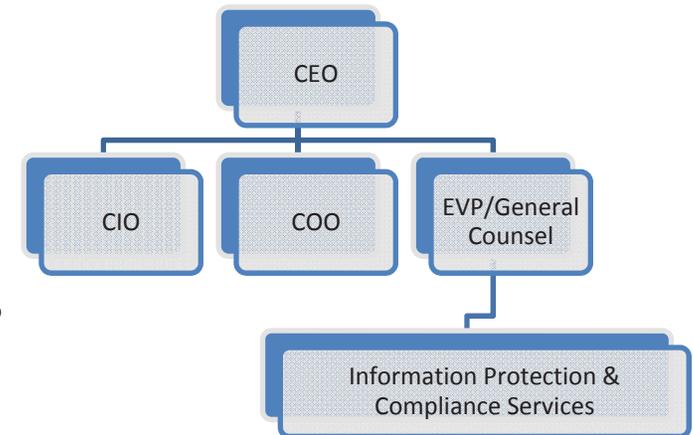


Information Security Program

- Overall responsibility for managing the Information Security Management System (ISMS) to include policy, process, and procedures and technology controls across the enterprise.
- Additional Responsibilities: Internal Operations and IT Audit, Operations and IT Compliance (legislative and industry), Risk Management, Investigative/Incident Response, and Business Continuity



Information Protection Services

Information Security Program

- Certifications from staff include: CISSP, CISM, CISA, PMP, CRISC, ITILF, ISO 27001 Lead Implementer, NSA IAM, NSA IEM
- Staff has IA education and training including:
 - NSTISSI-4011: National Training Standard for Information Systems Security (INFOSEC) Professionals
 - CNSSI-4012: National Information Assurance Training Standard for Senior Systems Managers
 - CNSSI-4013: National Information Assurance Training Standard For System Administrators (SA)
 - CNSSI-4014: Information Assurance Training Standard for Information Systems Security Officers
 - NSTISSI-4015: National Training Standard for Systems Certifiers



Information Security Program

- Information Security policies and standards are reviewed and updated annually with approval from executive management and are based on:
 - ISO/IEC Standard 27002:2005
 - Payment Card Industry (PCI) Data Security Standard, Version 3.0
 - Payment Application Data Security Standard, Version 3.0
 - FFIEC IT Examination Handbook – Information Security
 - NIST SP 800-53 r4 - Generally Accepted Principles and Practices for Securing Information Technology Systems
 - IRS Publication 1075
 - US Department of Energy Cyber Security Program Media Clearing, Purging, and Destruction Guidance: DOE CIO Guidance CS-11, January 2007
 - Health Insurance Portability and Accountability Act of 1996 (HIPAA) and HITECH
 - Gramm-Leach-Bliley Act (GLB), November 12, 1999
 - North American Electric Reliability Corporation Critical Infrastructure Protection Cyber Security Standards 2003-01-01
 - Fair and Accurate Credit Transactions Act of 2003

- We currently maintain the following external certifications and attestations:
 - PCI DSS
 - PA DSS
 - SSAE 16 SOC 1, Type 2
 - REG AB 1122
- We have an active internal audit program to cover Finance, Operations, IT, Security, and Development

Addressing Standards

Safeguards Technical Assistance
Protecting Federal Tax Information (FTI) in Web Portals



Important Guideposts

- Solution is not taxpayer-facing
- Three-tiered architecture
- Crypto (storage and hashing) used is FIPS 140-2 compliant

Certification Testing & Evaluation

- Modified program designed to test the application against existing standards and baselines
 - Program managed by Information Security
- CT&E contrasted against full C&A

Computer Controls Testing

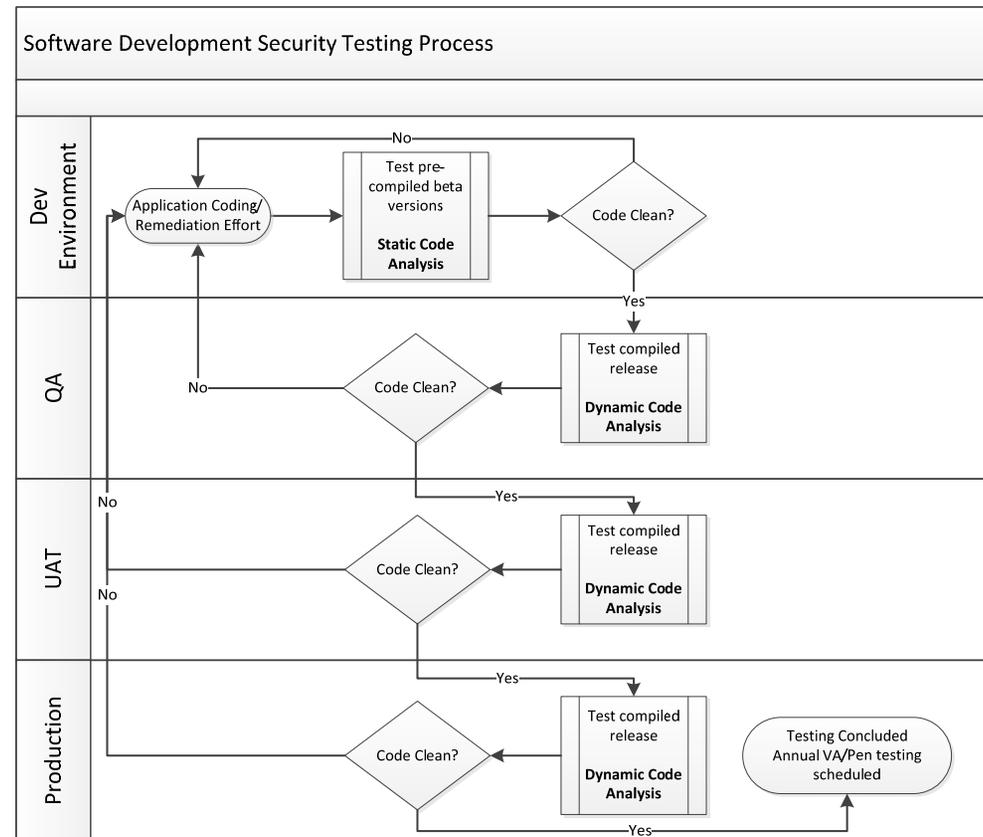
- VA and hack testing at the network and host level protects development environment
- Application testing assures us of code and design free of exploitable vulnerabilities

What	As Needed	Quarterly	Annually	3 rd party
Internal Vulnerability Assessment	✓	✓		
External Vulnerability Assessment		✓		✓
Internal Penetration Test			✓	✓
External Penetration Test			✓	✓
Web Application Vulnerability Assessment	✓			
Web Application Penetration Test	✓			
Dynamic Code Review	✓		✓	✓
Static Code Review	✓			✓

Computer Controls Testing Calendar

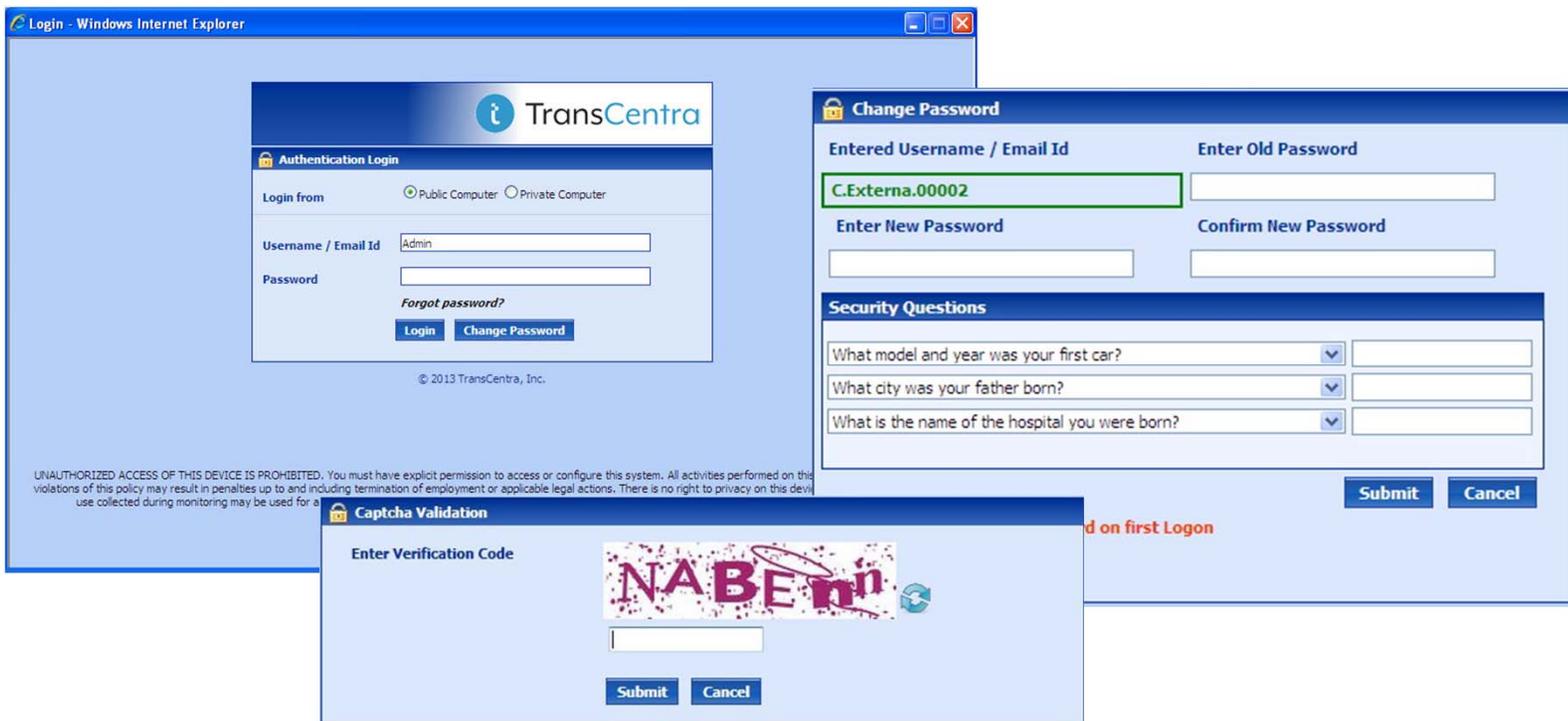
Security Development Lifecycle

- Test web applications at various stages of the product lifecycle:
 - Applications tested in four ways (all include OWASP):
 - Static: During the code development process
 - Dynamic: UAT/QA & Prod
 - Minimum Annual Web Penetration tests
- Providers of third-party code used with TMS contractually required to perform the same tests
- Secure Coding Training



Strong Identity Verification and Banner notification

- Further integration with traditional multi-factor authentication products (RSA, etc.) if needed



The image displays three overlapping screenshots of the TransCentra web portal interface:

- Authentication Login:** Shows a login form with fields for Username / Email Id (containing "Admin") and Password. It includes a "Login" button and a "Change Password" button. The page also features a "Forgot password?" link and a copyright notice for 2013 TransCentra, Inc.
- Change Password:** Shows a form with fields for Entered Username / Email Id (containing "C.Externa.00002"), Enter Old Password, Enter New Password, and Confirm New Password. It also includes a "Security Questions" section with three dropdown menus and input fields for questions like "What model and year was your first car?".
- Captcha Validation:** Shows a form with a field for "Enter Verification Code" and a CAPTCHA image displaying the word "NABE" in a stylized font.

Additional text visible in the screenshots includes "UNAUTHORIZED ACCESS OF THIS DEVICE IS PROHIBITED..." and "on first Logon".

Safeguards Technical Assistance for Protecting Federal Tax Information (FTI) in Web Portals

How we got there

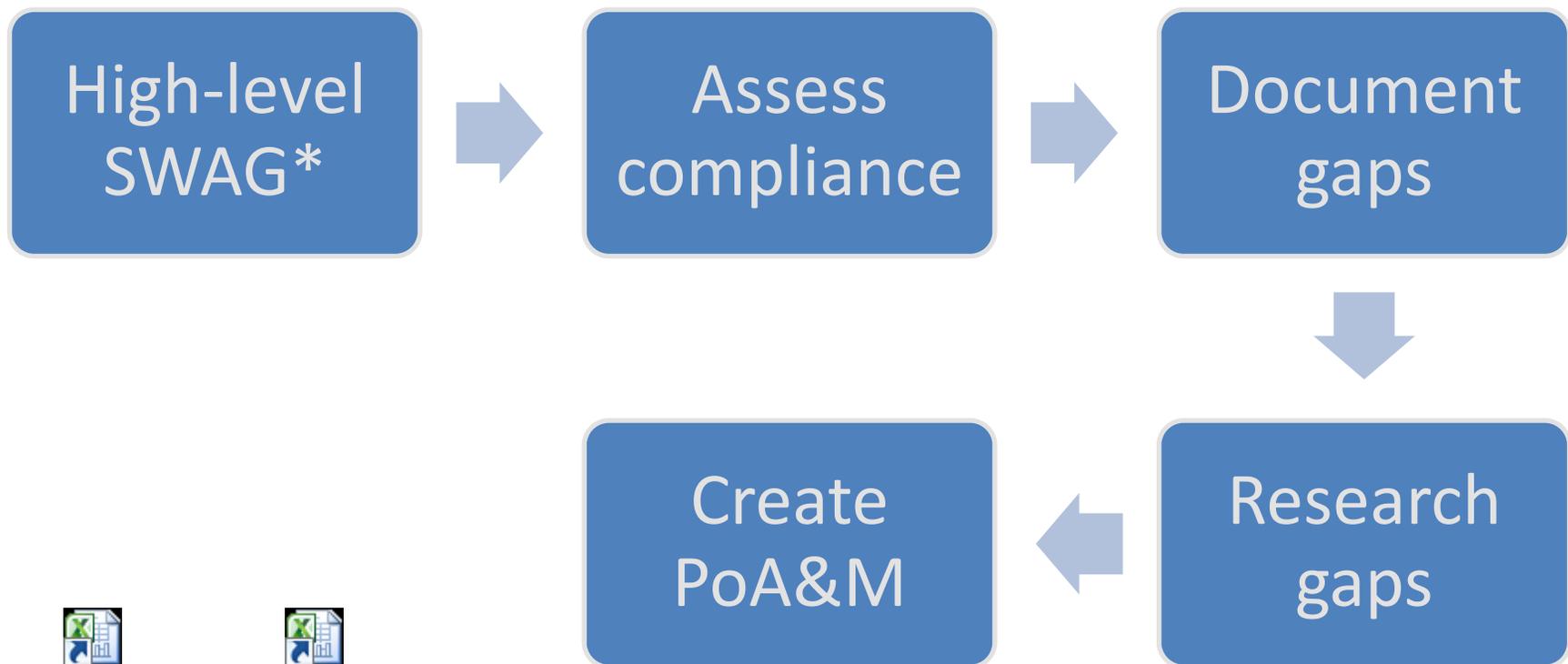
Supporting IRS Pub 1075



Step 1: Read & Understand

- IRS Pub 1075
 - § 4, 9 for controls
 - § 2, 3, 6, 7, and appendices for support of client
- NIST SP 800-53 (r4a)
 - 1075 identifies 18 sections of 800-53 as applicable
 - 147 subsections from those 18
 - Multiple controls within each of the 147
- Safeguards Technical Assistance for Protecting Federal Tax Information (FTI) in Web Portals
- STIG
- CIS Benchmarks

Step 2: Perform gap analysis



IRS
worksheet_blank



TransCentra
Worksheet AppSe

*Scientific Wild-Ass Guess

Step 3: Implement changes

- Gain funding – Important first step
- Incorporate funded changes into code
- Test (security & user)
- Finalize and commit to final dot release

Questions?