Managing FTI Data Compliance

Addressing Publication 1075
Introduction

Daniel Gabriel, Manager, Security & Privacy
Deloitte & Touche LLP

Daniel has over nine years of experience providing ERP security and control implementation and review services across numerous industry sectors including State and Local Government. He has extensive project management and hands-on experience in global security solution implementations, redesigns, segregation of duties (SOD) analysis, and Governance, Risk and Compliance (GRC) initiatives. In addition to driving ERP security and control solutions, Daniel has experience leading security incident and event management (SIEM), identity and access management (IAM), and data loss prevention and monitoring solutions for Deloitte.

Objectives

- Understand industry trends impacting an agency’s information technology environment
- Learn the top three compliance issues facing agencies today
- Gain insight into how different agencies address common Publication 1075 compliance concerns
Agenda

Current Industry Trends
Evolving Compliance Requirements
Different Approaches to Maintaining Compliance
Questions
Publication 1075

“This publication provides guidance in ensuring that the policies, practices, controls, and safeguards employed by recipient agencies or agents and contractors adequately protect the confidentiality of the information they receive from the IRS.”

* Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, page 12
Current industry trends
The climate state governments face require tax administrators to consider new approaches to managing Federal Taxpayer Information (FTI) data compliance

Current climate… ...yields new trends… ...that create new security concerns.

Uncertainty in revenue collections due to economic conditions
Focus on cost reduction

Increase in agency collaboration and data consumption to better service taxpayers
Shared Services

Further technological innovation
Information sharing

Multiplying avenues of attack
Data leakage

Multiple access channels
Privacy

Compounding risk landscape
Trend 1: Heightened interest in cost reduction

The current fiscal climate is applying increased pressure on already severely limited state resources. Government bodies are continually challenged with identifying methods for further cost reduction which may introduce a new set of risks.

Less funds to allocate to applying the necessary safeguards

Inability to acquire best-of-breed technologies

Reduction in training opportunities for key personnel

Overload of existing personnel

Aggregate of State Revenue and Expenditures by Year

Revenue returned to 2007 levels, however uncertainty prevails.

Expenditures continued to grow throughout recession period and beyond.

State capitals must look for ways to reduce debt incurred during years of shortfall.

Source: US Census Bureau
**Trend 2: Focus on shared services**

With a greater shift toward a shared services model to provide key state services, including information technology, agencies are looking to achieve cost savings through the consolidation effort.

**Basic Shared Service Model**

- **Focus on your agency mission**
  - Core operations
  - “Cheaper than outsourcing” activities

- **Execute non-core activities**
  - Information Technology
  - “Arms and Legs” work

- **Other Agencies**

  - Increased concerns of data leakage
  - Will I see my name or the agency’s in the headlines?

- **Inadvertently becoming non-compliant with federal and state regulations**

- **Will our data be available when we need it?**

- **Possible data integrity concerns**

- **Shared infrastructure makes commingling of data difficult to avoid**
Trend 3: Information sharing
Tax and revenue agencies are continuing to consume vast amounts of information from multiple sources, including federal organizations, with mandates to share with other state agencies.

Challenges from information sharing…

- Complex web of federal and state regulations continue to evolve and challenge agencies to comply with ever more stringent requirements.

- Greater cost associated with acquiring and housing increased amounts of sensitive information.

…actions for agencies.

- A greater need to differentiate between federally sourced and agency owned information.

- Understanding the contents of the organization’s data as well as how sensitive information transverses through the environment becomes critical.

Having a deep insight and understanding of your information will allow the agency to comply with complex data privacy and protection regulations.
Trend 4: Growing complexity of technology
As technology continues to evolve and organizations embrace true service oriented architectures to meet taxpayer demands, tax and revenue solutions will continue to grow in complexity resulting in new, and changes to existing, compliance requirements.

- Avoiding commingling of data becomes increasingly difficult to achieve
- Increased avenues available to access data
- Greater burden on the security and compliance departments to track and monitor FTI
Compounding pressures
The list of outside influences continue to grow putting additional pressures on overly stretched agencies with ever dwindling resources
Result: Increased regulatory scrutiny
As the amount of federally sourced data agencies receive continues to increase, tax and revenue agencies may fall under further scrutiny from the IRS and be held accountable for securing that data

Current climate... ...yields new trends... ...that create new security concerns.

- Compliance regulations continue to evolve and challenge agencies to comply with more stringent requirements
- Complex web of federal and state regulations as well as industry standards
- Increasingly complex regulatory requirements may drive up the cost of maintaining compliance
- A greater need to differentiate between federally sourced and agency owned information
- Complying with stringent privacy requirements
Evolving Compliance Requirements
Evolution compliance requirements
One of the most difficult, yet important, requirements of Publication 1075 pertains to understanding and tracking the various data elements provided by the IRS throughout the organization’s information systems (IS) environment.

Addressing the issues:
- Understand your data
- Document the flow
- Training and awareness
Evolving compliance requirements
Tracking user activity across a complex systems landscape requires a multifaceted approach leveraging a combination of point solutions monitoring each possible avenue of user interaction with the environment.

I. Application Layer
- Monitoring user activity
- Multiple user interfaces

II. Database Layer
- Database activity monitoring
- Privilege user activity
- Pattern matching

III. Network Layer
- Pattern matching
- Network traffic monitoring
- Server scans

III. User Activity Repository
- Consolidated user activity
- Single unified reporting interface
**Evolving compliance requirements**

Understanding and addressing encryption requirements is difficult enough without inconsistent vendor application of industry standards such as the Federal Information Processing Standards (FIPS).

---

**Challenges**

- General lack of deep technical knowledge related to encryption
- Ambiguity and uncertainty in application of standard
- Incompatibility between FIPS enabled products
- FIPS compliance can provide false sense of security through certification

**Considerations**

- Desired “level” of FIPS compliance
- Processing overhead
- Key and certificate management
- Interoperability of FIPS cryptographic modules
- Effect on other applications in the landscape

---

**Approach**

- Consider total landscape
- Understand your data
- Map communication channels
- Assess potential vulnerabilities
Practical Applications
Data Labeling
Two distinctly different approaches to put the pieces together

<table>
<thead>
<tr>
<th>Singular requirement</th>
<th>...two approaches...</th>
<th>...common goal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Addressing the data labeling requirement</strong></td>
<td>Prohibiting outside access to agency data</td>
<td>Protecting taxpayer data</td>
</tr>
<tr>
<td><strong>Granting outside access to agency data</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data Labeling
Organizational Direction – Don’t share our data

Business requirement

Process tax and revenue functions in a secure, closed environment to provide taxpayers with a valuable service including quick disbursements of refunds

Key agency decision

Do not share our data outside the agency

Technology solution

- Restricted access
- Flag the entire environment as IRS sourced data
- Provide labels on the user interface and printed reports

Benefits

- Easier to address labeling requirement
- Less complicated to implement and maintain

Drawbacks

- Inability to realize benefits of data
- Stifles inter-agency cooperation
Data Labeling
Organizational Direction – Share our data

Business requirement
Deliver an integrated tax and revenue solution to support the Department of Revenue’s activities and allow the sharing of agency data to the greatest extent possible

Key agency decision
Share our data outside the agency

Technology solution
- Restricted access
- Identified and mapped IRS data elements throughout the solution
- Third-party validated and rewritten
- Labeled user interface and printed reports

Benefits
- Enabled the ability to share non-protected data
- Increased inter-agency cooperation

Drawbacks
- Complicated to initially undertake
- Requires established data governance
Data Labeling
Key points to remember…

✔ Develop a robust data classification program
✔ Draft supporting policies and procedures
✔ Document the flow of FTI through the environment
✔ Label FTI at the element level
✔ Provide warning notification on user interface
✔ Deliver awareness training
✔ Establish an incident response program
## Monitoring access to FTI
A multifaceted approach to monitoring FTI

### Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited availability of monitoring tools</td>
<td>The components within the solution drive the requirements for data monitoring tools and capabilities</td>
</tr>
<tr>
<td>Agent based solutions</td>
<td>A number of monitoring products available today remotely monitor user activity at the source, the user’s desktop</td>
</tr>
<tr>
<td>Need for multi-layered approach</td>
<td>Traditional application layer monitoring no longer suffices. A concerted monitoring effort is necessitated by complex solution architectures</td>
</tr>
<tr>
<td>Privacy concerns with captured data</td>
<td>Capturing too much information can lead to violations of other standards, publications, or regulations (i.e., PII and PCI)</td>
</tr>
</tbody>
</table>

### Components

- Application level monitoring
- Database activity monitoring
- Data loss protection

- Aggregate and correlate
- Security event monitoring
- Intelligent reporting
Monitoring access to FTI

Key points to remember…

✓ Today’s integrated tax and revenue solutions are highly complex with multiple components

✓ Understand where your FTI resides

✓ Establish a program to continually evaluate incoming and outgoing data flows

✓ Access monitoring should occur at multiple levels

✓ Enable timely and relevant monitoring

✓ Deliver awareness training

✓ Establish an incident response program
Homework
Ask yourself the following questions…

Do we really know our data?

Are we comfortable that the agency understands the flow of sensitive information through the organization?

Are we appropriately protecting our sensitive information?

When was the last time we checked?

Do we have the right relationship with the IRS?
Questions?

Daniel Gabriel
Manager
Security & Privacy
State and Local Government
USA
Tel: +1 704 887 1654
Mobile: +1 704 615 1777
Fax: +1 704 339 5618
dgabriel@deloitte.com

Member of
Deloitte Touche Tohmatsu Limited

Srini Subramanian
Principal
Security & Privacy
State and Local Government Lead
USA
Tel: +1 717 651 6277
Mobile: +1 717 805 0364
Fax: +1 717 412 9677
ssubramanian@deloitte.com

Member of
Deloitte Touche Tohmatsu Limited

Bari Faudree
Director
Security & Privacy
Health Sciences and
State and Local Government
USA
Tel: +1 317 656 2425
Mobile: +1 317 508 2497
Fax: +1 317 453 2613
bfaudree@deloitte.com

Member of
Deloitte Touche Tohmatsu Limited
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2012 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited