IRS Submission Processing Program Strengthens IT Security through dedicated, holistic security engineering & FISMA services

Customer Case Study

The IRS Integrated Submission and Remittance Processing Program (ISRP) processes greater than $1 Trillion in revenue per Tax Year.

Integrated Submission & Remittance Processing Program (ISRP)

- IRS Mission Critical System
- 6 Geographically dispersed Service Centers
- 2 Testing Facilities
- 1 Development Environment
- 300 + Servers, 7000 + Workstations, 5000 + End users

Business Challenge:

• Comply with FISMA as required law & implement numerous enterprise security requirements in a diverse architecture

• Learn best practices for improving program-specific operational security to include secure application development, secure architecture, and risk management

Engagement Solution:

• Security 360 LLC's Lead consultant established a FISMA Risk Assessment Service & Architecture Security Review Program which brought a comprehensive and wide range of security expertise and knowledge to help meet and exceed customers many and varied requirements.

• Detailed assessment of security and risk controls identified areas for improvement

• Comprehensive security direction to cover all facets of the program

Business Results:

• Successfully mitigated 100 program level POA&MS

• Simplified compliance for future projects with reusable security assessment methodology

• Integrated over 30 Security and COTS compliance requirements implementation with ZERO impact to production.

Project challenges in engineering, implementing and monitoring Enterprise and FISMA Security requirements.

The Integrated Submission and Remittance Processing (ISRP) is a major application designed to capture, format, and forward information related to tax submissions and remittances in electronically readable formats to downstream IRS systems. When a tax document is received, it is opened and sorted by form type (e.g., Form 1040 and Form 1040A, etc.) by mailroom operations who then forward to ISRP. Any remittances received with a tax document are forwarded and processed for deposit to the Remittance Processing function. In addition, ISRP uses Enterprise File transfer Utility to transfer remittance data to the Remittance Transaction Research (RTR) system.

The ISRP application includes taxpayer data elements and fields from over 200 paper tax forms (i.e. 1040, 1040A, 1040EZ, 1120) and taxpayer checks for forwarding to downstream IRS systems for processing.

ISRP faced a number of security challenges as the system continually had to meet the processing demands of what it is mandated for yet still integrate and implement numerous technical, process, and program security requirements.

Security requirements which had to be implemented needed to be thoroughly developed, tested, and integrated into the ISRP system with minimal to no operational impact due to the sensitivity and criticality of the transactional data which continually flowed through the system and had to be processed in a timely manner.

Challenges at both the program and technical level

- These requirements varied and were continually changing to satisfy evolving regulatory compliance mandates (USGCB, COE, T-NET, Enterprise TACACS+, FIPS, HIDS, GERS, etc.)
- FISMA requirements were large driver for lower level technical security requirements.
- The customer was not always aware of all security requirements (mostly aware of front line requirements such as the Internal Revenue Manual (IRM) which are derived from the higher FISMA and NIST Standards).

Applying intricate, verifiable, and sustainable security controls within a rapid application development environment.

ISRP's development, testing, fielding, and support of several key program specific customized applications was the primary focus and foundation of the program. These applications generated their own security requirements but accounted for only a portion of the security work and requirements levied on the program.

The supporting architectural infrastructure which allowed ISRP custom applications to properly function and process generated a large volume of their own security requirements that were continually evolving due to regulatory compliance mandates and internal security standards. Often these security requirements had the potential to impact all architectural areas that support the primary applications.

Each supporting architectural infrastructure technology component basically required a Security SME in that technology to properly assess and implement the security requirements for that component with minimal impact to dependent applications and processes.

Numerous Application and Architectural Security Requirements

Area	Requirement
Software	SDLC/IRM*/Coding Standards
Servers	System Hardening/IRM
Workstations	IRM/USGCB/Common Operating Environment
Databases	IRM/Reduced functionality/PII reduction, auditing, and security
Network Communications	Authentication/Authorization Accountability/Encryption
Vulnerability Mitigation	Anti-Virus/Host Intrusion Detection/Compliance and Scanning tools integration/Patch Management
Auditing	IRM/Entrust/ArcSight integration

*An IRM is an Internal Revenue Manual which cover Enterprise standards and requirements for a wide range of subjects.

Several challenges were prominent when it came to properly implementing and fielding security requirements for the ISRP system, these include but were not limited to:

- Developing parallel security activities with significant impact to the system
- Limited volume testing ability in localized lab environment
- Number of security changes were sometimes very significant and configuration issues sometimes did not quickly manifest themselves during testing
- Components which required enterprise integration could only be partially analyzed and some limited testing completed but often the program could not conduct full integration testing until hub site deployment
- Timeliness of development and implementation in relation to the projects desire and sensitivity to filing season processing
- SME for all components during development and testing
- Ability to regenerate isolated configuration issues in the was often limited
- Historically ISRP had been a "closed" system but security requirements were pushing for more and more "enterprise" integration

Security 360 LLC's lead IA engineer, well versed in all aspects of security, analyzed, guided, implemented and verified all program security requirements across the entire architecture. Over 30 Security and COTS integration efforts over 3 years were successfully developed, tested, fielded and verified with no impact to critical processing operations. Additionally our consultant led 3 successful SA&A efforts resulting in Authority to Operate each time.