Three Pillars of Government IT

Getting data governance, compliance and security into alignment.

Building a foundation, whether for a building, a legal case or an IT system, may not win public praise, but it's an absolute necessity. Without a solid foundation, any edifice built on top of it can fail.

For federal agencies evaluating their IT systems, three of the critical components that make up that foundation are data governance, compliance and security. But aligning these three elements not only creates the basis for an efficient, well run network, it can also save agencies time, money, processing capacity, and provide the means for the agencies to connect information across databases, even across multiple agencies, according to Jason Wilson, senior product manager at Insight Enterprises. "We often help agencies manage what's on their plate today so they can begin transforming their operations for what's next."

Data governance is essential

"One challenge is how to build a governance strategy around your data management," Wilson says. "It doesn't sound exciting, but when you understand how data sits inside your datasets, the value of it becomes clear."

Every program manager wrestles with the problem of data inconsistency—such simple things as empty fields, fields in different orders, last name/first name or first name/last name, use of middle initials, and so on—that make it extremely difficult to connect records even within a single database, let alone across multiple datasets.

Establishing standards for machine readable data formats in line with international standards, for instance, on specific ways to format dates and names, will address many of these shortcomings. Using certain SQL-based tools can further "scrub" data to reach greater levels of cleanliness, and lead to an improvement in records management and linking compatibility.

Compliance, the bane of IT managers' routines

One of the headaches faced by government IT systems administrators stems from ensuring their systems comply with the thicket of statutory and regulatory requirements laid out by an alphabet soup of agencies. The job of demonstrating compliance can often be seen as taking valuable time away from other work. But compliance standards are intended to further transparency, system standardization and risk management, all of which help IT systems operate more effectively.

Over the years, agencies such as the National Institute of Standards and Technology, the Government Accountability Office and the Office of Management and Budget have gotten better at disseminating compliance mechanisms that go beyond "check the box" requirements, instead requesting real metrics that actually promote real goals, such as network security.

Constructing IT systems and datasets, and taking advantage of software that than can confirm compliance, can help streamline the work involved in producing required reports that show targets are met. "SQL Server as a product has got all kinds of excellent features built around compliance issues," Wilson said.

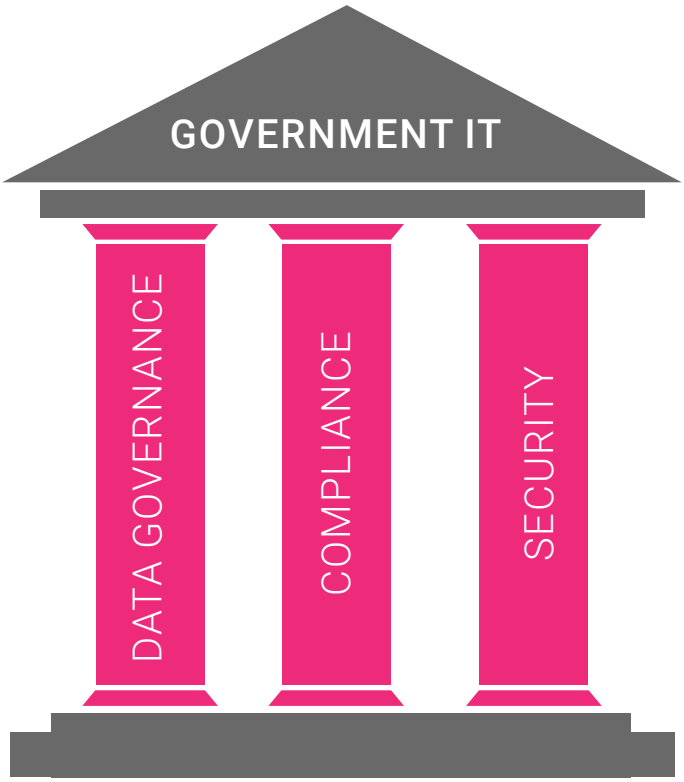
Protecting data assets is the heart of security

As in the private sector, the federal government recognizes that data is an asset. Unlike the private sector, however, the value of government data extends well beyond its potential for commercialization. The impact of security failures—whether exfiltration of data, denial of service, or other exploits—has been seen in recent high-profile incidents, such as the Office of Personnel Management breach.

Additionally, federal officials have made it clear, some data assets are more valuable than others and must be handled accordingly. The Office of Management and Budget has defined "high value assets" as "those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people."

Because of its importance, the Office of the Federal Chief Information Officer has defined an "Agency HVA Process" which sets guidelines for making these determinations. The National Institute for Standards and Technology also issued requirements in Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."

And there are further requirements in such laws as the Federal Information Security Management Act and the Government Performance and Results Act, numerous federal mandates created through Presidential Executive Orders.



Keeping on top of other data demands

Additionally, agencies need to stay on top of international standards and requirements that may apply. "We can be subject to foreign countries' laws, as well," Wilson said. "For instance, the European Union has issued the General Data Protection Regulations, set to take effect May 25, 2018."

Another dimension of the data landscape is the global movement by governments to promote open, machine-readable data, which has added an additional challenge for CIOs.

In a Federal CIO Council report on "The State of Federal IT," issued in January 2017, the council noted, "While most CIOs reported interest in open government and open data initiatives, many expressed challenges in obtaining resources, navigating conflicts with existing policies, and balancing priorities against other efforts such as infrastructure modernization and cybersecurity."

Between budgeting constraints, manpower limitations, pressures to modernize IT infrastructure, and heightened emphasis on cybersecurity, federal IT managers have a challenging time keeping data governance, compliance and security in alignment.

A Path Forward

Wilson suggested that managing governance, compliance and security can be addressed as a whole, incorporating all of them into an agency's data strategy. "Agencies are always looking for companies who can help navigate the security and compliance piece," he said. "What they really have is a problem that has to be solved. We tackle that head on so we can start transforming their IT to grow with them."

Part of data governance should include identifying the services an agency needs to provide, which of those services generate data, and the kind of data being produced, he said. That helps to address the issue of format standardization and the ability to connect records within and across datasets. SQL Server continues to add new tools and features that enable improved data quality, such as Master Data Services and Data Quality Services.

Two critical elements of security and risk management are encryption, including encryption key management, and automation of patch/vulnerability management.

Many agencies may already have tools at their disposal to address these elements, according to Wilson. For instance, SQL Server has included "always encrypted" in its standard features since Service Pack 1 was released. For the past seven years, NIST has scored SQL Server as the least vulnerable approved tool for government use.

Additionally, SQL Server Enterprise offers features that can address data governance, compliance and security, including dynamic data masking, the ability to separate duties, and protections of personally identifiable information (PII). It also can provide integrated development and deployment of upgraded or replaced databases that leads to faster performance, less downtime, and strengthened security.

Agencies' partnerships with IT providers and integrators can also provide the resources and knowledge to track and meet compliance requirements, and could be used as a decision criterion when evaluating offerings. Many in the private sector also provide their products and services in other countries, and have the expertise to include foreign compliance as well.

Many integrators, in particular, with their experiences working with many assorted products and services, have the expertise to knit together solutions that keep data governance and security requirements in line with the changing landscape of compliance policies.

Conclusion

Rather than viewing governance, compliance and security as separate requirements that compete for attention and resources, federal IT managers benefit from understanding how these three elements mutually reinforce each other.

Besides improving agencies' track records and reporting, this approach will streamline overall management of all three areas, resulting in both improved performance and greater efficiency—also likely benefiting the expense side of their ledgers.

This article was produced by fedscoop *for, and sponsored by,* Insight.