Mastering Information Portfolio for Government
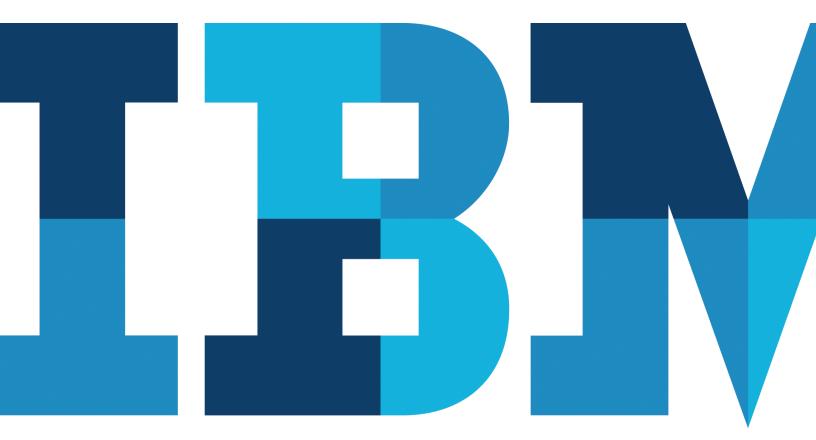
IBM InfoSphere software for trusted information

IBM ®

Contents

Introduction

Information is fundamental to all aspects of government. Whether determining citizen benefit eligibility, granting licenses and visa applications or solving crimes using data culled from multiple departments and agencies, governments are reliant on information management. Mandates to improve information accessibility and transparency, operating efficiency and deliver improved outcomes are the impetus for government to manage information as a strategic resource.

Government is not only one of the largest and longest established organizations but it also produces and manages massive and growing volumes of information from an increasing number of sources for information creation and consumption. The information needs of government are complex and growing in complexity all the time. Government information management is made more challenging with information sharing across agencies, privacy legislation and the public nature and high stakes involved with public safety. The information management needs of government are shaped by executive mandates, regulations, program operations and integrated service delivery.

This paper will discuss the challenges that government organizations face in managing information that must be resolved, shared and trusted in order to address the broad and vital requirements of government:

• To make information sharing a strategic imperative
• To better adapt to the ever changing challenges and threats around public safety
• To operate more efficiently

The paper will explore the strategic information management mandates of linking and sharing, fraud and threat detection and business modernization. In doing so, the paper will describe how IBM InfoSphere software addresses these complex information management requirements.

Government agencies that are mastering information are able to make information sharing a strategic imperative so they can effectively use information in multiple contexts across the agency while also working in collaboration with other agencies. IBM's mastering information portfolio for government enhances the government's ability to meet program and policy commitments to improve public outcomes while responsibly stewarding public information assets and adapting to change.

Government Information Challenges

The growing volume of information that government produces and manages is stored across countless disparate systems both internal and external to government organizations be it local, regional, national or trans-national. Multiple systems of record exist with multiple types of data in different formats and with different purpose and context. The government is challenged to ensure its information assets are complete, accurate, timely and authoritative. Programs need quality, trusted information to function, be effectively managed and to meet the needs of citizens. The importance of public trust, accountability and transparency cannot be overstated – especially concerning the safeguarding of personal information.

Government as an enterprise spans offices, agencies, ministries, departments and jurisdictions. Each government organization

has its own vertical information sharing requirements in order to be able to operate efficiently and respond to public demands, while also needing to share information horizontally across government organizations. Escalating issues of national security, health care and fraud detection require governments to establish programs that may cut across the mandates of several departments, agencies and even jurisdictions. Programs that cross organizational boundaries or integrate service delivery to citizens require trusted information to be presented in the context in which it was created or collected. In addition, detecting and identifying persons consuming integrated government services and aligning information flow across departments is essential for operations efficacy and transparency. At the same time, this sharing of information demands strict adherence to security and privacy regulations.

A multitude of member records from different sources with various attributes make identifying and resolving entities such as persons, organizations, locations and events complex and time consuming. Government requirements for entity resolution are critical in order to provide government services to the right persons, and more importantly to prevent and detect fraud and threats to national security and public safety. Public pressures and high stakes are involved when successfully identifying or correlating information can literally save lives or when failure to correlate and resolve information can be catastrophic.

The extensive information management challenges that government faces not only degrade the quality and timeliness of services and programs but also cause programs to incur unnecessary costs such as increased staff costs and lost productivity on manual data management tasks. Moreover, poor information quality that feeds operational systems translates into inefficient government operations. Government information assets must be organized and managed while the downstream business processes are structured so that government can adapt and accommodate change. The escalating requirement for government to consolidate, transform and modernize legacy information systems and business processes is directly linked to information management.

Smarter Government

The benefits of mastering information for government address the complex and systemic nature of these information challenges by improving essential government services and their underlying business applications. Moreover, governments that are mastering information are able to manage information as a strategic resource and realize its derived benefits. Being able to predict, mitigate and prevent risk guides government's ability to meet program and policy commitments and improve citizen services and public safety.

Above all else, government is ultimately responsible for the economic health, welfare and security of its citizens. Smart governments continually work to improve these outcomes by strengthening national security and public safety, improving citizen and business services, effectively managing resources and ensuring a sustainable environment. Information is the cornerstone to fulfilling these serious responsibilities. Smart governments are turning to information management solutions to:

- Make information sharing a strategic imperative
- Adapt to an ever changing national security landscape
- Modernize and evolve to operate efficiently

National security and public safety mandates are dependent on Intelligence and Law Enforcement having access to and confidence in information to achieve situational analysis and awareness. With access to resolved, trusted identity information Intelligence and Law Enforcement agencies are able to understand the context of who a person is, who they know and what they do.

This knowledge increases both the speed and quality of command or response by successfully identifying and correlating information to save lives and improve public safety. Knowing your threat and the information management demands that enable such knowledge intersect the government services of National Security, Homeland Security, Border Security, Police and Immigration and Customs. Governments benefit from mastering information across each of these

A municipal health and human services agency uses IBM InfoSphere MDM Server to aid citizens in need more quickly by having deployed a holistic information management strategy. The agency wanted to improve the efficiency and competence of its caseworkers. Previously, staff had to access several independent subsystems to gather all of a citizen's pertinent information, delaying service delivery and sometimes overlooking available support programs. The organization launched a program to promote intradepartmental information access.

With support from IBM, the agency launched a common record index that compiles all available citizen data in a single location. Caseworkers can use this system to better manage public services, and citizens can now easily access and update their information online. Furthermore, the solution, built with IBM InfoSphere software, offers advanced analytics tools that help with trend analysis and forecasting future service demands.

essential services by resolving identities, sharing information that is buried in myriad data silos, and searching across the full potential of associated data in a timely manner.

Similar information insights are critical to resolving the identity of citizens and persons and gaining access to a single view of persons, organizations, locations and events for government to meet its monetary and tax related services. Knowing your citizen assists in the prevention and identification and conviction of tax fraud and tax evasion, financial crimes, cyber crimes and identity theft. Moreover, information management and reporting enable government to find and report non-compliance with government regulations.

Social Services and Healthcare government services also benefit from the ability to predict, mitigate and prevent risks associated with the need to verify citizen identity, determine program eligibility, reduce improper payments and detect member or provider fraud. Knowing your client in these cases improves citizen and business services by connecting people to programs based on individual needs while reducing operational costs and maximizing taxpayer value.

Smarter governments are mastering information not only to improve these and other core government services and their underlying business processes; but also, to realize the derived benefits from information assets that are complete, accurate, timely and authoritative.

Information management enables the creation and management of a single, trusted view of data across government organizations and enables the modernization of systems to derive these additional benefits, among others:

- Reduced costs with citizen self service, less manual processes and rework
- Improved quality of service with transactions that are reliable and 'right the first time'
- Improved information quality with information that is accurate, resolved and trusted
- Improved decision making with trusted, quality information.
- Streamlined business processes that improve operations efficiency and adapt to change

Government agencies that are mastering information are able to make information sharing a strategic imperative so that they can effectively use information in multiple contexts across the organization while also working in collaboration with other governmental organizations.

Government is also better able to adapt to the ever changing challenges and threats around public safety by detecting and managing fraud and threats across indiscriminate geographic boundaries. Lastly, smarter governments are mastering information in order to modernize and operate more efficiently by streamlining aging and decentralized information systems and business processes.

Government Information Management Solutions

Achieving each of these strategic and operational imperatives by mastering information is enabled with the IBM mastering information portfolio for government. IBM's mastering information portfolio for government addresses the broad and vital requirements of government by delivering unique capabilities that allow government to meet its strategic imperatives, and includes:

- IBM Initiate Master Data Service
- IBM InfoSphere Identity Insight
- IBM InfoSphere Global Name Recognition
- IBM InfoSphere Master Data Management Server

IBM InfoSphere software for trusted information offers this adaptive and flexible portfolio of software solutions to meet the overarching and complex information management needs of government.

Linking and Sharing

Government as an enterprise collects data from multiple, disparate sources and shares data both vertically within an organization and horizontally across agencies and jurisdictional boundaries. Smarter governments are continually looking for unique and innovative ways to collaborate – to be able to take advantage of the data collected and stored across data silos internal and external to the agency.

Government business processes such as intelligence and granting immigration benefits demand inter-agency collaboration despite the fact that the data is collected and resides across multiple agency systems. Certainly, policy and legislation drive the need to link and share this information but so do the benefits of linking and sharing historical data stored in a variety of formats. Furthermore, threats like terrorism, cyber security and fraud are not contained within a country or government organization. Rather, threats to national security and public safety are more commonly international and indiscriminate requiring governments to share information.

Inter and intra-government collaboration requires dissemination, integration and management of information to link fragments of information together into a smaller, cleaner subset and share it with the right user in the format most useful to them. Information linking and sharing as a strategic imperative entails more than simply making information available, it also means adhering to privacy regulations and viewing authoritative information in context of its purpose and use. This includes improving the quality of data that is commonly incomplete, conflicting and riddled with errors. Agencies need to be able to use information in multiple contexts across their agency and also work collaboratively with other agencies.

Government organizations that share information need to ensure that sensitive information is protected and that only those persons with the right authority are allowed to view the sensitive information. At the same time, information stakeholders need to maintain ownership of their shared data assets and to continue governing their data without compromising data quality.

IBM Initiate Master Data Service delivers single, trusted versions of identities, entities and their relationships to government organizations faced with the challenge of analyzing disparate and fragmented data to create actionable information. Using statistically advanced methods to match and link entities across a range of possibilities and to identify relationships among entities (people, objects, locations and events), IBM Initiate Master Data Service creates accurate views of information and enables sharing of this information across the organization. Such accurate views can be customized down to the user level depending on the consumer whether for an analyst, asset manager or senior level executive.

IBM Initiate Master Data Service can create on demand, customized single views of entities correlated across multiple sources. Entities can be persons, objects like weapons, locations like crime scenes or events like border crossings. This entity correlation enables information sharing by providing entities with rich context for users and applications that are authorized to view it. For example, sharing information about a traveler is useful but when you are able to correlate that traveler with

border crossings and perhaps threat alerts from other systems the information is made actionable.

A key benefit of IBM Initiate Master Data Service for information sharing is that the source systems do not change and do not need to be completely copied or moved to another location. You no longer have to manually piece together data from stove-piped systems for system requirements. With IBM Initiate Master Data Service, you can automatically access rich data with context from numerous sources. Enriching entities this way ensures that applications or persons that are using this information to make decisions (detain, arrest, grant access, etc.) are operating from trustworthy and reliable information. The key is accuracy. Information needs to be put together in a way that minimizes incorrect intelligence and consequently incorrect decisions.

These capabilities are key components in information sharing architectures delivered by IBM Initiate Master Data Service given its unique ability to link and share. Key features include, among others:

- Multi-Entity Support to resolve people or things in views unique to the organization and the role
- Role-based Access prevents specific organizations and users from having access to or changing your data, down to the attribute level
- Composite Views enable each organization to have its own view of the matched, resolved data, depending on what they think is trustworthy

Government agencies that are mastering their information with IBM Initiate Master Data Service are able to make information sharing a strategic imperative so that they can effectively use information in multiple contexts across the agency while working in collaboration with other agencies.

The Law Enforcement National Data Exchange Program (N-DEX) provides law enforcement agencies in the United States with an accurate, scalable and high performance method for linking and sharing national law enforcement information.

The program also provides a powerful investigative tool to search, link, analyze and share information such as incident and case reports to a degree never before possible.

IBM Initiate Master Data Service manages the service's information assets effectively and makes them available wherever they are needed, regardless of agency boundaries or their originating data source. The solution uniquely rationalizes identities including citizens, persons of interest, children, organizations, customers and patients – as well as events, locations, vehicles, weapons, incidents and investigations.

More than 18,000 law enforcement agency users at local, state, regional and national levels of government have access to a single point of discovery for "connecting the dots" in order to improve the speed, accuracy and efficacy of pursuing criminal justice. Information collected by one organization is now available to colleagues in other organizations breaking down artificial geographic and system boundaries – from which criminals do not discriminate.

Fraud and Threat Detection

Government is increasingly turning its attention to more effectively deal with fraud and threat, and in doing so requires unique analytical capabilities (beyond linking and sharing information across agencies) to discover where threat and fraud exist in order to take expeditious action – whether preventative or responsive.

Fraud and threat detection is about turning information into insight, and understanding how to establish the true identity of an individual. Depending on the nature of the organization's mission, the impact can lead to problems such as missing threats posed to public safety, duplication of benefit payments, accepting business from known criminals or tax evasion.

The government requires analytical technologies to help them proactively detect suspicious or nefarious activity in real-time and then support related investigative efforts. Social Services agencies are better able to improve service effectiveness and control costs when program fraud is minimized. Preventing and

identifying fraudulent activity in this context reduces improper payments and uncovers hidden relationships between citizens that may negate or reduce benefits. Tax agencies can typically lose as much as 15% of total revenues to tax evasion and other noncompliance. Auditors require tools that determine how noncompliance occurs and identify persons who are evading tax liabilities – while protecting taxpayer privacy.

Law Enforcement and Intelligence agencies face intensifying challenges due to the growing complexity, frequency and scope of security threats that are increasingly cross-cultural and arise from a variety of individuals and groups. Harnessing the information at hand to detect not only the obvious and non-obvious; but also, the adversary's efforts to conceal their identities and activities is no trivial task and must be researched and acted upon in a timely manner – if not in real-time. These challenges mandate a fresh approach to managing threat information in order to recognize and respond to threats in real-time and automatically link suspect's representations that are buried in myriad data silos. Preventing and detecting security threats and criminal activity is dependent on identity, relationship and event resolution analytics.

IBM InfoSphere Identity Insight is a real-time, scalable entity resolution and analysis platform for fighting threat and fraud. Pioneering identity and relationship disambiguation technology combines with innovative, complex event processing to help organizations prevent and detect fraud and threat.

IBM InfoSphere Identity Insight analyzes the three most essential elements of context: Who is who? Who knows who? and Who does what? By doing so, organizations are able to understand the whole picture of who a person is, whom they know, and what they do. This whole picture provides the context upon which to prevent and detect fraud and threats.

Who is Who – Identity Resolution
The Identity Resolution or disambiguation process determines whether multiple records that appear to describe different individuals or organizations are actually records for a single identity. Once the process has determined that two or more identities are the same, it integrates multiple records into a single entity and assigns a unique identifier. The resolved identity data is presented in a comprehensive, unified view that maintains all of its original attributes, such as information about the individual or organization from prior records – even identifying the source system records that provided the original data.

Who knows Who – Relationship Resolution
Once accurate identity is established, InfoSphere Identity Insight uses the entity data to establish the nature of relationships between different individuals. InfoSphere Identity Insight learns whether people are, or ever have been, related in any way. Not every relationship matters, so, the software only raises alerts on discoveries of relevance. It understands both expressed and unexpressed relationships. Expressed relationships, such as two individuals sharing a bank account, are fairly simple to identify. Unexpressed relationships are often hidden in the data, and require more diligence to recognize. These unexpressed relationships may indicate simply that people interact on a regular basis or may designate networks of persons engaging in suspicious or illegal activities through intermediaries.

Who does What – Complex Event Processing
InfoSphere Identity Insight applies complex event processing to evaluate all transactions of the resolved entity, and optionally, of associated entities. The capability to determine all occurrences of the same person across the information landscape is required to have a clear picture of how an individual is interacting with the organization. This sophistication allows InfoSphere Identity Insight to discover well-concealed fraudulent activities.

These capabilities are key components in identity, relationship and event resolution analytic technologies that IBM InfoSphere Identity Insight delivers with reliable results. Key features include, among others:

• Entity Resolution resolves who is who by determining whether multiple records that appear to describe different entities – even with different attribute variations – are actually records for a single, disambiguous entity
• Non-Obvious Relationship Awareness (NORA™) extends the recognition of undeclared affinity groups and networks of identities across customers, employees, and suppliers or other relevant parties (up to 30 degrees of separation) by evaluating the strength of obvious and non-obvious relationships
• Complex Event Processing evaluates all transactions of the entity, and optionally, of associated entities with real-time transaction/event processing and customizable event alerts

Another challenge to gaining insight into a person's identity is to be able to view individual's names with an understanding of cultural roots and gender. Culturally-relevant insight about individual and business names helps organizations understand more about a particular name, such as culture, gender, and name parsing, as well as identify names that are likely to represent the same person in a list.

IBM InfoSphere Global Name Recognition is a patented technology and the only naming technology that has been certified under the US Department of Homeland Security SAFETY Act for its ability to search names based on the linguistic, phonetic, and specific cultural variation patterns. This technology is based on knowledge built from analysis of over 800 million names, and provides IBM InfoSphere Identity Insight with the ability to discover more strictly qualified matches than any other technology.

Government agencies that are mastering their information are able to better adapt to ever changing public safety in order to better detect and manage fraud and threats within indiscriminate geographic and cultural boundaries.

A European police agency uses IBM InfoSphere Identity Insight to accurately recognize individuals (despite different variants of the data), and then detect relationships – fully automated and in real-time. The agency has found the solution expedites an investigator's access to the relevant data, especially in extensive, complex cases with massive amounts of data typical of their most high priority investigations. New data that has connections to existing information automatically raises alerts (data finds data) to streamline investigations.

Several U.S. agencies use IBM InfoSphere Identity Insight to support their national security and intelligence missions. National security challenges have never been greater. Near-misses like the Christmas Day bombing of Northwest flight 253 remind the world that higher levels of vigilance are necessary. Coping with the ever-growing volumes of data make the nature of the problem all that more complicated. Harnessing the information at hand to detect not only the obvious and non-obvious, but the adversary's efforts to conceal their identities and activities is no trivial task. Identity Insight was originally developed by Systems Research and Development (later acquired by IBM). By 2001, the venture capital arm of the CIA (In-Q-Tel) recognized the applicability to various intelligence programs, and twice granted funding to the company to further advance the technology. As a result, Identity Insight plays a unique role in protecting the nation's security.

A county in the State of California was seeking to reduce costs while improving the performance of state social programs in alignment with the state's Deficit Reduction Act. The legislation required that the Work Participation Rate (WPR) for welfare recipients reach 50 % and put the burden on county social service agencies to find a way to enforce this policy. The county teamed with IBM to deploy an information management system that combines IBM InfoSphere Identity Insight with business intelligence to give workers an agency-wide, comprehensive view of individual cases. The system provides managers and caseworkers with a complete, real-time understanding of case and program status, reveals relationships between benefit recipients and programs, and generates reports in minutes instead of weeks or months. To prevent abuse, the

system initiates alerts when clients are out of compliance, and more importantly, when clients are eligible for additional services that could benefit them.

Business Modernization

Government information systems are aging, decentralized and fragmented. Agency systems are typically comprised of myriad siloed systems that hamper vertical business process integration and integration across the entire business process. Furthermore, legacy data is often duplicated, incomplete and inaccurate across source systems resulting in citizen, applicant and case information being out of synch across essential service applications. These burdens result in lost productivity, excessive manual data entry and wasted time that unnecessarily delays service delivery and increases case backlogs. At the same time, legacy systems can no longer be efficiently maintained and need to be replaced.

Cost control is driving transformation across government business processes and IT systems in addition to mandates to adhere to policy and legislative changes, privacy regulations and concerns of the public. Aging and decentralized information systems and business processes need to be improved to maintain efficient government.

Government wants to create a single repository of trusted data from various source systems – a single unified version of the truth about its critical entities – to gain the deeper insight it needs to make better decisions, improve service delivery and program outcomes, and reduce Information Technology delivery and maintenance costs.

IBM InfoSphere Master Data Management Server delivers a single version of the truth of an organization's critical data entities. Organizations can easily manage multiple data domains, across a wide set of business requirements. IBM InfoSphere MDM Server provides out-of-the-box capability for both traditional domains (citizens, cases, agreements, employees, agents) and the tools to manage custom domains. With proven capabilities to create, view, edit and analyze

master data, IBM InfoSphere MDM Server becomes the source of trusted information across the organization.

IBM InfoSphere MDM Server manages master data for all business processes that consume it and is designed to be the system of record for master data. In this way, it addresses fragmented and siloed data by providing a proven framework designed to help organizations manage master data by decoupling it from operational, transactional and analytical systems into a centralized independent repository.

This centralized, trusted information is then provided to SOA business services so data is managed independently of any single line of business, system or application. This enables organizations to identify common functionality for all systems and applications and then support efficient, consistent use of information and processes.

IBM InfoSphere MDM Server can easily integrate master data into any operational process across the IT and business ecosystem. Key capabilities include, among others:

- Business Services that manage master data are provided in the core functionality with more than 800 extensible business services (and administrative services) that allow organizations to build their own composite business services. Business services define how users access master data while seamlessly integrating into current architectures and business processes.
- Business Rules Engine gives users flexibility to manage rules without having to change application code and allows customers to "externalize" rules.
- Event Management allows InfoSphere MDM Server to detect transactional and data driven events by creating event rule definitions using the business rules engine.
- Event Notification is a framework that allows the definition of rules that monitor data changes that require event notification.

Government agencies that are mastering their information are able to modernize and operate more efficiently by streamlining aging and decentralized information systems and business processes.

9

About IBM MDM

The IBM MDM portfolio delivers a single, unified, trusted version of truth about an organization's critical entities – customer, supplier, product and more. Armed with this single, trusted view, organizations can make better decisions and improve business outcomes – higher revenue, better customer or citizen satisfaction, improved patient care, lower cost and risk. With IBM MDM, organizations can understand their core master data (customers, patients, products, etc.) at all touch points, improve cross and up-sell, optimize the value of ERP, CRM, analytics and warehouse systems, support governance initiatives and make business processes more effective.

InfoSphere.
software

Please Recycle

IMW14484-USEN-00