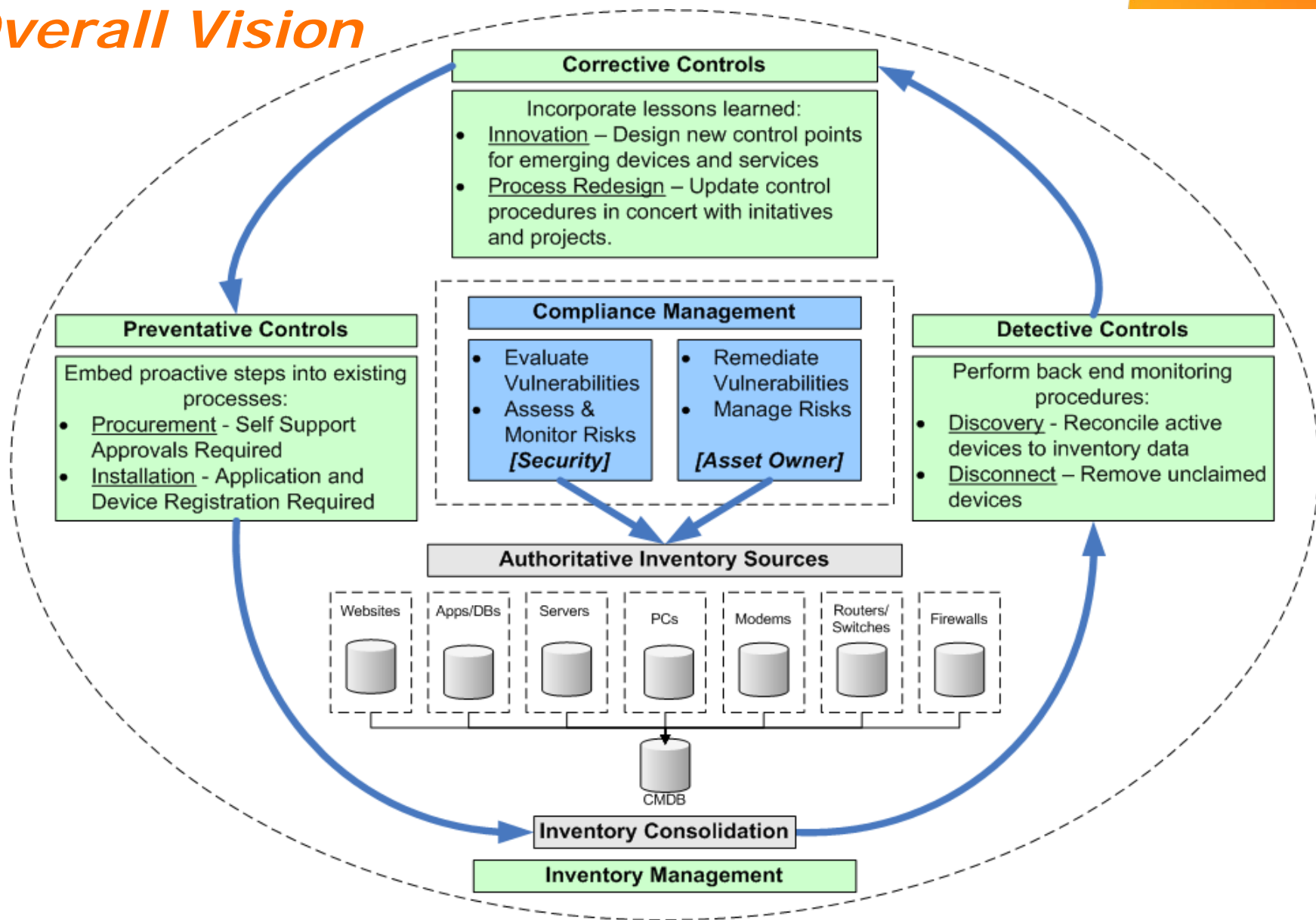


# Compliance Management

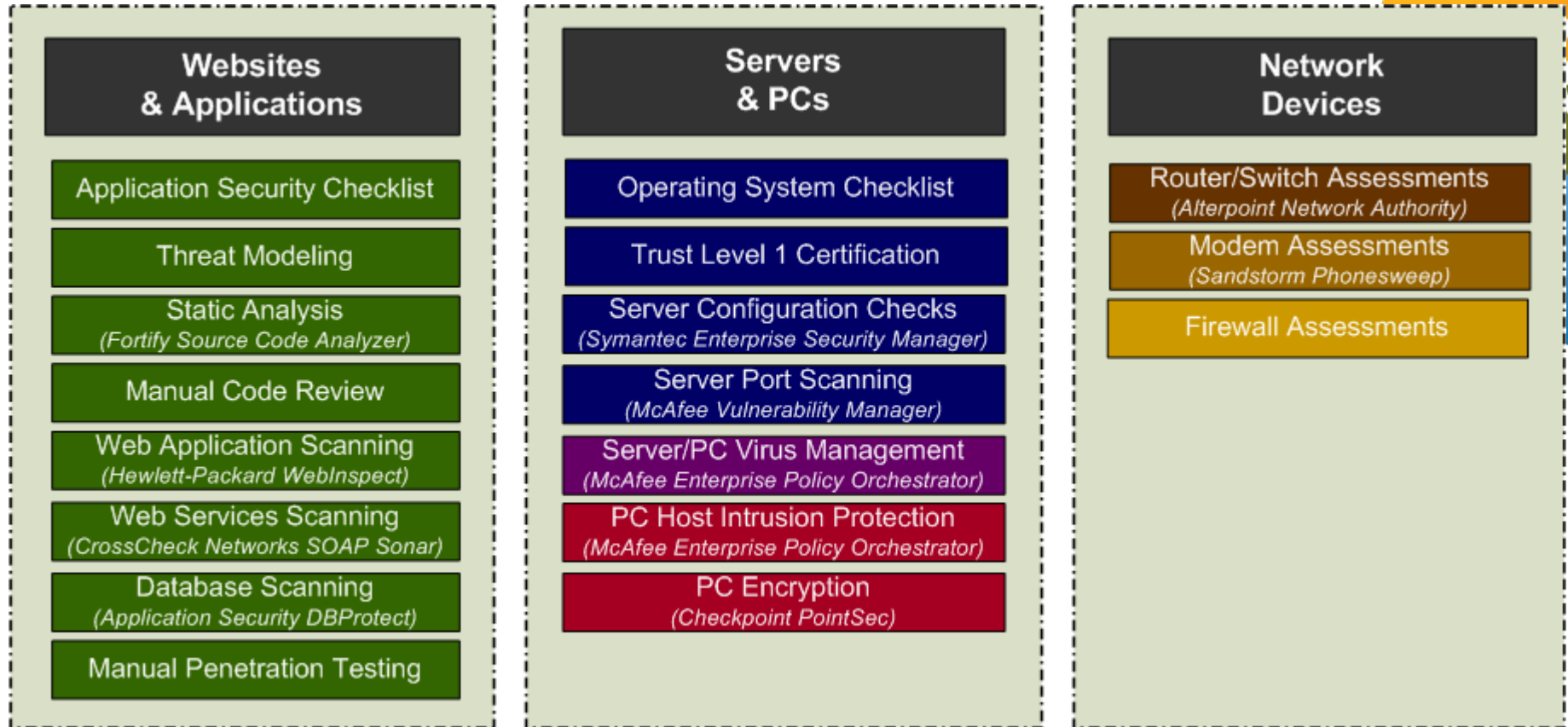
Security Evaluation Program (SEP)



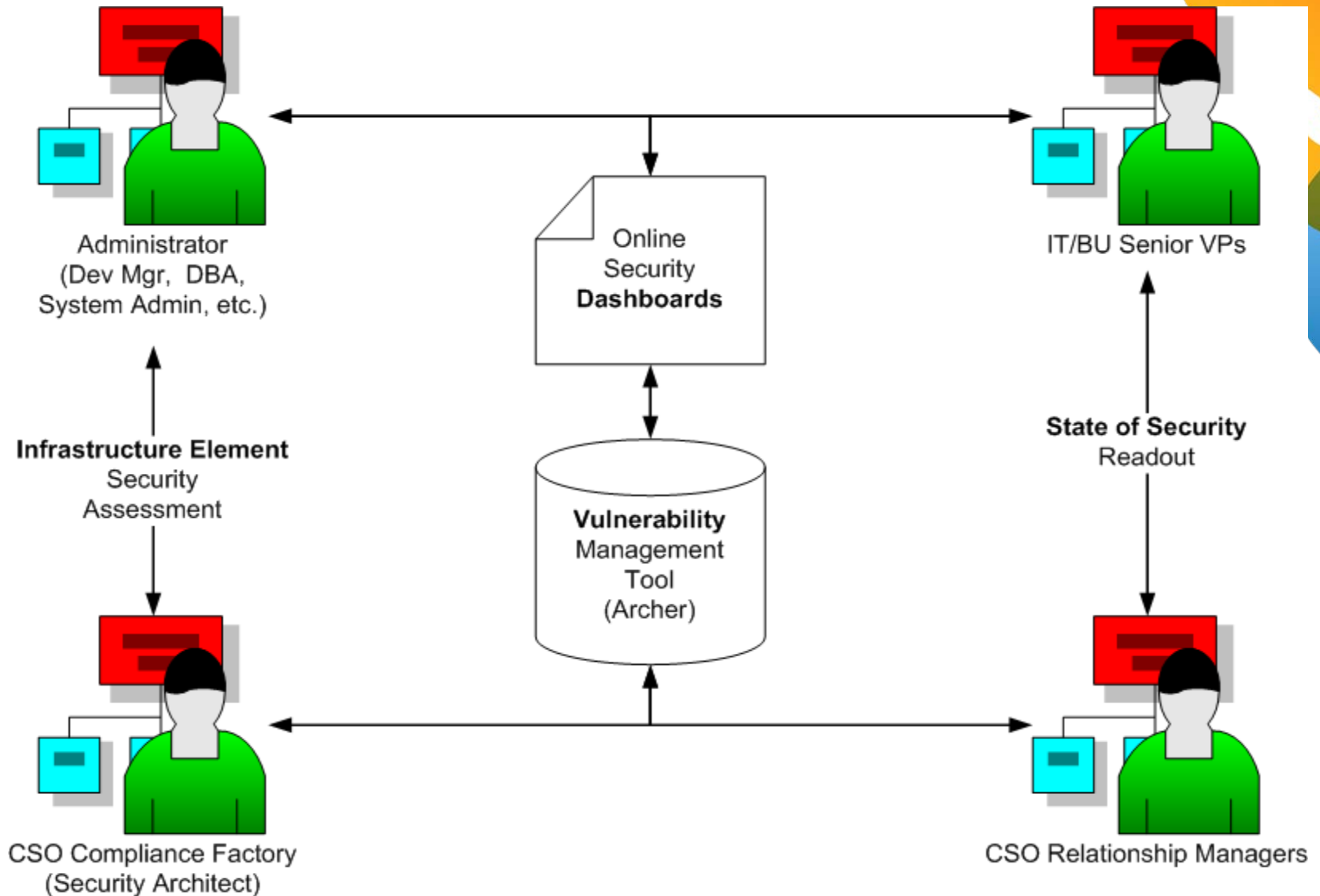
# Security Evaluation Program: Overall Vision



# Security Evaluation Program: *Methodologies & Tools*



# Security Evaluation Program: *Roles & Responsibilities*



# Application Security Program

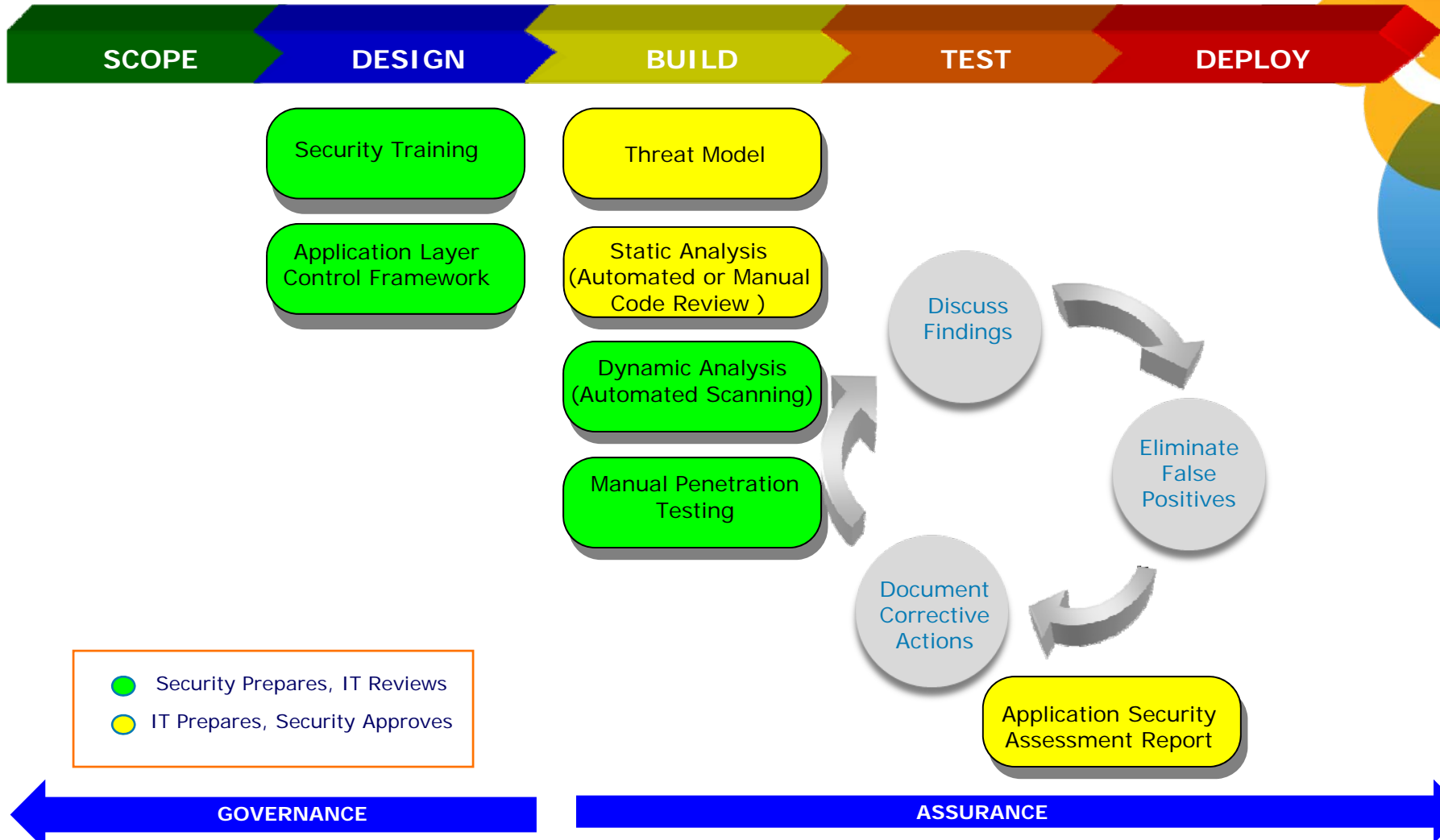


# Application Security Program: *Development Focus*

- Information Technology Unified Process (IT UP)
  - AT&T IT system development lifecycle
  - Updated to includes security activities in 2008
  - Security methodology available to all application development projects
  - Security testing initially mandated for projects involving Payment Card Industry (PCI) applications
  - Currently includes high risk applications: PCI, customer-facing, etc.



# Application Security Program: Major Activities by SDLC Phase



# Application Security Program: *Methodology*

## •PEOPLE

- Security Liaison [IT or Business Unit Development Team]
- Security Analyst [IT or Business Unit Development Team]
- Security Architect [Chief Security Office]

## •PROCESS

- Develop Threat Model [New Applications]
- Conduct Static Analysis [Automated or Manual Code Review]
- Conduct Dynamic Analysis [Automated Scanning]
- Conduct Manual Penetration Testing
- Compile Security Assessment Report

## •TECHNOLOGY

- Fortify [Automated Code Review]
- WebInspect [Web Application Scanning]
- DBProtect [Database Scanning]
- SOAP Sonar [Web Services Testing]



# Application Security Program: *Application Security Assessment Report*

- **Final Report on Application Security**
  - Consolidates findings from all detail testing
  - Captures remediation plans and closure dates for vulnerabilities
  - Contains metrics for application compliance program
  - Includes signoff by development and security team personnel
- **Provides readout on compliance with:**
  - AT&T Security Policies and Requirements
    - Customer-facing vs. internal application requirements
    - Platform specific requirements (mobile device, etc.)
  - Open Web Application Security Project
    - OWASP Top Ten Risks
  - Payment Card Industry Data Security Standards (PCI DSS)



# Application Security Program: Training Courses

Course Name	Course #	Hrs	Description	Audience
<b>Application Data Security Awareness</b>	51340537	1	Introduces common security vulnerabilities in applications.	All Personnel <i>(Security Liaison, Security Analyst, Developer, Tester)</i>
<b>Secure Coding Practices</b>	51381140	1	Identifies security vulnerabilities in code and provides strategies to avoid common programming pitfalls.	All Development Personnel <i>(Security Analyst, Developer)</i>
<b>Secure Code Review</b>	51340473	1	Describes the analysis of application source code to help to ensure the utilization of general security principles and evaluate the adequacy of countermeasures for known threats.	All Development Personnel <i>(Security Analyst, Developer)</i>
<b>Secure J2EE Deployment</b>	51340536	1	Details the J2EE secure deployment checklist suggested by Security.	All Development Personnel <i>(Security Analyst, Developer)</i>
<b>Threat Modeling</b>	51340472	1	Details the Threat Modeling process used by Security.	Development Personnel with Security Responsibilities <i>(Security Analyst)</i>
<b>Static Analysis Methodology</b>	51340471	1	Details the Static Analysis process used by Security.	Development Personnel with Security Responsibilities <i>(Security Analyst)</i>
<b>Fortify Audit Workbench (AWB)</b>	60071047	1.5	Details how to utilize the Fortify® Source Code Analysis Software supported by Security.	Development Personnel with Security Responsibilities <i>(Security Analyst)</i>



# Test Steps



# Application Security Testing: *Threat Modeling*

- Structured representation of information that affects the security of an application
- Process for capturing, organizing, and analyzing application information
- Enables informed decision-making about application security risk
- Produces a typical threat model
- Produces a prioritized list of security improvements to the application concept, requirements, design, and/or implementation



# Application Security Testing: *Static Analysis (Code Review)*

- Secure code static analysis performed using Fortify Source Code Analyzer (SCA) tool
- Development team runs code scan, validates results and draft remediation plans
- Results of code review uploaded to Fortify 360 server
- Security team reviews source code results and approves deliverable



# Application Security Testing: *Dynamic Analysis (Automated Scanning)*

- Performed in pre-production/staging environment
- Security personnel run several types of scans:
  - Web Application Scanning [WebInspect]
  - Web Services Scanning [SOAP Sonar]
  - Database Scanning [DBProtect]
- Development team validates results and draft remediation plans
- Security team reviews scan results and approves deliverable



# Application Security Testing: *Manual Penetration Testing*

- Security personnel perform manual test using standard web browser and web proxy client
- Walk through normal application functions and transactions
- Attempt application attacks including intercepting server responses, editing client requests, etc.
- Development team validates results and drafts remediation plans



# SEP: Application Compliance Program

Program Component		
<b>Scope of Coverage</b>	All AT&T Owned or Supported Applications	All applications registered in corporate portfolio (MOTS) with focus on PCI and other critical applications
<b>Inventory Source</b>	Mechanized Operations Tracking System	<u>PCI Application List</u> derived from PCI Indicator in corporate portfolio
<b>Control Points</b>	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
<b>Tests Performed</b>	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
<b>Support Organizations</b>	IT Towers and Business Unit Development Teams	Coordinated via CIO Compliance Team for IT Towers
<b>Frequency of Assessments</b>	3x Annually	As part of standing release schedules or 1x/year if no code modifications



# QUESTIONS?

## **Ron Bolin**

Lead Member of Technical Staff

[Ron.bolin@att.com](mailto:Ron.bolin@att.com)

770.633.3132

## **Rebecca Finnin**

Director

[Rebecca.finnin@att.com](mailto:Rebecca.finnin@att.com)

678.893.1762

## **Ron Williams**

Lead Member of Technical Staff

[rwilliams@att.com](mailto:rwilliams@att.com)

678.313.7940

