# Data Security Governance Impacts Analytics

Updated Security Governance Needed to Enable Better Return on Investment (ROI) from Analytics

## Outdated Security Governance Generates Diminished Analytics

A separate white paper discusses why business structures must change to achieve the benefits from modern Information Technology (IT) architectures. This applies to security governance, because analytics adoption requires trust in the results. Orchestrated Analytics has the power to return far superior responses and returns on investment than any other type of analytic implementation. However, orchestrated analytics requires access to information to work. If it is denied access to critical information, it will fail to return the answers that would have saved lives and saved millions of dollars.

The fault is not in the analytics technology. Nor is it in the ability to integrate technologies on a technical level. The fault is in failure to develop and ingrain new security policies, processes and governance models that sync with current technology. Lackluster Return on Investment (ROI) can result from security policies and models that unnecessarily inhibit analytic tools.

The real problem is two-fold:

- Application of an Inappropriate Person-to-System Security Model on Analytic Services
- Data and Service Implementations not Guided by Enterprise Security Governance

## The Analytic Processing Security Touches Inside Service-Based Architectures

When looking at the National Institute of Science and Technology's (NIST) Cloud Computing Reference Architecture[i], it is easy to mistakenly confuse their placing of Security and Service Aggregation services outside the Service Orchestration stack to miss a very important relationship they have with what is occurring in the Orchestrated Services at the Platform as a Service (PaaS) and Software as a Service (SaaS) levels. (See Figure 1.)

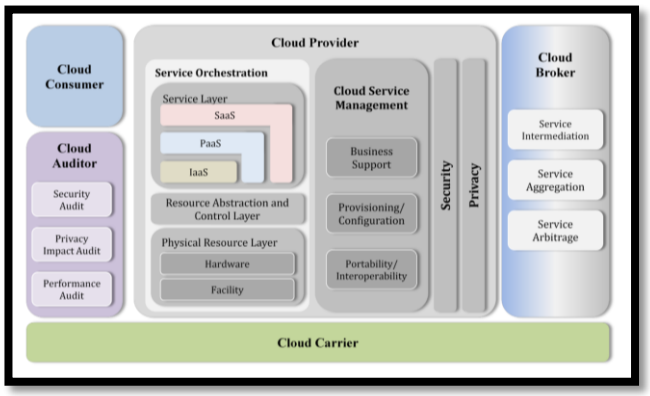


*Figure 1 NIST Reference Architecture Cloud Conceptual Model*

Ultimately, every service-based analytic system, whether orchestrated or not, and whether in a cloud or not, is gathering original content, brokering it, enriching it, re-brokering it, and re-consuming it (see Figure 2).

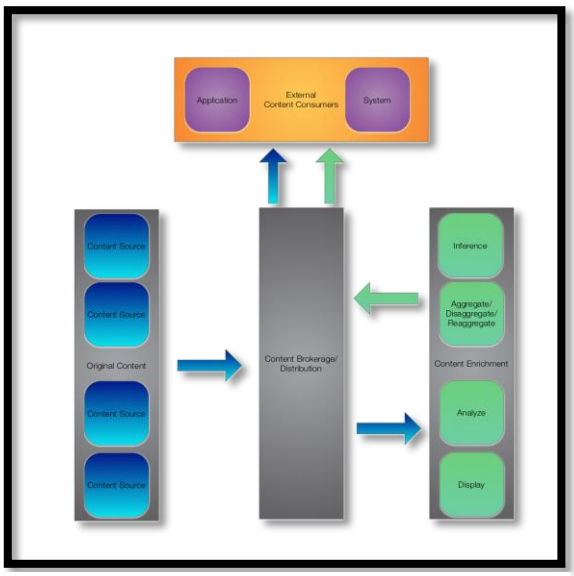


*Figure 2 Separate Content Actions in Knowledge Chains*

Big Data analytics rests on its ability to broker and enrich (aggregate, disaggregate, analyze, infer, etc.) original content, and then re-broker and re-enrich from the new set of combined original and enriched information to which it has access.

## Technical Security Models

If the data security model is person-to-system based (e.g. do not provide a response to any query unless the ultimate initiator has the clearance), then it misses the point of analytics. While this may be shocking, it is only because it has not been compared to a fully accepted and working person-to-person information security model. John can ask his boss, Sarah, "What should I do?" Sarah can look at data that John does not have access to, reason over it and provide him an answer without disclosing the privileged information.

Traditional technical information security models treat an analytic service's query as the original person themselves attempting to query for that information, rather than an outsourced intermediary executing a step by itself as a step in its analysis to develop the outsourced answer to a question.

While it is not appropriate to classify analytics as Artificial Intelligence (AI), there is a certain reality to analytic services as mimicking human reasoning and acting as a distinct entity from their human user. Their programming adds reasoning and action outside the user's ability to control. If it is programmed to strip background information before providing a result for certain classes of users, then the human user can influence that background data stripping even less they could in a human-to-human filtering scenario.

Analytic services need a similar security model on a technical level. Rather than a content source asking, "Does the Active Directory show the human originator of the query as someone permitted to get this information from me?", it should ask, "Is this a security-conscious analytic intermediary service, like Sarah, that can broker and enrich information to provide answers without compromising privileged information?"

This is doable with analytic services that exist in "lineage" markup environments. While not all analytic services exist in this environment, organizations should develop and add a nuanced "security-conscious analytic intermediary" security model to handle analytic services in environments that maintain lineage and have the security reasoning infrastructure to leverage it.

## Updated Model Cannot Exist without Enterprise Security Governance

Developing a technical security model for security-conscious service-based analytic environments that maintain and act on lineage information must be concurrent with implementing an enterprise security

governance paradigm that enforces standards across content sources and enrichment services that lie within the enterprise's control.

Frequently, Product Managers are told, "You are responsible for security breaches. Build your own security controls, sharing policies and access policies to prevent them." This leaves a patchwork of unique defenses that are expensive to maintain and renders system-of-systems interoperability extremely expensive to implement. It also places the structural power to block access not at a level accountable to the results of decision makers, but at the information supplier-level.

In order for a technical security model to mimic person-to-person interfaces, organizations must implement an enterprise security governance model that covers security policy, processes and technical implementation patterns over Data and Services, not just People and Systems. It needs to address:

- Accountability for Security and Enterprise Performance
- Policies and Criteria for Assessing Value, Risk and Legal Implications of Data
- Criteria for Restricting Data/Service/Person Access
- Criteria for Sharing
- Enterprise Security Architecture
- Technical Standards to Be Used
- Acceptable Implementation Patterns within Standards
- Rapid Enterprise Review and Approval Process throughout Lifecycles

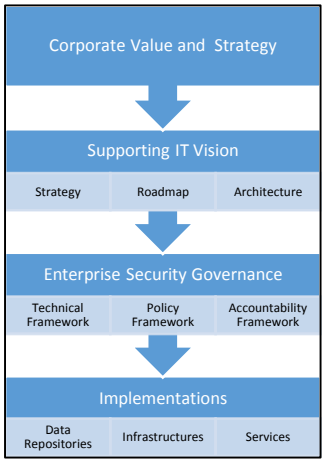

*Figure 3: IT Governance Drivers*

## Positive Security and Cost Impact

Patchwork security is vulnerability. "Does the person exist in my Active Directory?" is an expensive model to keep current and still risks being wrong (and vulnerable) somewhere in the plethora of security silo'd systems.

Patchwork security is expensive. It impacts the cost to maintain IT and the cost to enable analytics. Variation is a cost driver requiring reasonable, balanced direction supporting a company's market value and strategy.

Patchwork security increases cost, while outdated models inhibit analytic processing. An analytic investment that cannot return accurate answers does not get used. An analytic investment that cannot access another business unit's information cannot be re-used elsewhere. As cost rises and usage declines, ROI suffers.

Ultimately, organizations need an updated technical security model and enterprise security governance to:

- Improve Security
- Lower the Cost of Security
- Improve Return on Investment of Analytic Technology Implementations

[i] NIST Special Publication 500-292, Sept 2011. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505