Leveraging Technology to Aid Compliance
Lessons Learned in Compliance Automation at NSA

October 2017
JASON MARBURG
MELISSA LIPPLE

Objectives

• Managing Rules and Requirements – Gain a deeper understanding of how to integrate compliance processes based on common knowledge of the legal and policy rules rather than ad hoc procedures based on limited interpretation. This enables organizations to link operational activities to the rules under which they apply.

• Operating Under Multiple Rule Sets – Explore the challenges associated with the complexity and volume of rules in organizations and learn how technology can offer the best option for addressing this increase in scale and complexity.

• Automation Activities – In this area, we will cover automation of rules for business functions, internal controls and monitoring, and compliance activities. Discover the lessons learned from NSA’s perspective, to include challenges and dependencies.
Background

- NSA acquires and produces a range of data/information to support two vital goals – foreign intelligence and information assurance.
- NSA’s activities are both authorized and regulated by the executive branch, Congress, the Foreign Intelligence Surveillance Court, and the Constitution.
- Authorizations and regulations come in many forms, often with distinct procedures.
- Automation is one component of NSA’s compliance program.

Key Challenges

- Many individual authorizing documents with distinct procedures and rules applicable to specific datasets.
- A large workforce performing thousands of daily transactions which must comply with complex rule sets.
- A complex architecture which is used to perform various activities and manage data.

Why Compliance Automation?

Incident Response & Mitigation
- Necessary to address incidents
- Provides feedback loop regarding issues
- Not preventive

Proactive Compliance Program (e.g., training, policy/standards, audits/reviews)
- Provides workforce with critical compliance information
- Audits/reviews may identify incidents or risks
- Removed from the point of a given transaction

Integrated Automation
- Once integrated, provides assurance at the point of a transaction
- Can aid management of complex rule sets
- May be necessary depending upon the amount of sensitive data managed
- Does not replace other components of a compliance program
- Requires a substantial investment in time and resources

Components of a Compliance Program
Submit a Requirement

- Summary
- Traceability
- Timeframe
- Stakeholders
- Use Cases
- Inputs
- Outputs
- Dependencies/Risks
- Assumptions
- Funding
- Scale/Performance

Need
Purpose
Outcomes
Implementation Hurdles

Initial Capability
Final Capability

How We Refine a Requirement

Idea
Scoring & Prioritization
Identify/Review Technical Approach

Sounding Board

Approve Requirement

Submit Requirement

Review Requirement

Begin Agile Development

Systems Engineering

Agile
Lessons Learned in Managing Requirements

- Compliance requirements are most often derived from legal and policy requirements, therefore requiring a higher level of precision in their definition and implementation than other customer-driven requirements.
- Decisions related to compliance requirements need to be defensible and traceable, due to increased scrutiny.
- Procedural vs Technical requirements.
- System changes and the compliance impacts associated with those changes must be well understood and socialized prior to implementation.

Managing Rules Starts with Comprehensive Document Management

NSA’s mission authorities and the rules governing those authorities are contained in numerous types of documents, including:

- Executive Orders
- DoD Directives
- Minimization Procedures
- FISC Orders and Opinions

*Key Principle: Apply best practices from the fields of legal and compliance information management to manage the set of classified documents governing NSA.

Comprehensive Document Management

Provides the basis for support to rules automation

Key Features
1. Conversion to searchable text
2. Categorization and metadata enhance search features
3. Extraction of key information
4. Lifecycle management for rules documents, including
   a. Linkages to related documents which modify or supplement rules
   b. Real-time document status (active, active but amended, expired, superseded, etc.)
Lessons Learned in Managing Rules

• When to initiate a rules management program
  – Use this approach if the number of rules documents makes it impractical to manage via websites or spreadsheets
  – Evaluate possible commercial tools which may be applicable

• Usability
  – Excelling at the basics can get you far
  – Speed is essential if you want business units to rely on it
  – Define a separate process for challenging ad hoc scenarios
  – Extracted machine usable information provides a foundation for further automation

• Accuracy and consistency are critical, otherwise there is a risk of undermining compliance
  – Rely on source information to boost accuracy
  – Guides and training for curators are essential for consistency and speed
  – A mix of manual processes and automation throughout the workflow is sometimes best
Lessons Learned in Data Governance

- Any approach to data governance should be able to answer the following compliance-related questions
  - What is NSA’s authority to have the data?
  - What is the state of the data (to the extent that it impacts the rules)?
  - Where is the data, as well as copies and derived information?
  - What function is the data being used for?

- Consider tagging if you have multiple types of sensitive or regulated data which are not stored and used separately
  - While comprehensive tagging is a substantial investment, the benefits are also substantial
  - This is an essential step to automate compliance for transactions across data under multiple rule sets

- Robust tagging validation is critical for compliance-related tags
Types of Compliance Automation

• **Rules Management Services**
  - Comprehensive Legal and Compliance Document/Information Management
  - Structured Authorities and Rules Information to Support Compliant Mission Activities
  - Management of Compliance-Related Tag Values

• **Rules Automation Services**: Leverage the management of rules documents and compliance-related tags to provide real-time guidance regarding the permissibility of a given transaction or activity. Rules Automation Services are developed to answer key questions for transactions or activities (e.g., can a particular query be used to search data acquired under a particular authority).

• **Technical Control Systems**: Develop and maintain an effective system of automated internal controls to provide reasonable assurance that mission activities are conducted in a compliant manner. Technical Control Systems feature a series of internal controls designed to work together to enhance compliance for particular activities (e.g., review of queries, validation of transactions).

• **Support to Compliance Activities**
  - Incident Management
  - Compliance Monitoring

---

Rules Automation Concept

**Authorities Information to Support Compliant Mission**

Each authority record contains:
1. Basic authority information, including effective and expiration dates
2. Authorized activities
3. Links to relevant documents
4. Authority tags that reference the specific authority and the authority category

**Authority Notifications**: notifications of new authorities, changes, and expirations

*Key Principle*: Leverage management of rules documents and authority-based tags to enhance the evaluation of the permissibility of mission activities

**Example Function**: Users need to determine if query terms can be used to search data governed by each authority according to the authorizing documents and governing rules