



Software Assurance Forum

# DTCC Software Security Program

*Ajoy Kumar, DTCC*

12 March, 2010



# The Challenge in 2005



- **Background:** The Depository Trust & Clearing Corp (DTCC) had 450 application developers on shore and over 100 offshore creating product for their brokers, bank, mutual fund and insurance carrier customers. DTCC needed to implement improved security practices as part of the application development process. The goal was to create more *secure* applications to handle clearance and settlement of more than **\$1.8 Quadrillion worth of securities transactions each year**
- **Context:**
  - CMMI Level 3 Certified development organization
- **Dilemma:**
  - What is the best approach to improving the resiliency of software developed, outsourced or bought?



# The Goals

## Steps

- Start with Education Program
  - Start Small
  - Develop a Curriculum
- Set up a Application Security Policy
- Integrate Security Controls in Enterprise processes
  - Start with Opportunistic mode (Gate Keeper Controls)
  - Refine
- Automation (Static and Dynamic tools)
- Strong Governance
- Communication
- Dash Board

## Objectives

- The primary focus of the Software Security Program is to teach developers how to develop secure code
- Enhanced SDLC requiring security deliverables and controls at every phase of the lifecycle
- Designed a curriculum for a core team of highly skilled developers to teach them about security and then tested them
  - 18 selected for the program, 16 passed the test
- Selected vulnerability scanning tools (static code analysis, black box testing, integrated vulnerability reporting, and service firms for pen testing)
- Changed the model for CIS support



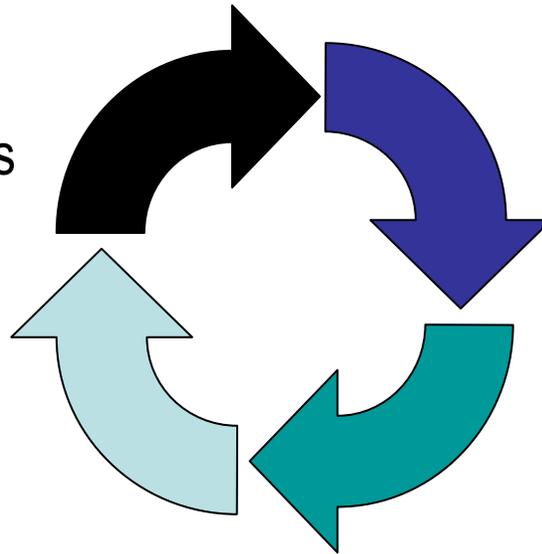
# Four Primary Areas of Focus

## Policy

- App Sec Policy Development
- App Sec Control Standards
- Secure Coding Guidelines

## Automation

- Deep Source Analysis
- Penetration Testing
- Vulnerability Assessment
- Metrics / Trending
- Reporting



## Process

- Security Requirements
- Threat Modeling
- Test Planning
- Stage Gate, PSA, CIS support, Work flow

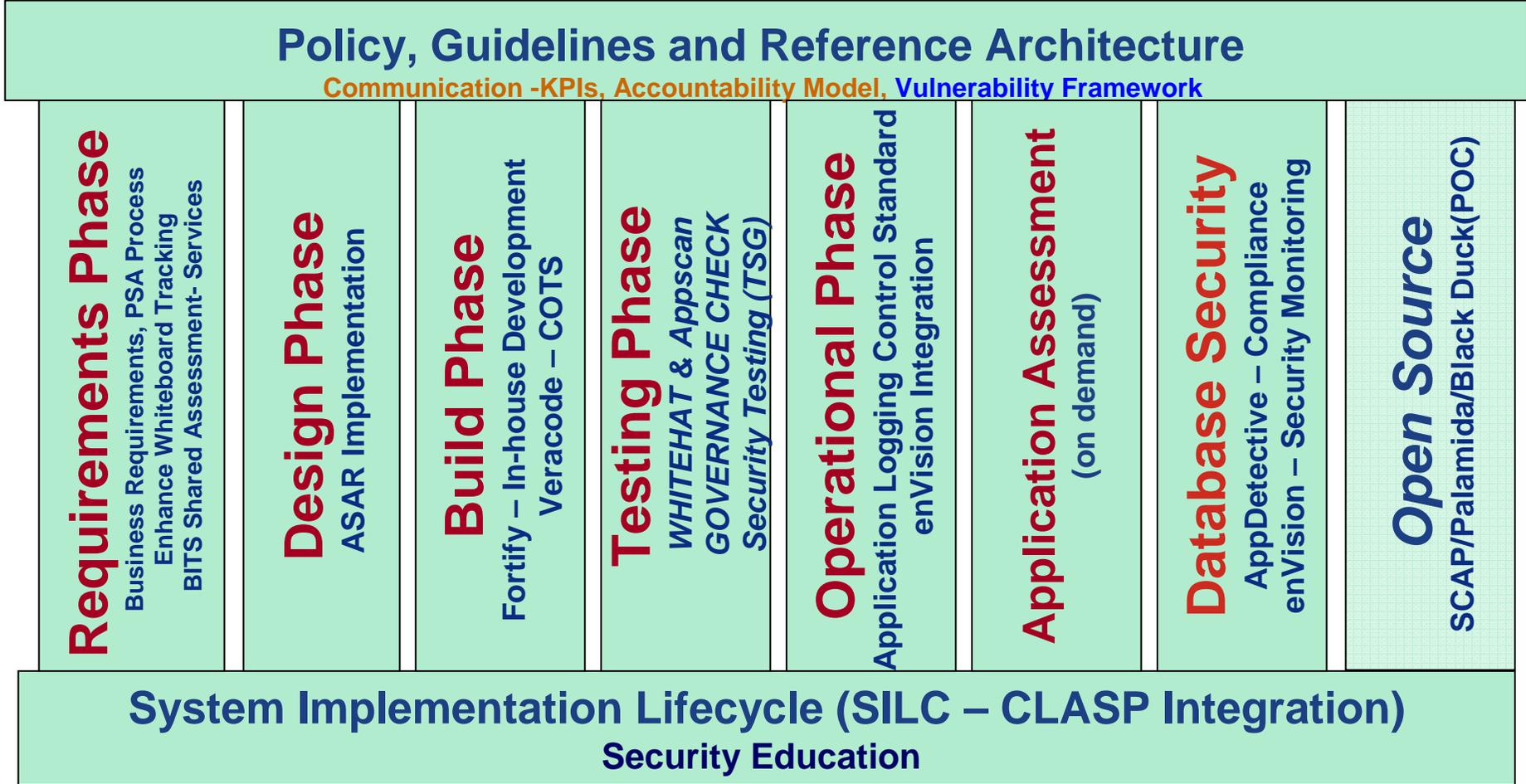
## Training

- Security Awareness
- Remediation for Developers
- Role Based Security Process
- Tool integration



# DTCC's Software Security Program

## 10 Core Control Points





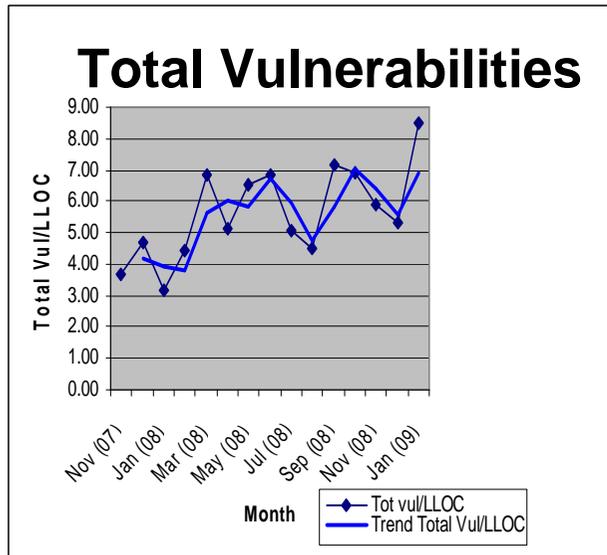
# DTCC's Software Security Program KPIs

SOFTWARE SECURITY DASHBOARD						
Senior Management Monthly Updates						
<b>Requirements Phase</b> PSA Processing SLA Improved PSA All projects filing PSA Whiteboard Session KPI	<b>Design Phase</b> ASAR process performed	<b>Build Phase</b> % code Analyzed, % High, Med and Total Vulnerabilities, % project > 10 NVS %High marked Not an Issue, % of Exceptions, % Vendor products with SSM controls	<b>Testing Phase</b> Projects scanned with WhiteHat Projects scanned with Appscan Security Testing (TSG)	<b>Operational Phase</b> Projects meeting ESM Control	<b>Application Assessment</b> Remediation of High Risk Vulnerabilities	<b>Database Security</b> % database in compliance – DB Protect Number of Database rules triggered
Monthly Team Leads meeting , Monthly Security Mavens meeting Monthly Educational Postings						

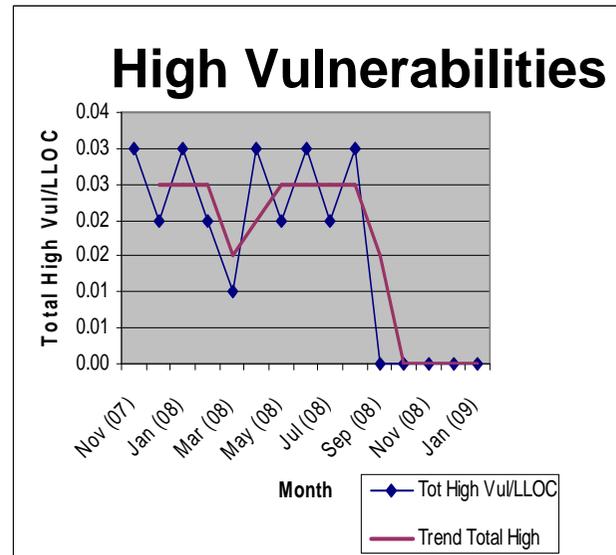




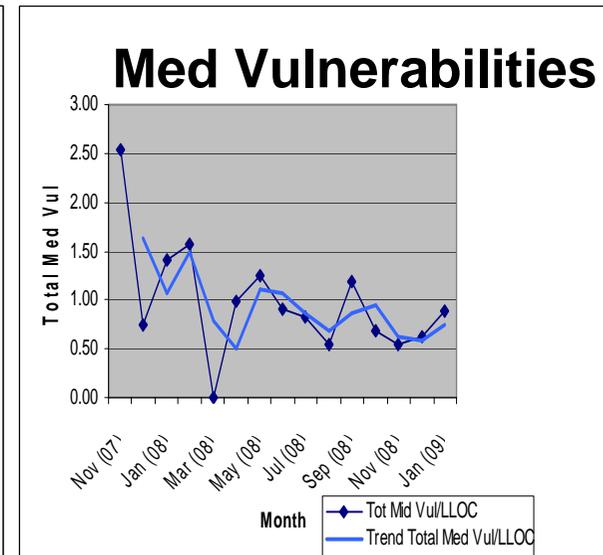
# KPI Analysis (Static Code)



slight **Upward Trend**



**Downward Trend**



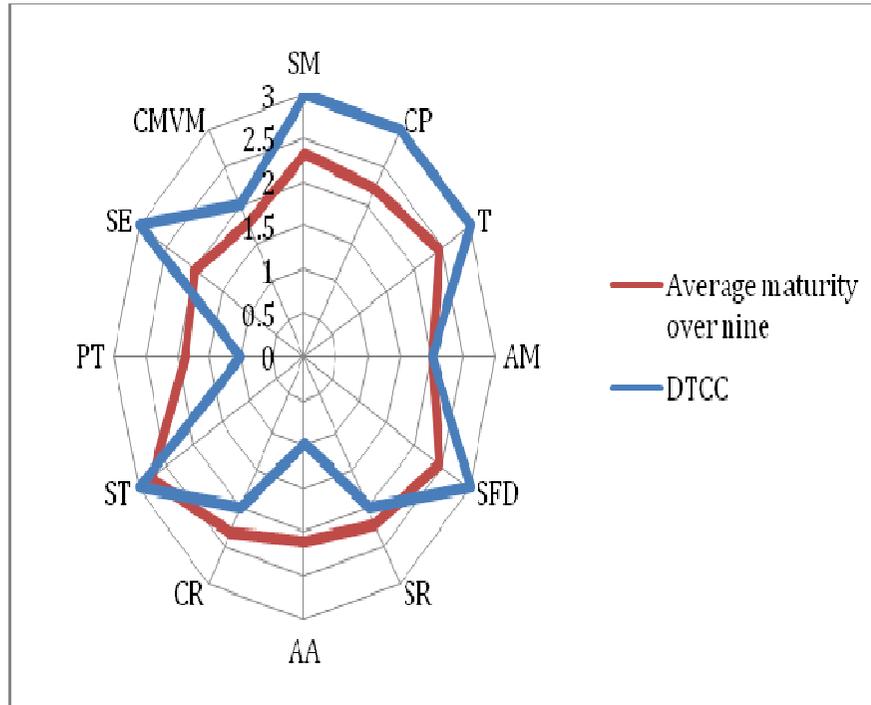
**Downward Trend**



# Lessons Learned

1. A comprehensive program requires more than tools and needs to be layered
2. Education of application developers is essential
3. The work effort supporting the implementation of controls is more like a behavioral change project than a systems integration project
4. Linking vulnerability results with an accountability model that is visible drives changes in behaviors
5. Security requirements must be explicit not implicit
6. Teaching developers how to “break” applications is hard
7. There is economic value in remediation of vulnerabilities, not in identification

# BSIMM- DTCC Maturity Level



DTCC leads industry in all practice areas with the exception of

- Penetration Testing (by design)
- Architecture Analysis

Behavior change is tough process... Value, Productivity and Cost Savings are natural outcome