HITACHI
Inspire the Next

Recession-Proofing: Do you Know Where Your Data is?

COMPLIANT DATA IS VALUABLE DATA

5 Steps to Control Your Data so you can put it to Work

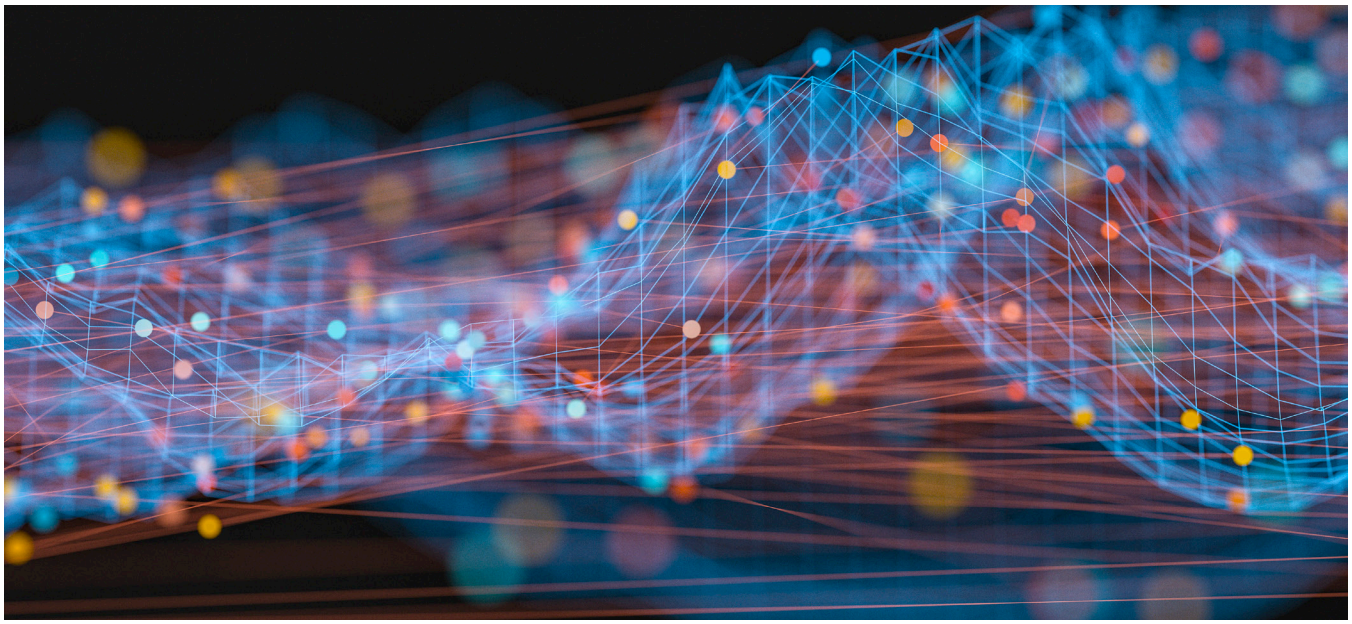
Chris Drieberg, CTO and Director Pre Sales, Hitachi Vantara ANZ

Australia's financial institutions are rich in data. Data that could yield insights, support innovation and improve the customer experience as banks, fintechs and other businesses in the financial sector face challenging realities. If they can put it to work, that is.

Adding an economic downturn to an already challenging mix of increased regulation and scrutiny, rising consumer expectations around the customer experience and data privacy, and the increased risk of sophisticated cyberattack and financial fraud, has created a perfect storm for our financial sector.

If data is to be the lifeboat that brings a financial institution safely to a post-recession shore, then gaining control of that data is the life preserver that gets them into the boat.

By Hitachi Vantara
May 2020



Better the Data you Know

In a highly regulated, open banking environment, financial institutions (FIs) could be forgiven for thinking of data in terms of compliance, privacy and security. With so much data to manage and new information being produced and captured on a daily basis, it's become a headache and an expensive liability. All of a sudden (ok, it's been a couple of years in the making, but who's counting?) they have to make data open and sharable, yet protected and secure, when historically their systems have all been about processing data and holding it within a closed system. Throw dark data into the mix and this task becomes even more daunting.

And what about innovation, digital transformation, and harnessing data to feed a machine-learning driven, AI-enhanced customer experience? These are also on the must-do list. For FIs to handle this perfect storm and come out the other side not only resilient, but productive, thriving and satisfying customers, they need to get a handle on their data.

It's time to gain control of your data and turn it into information that can be used for much more than compliance.

But first you have to find your data and get to know it a lot better.

The Problem is not "Big Data"

Most enterprise organizations do not know what data they have or where it is. How has this happened?

The data that financial services organizations have had to collect, monitor, store and secure has grown so rapidly that most couldn't keep up. The types of data they own have changed, and include new and prolific data types like social media and sensor data.

Acquisitions, consolidation, growth and diversification add to the complexity of an enterprise's infrastructure. Divided into divisions, departments, teams and projects, many financial organizations have created silos that are difficult to dismantle.

Thanks to new technologies and increasingly distributed architectures, data is dispersed across multiple environments, public clouds, software-as-a-service (SaaS) environments and edge devices.

The problem is not "big data". It's that organizations have so much unstructured, disorganized, bad-quality data. Organizations have stored a great deal of bad-quality data without knowing what it is and even where it is and they keep making more of it every day. It doesn't get cleaned or classified. It's not reliable. There are multiple copies and iterations of the same data stored around the business. And the list goes on.

How to get Control of Your Data

Step 1. Change Your Storage Mantra

"Save everything, just in case!" should be deleted from everyone's vocabulary. Expanding storage capacities to keep everything just in case it becomes useful, valuable or reportable just doesn't make sense. It won't help you manage complex compliance requirements or derive value from your data. It's expensive and risky.

Organizations should keep relevant and usable data for its appropriate retention period as set by the business for compliance, audit, recovery and analytics purposes.

Your new mantra should be "Classify the data, then decide what to save and for how long."

It takes a bit longer to say and to set up the necessary systems, policies and processes, but it makes more business sense and reduces risk.

Step 2. Demystify Dark and Toxic Data

Can saving everything and harboring unstructured data put the business at risk?

Yes. Organizations can unknowingly store highly sensitive data that would be dangerous if leaked or obtained through breach. They may unwittingly store data infected with ransomware. Static, unclassified and unstructured data, and data that is inappropriately or insecurely stored, can contain information that is potentially detrimental to the business.

Dark data is data sitting in storage repositories that may or may not have any value or serve any purpose to the business. The business doesn't know what or where it is, or whether it is useful or not, because no mechanism has been put in place to classify it and determine its value. It hasn't been deleted, because "just in case." It has simply been stored.

Toxic data is data that should not be stored or should be deleted after a certain time frame because it could be a liability or security risk. For example, identity data associated with an outdated and completed contract, or contained in a report that is no longer required for compliance purposes, is toxic. Yet it is stored, or retained too long, because no system has been put in place to identify whether it has any risk associated with it.

Loss or leakage of this data could result in brand and **reputation damage**, **noncompliance** issues and even **heavy fines**. **Data theft** is also a risk. Modern criminals know dark and toxic data are widespread issues, and they have the sophisticated technology required to perform search and indexing activities that organizations may not have invested in.

Dark and toxic data should not be feared, but rather found and controlled.

Step 3. Deal With [and Govern] Your Data

Raw data comes from many sources in many formats and is stored as ones and zeros: the language of machines. It is dispersed across the infrastructure and technology solutions of a modern business. To make that data useful for people and businesses, it must be transformed into information and appropriately classified.

Popular search engines use content indexing to make sense of data and make it useful. This very same concept of **content indexing**, combined with a rich and **powerful information index (or metabase)**, will help an organization extract information from its raw data.

It's all about **harnessing metadata**, which is the data about the data, to answer questions like: Who created the data? What is it about? Who has used the data? To whom does it belong? What value does it serve my business? What risk does it represent? Can I destroy it? Should I keep it? That information must be stored along with the data, to identify the data.

Context indexing and metadata provide information with which to understand your data. The data can now be **classified**, and appropriate privileges and

policies can be assigned to meet retention, protection and security requirements. This process will allow the business to identify and deal appropriately with dark, toxic and unstructured data to remove associated risks. A single distributed index architecture across all data environments will ensure the business has a **single source of truth**.

Data analytics will play a significant recession-proofing role. Once the content is indexed and classified, analytics capabilities will help financial institutions comply with requirements to isolate data down to the individual. Analytics can help to create an information map, define what is personally identifiable and sensitive based on characteristics, and profile customers in aid of improving the customer experience. Insights will identify opportunities to capture market share.

As you work to get control of your data, underpin these efforts with **data governance**: rules, controls and policies to guide data management. Formalize your organization's ability to understand and classify your data, to ensure you can accurately find the right data set when requested or required. Turn regulatory requirements into policies and procedures that protect the business and ensure compliance, while enabling users to work with data in new and insightful ways. Start at the storage layer with a data governance program that addresses scalability and provides security, auditability, policy based controls, encryption, access management and data mobility.

Step 4. Support Compliance With RegTech

People within the business must set compliance in motion with well-defined, clear compliance policies. But due to the sheer amount, complexity and data-intensive nature of the financial sector's regulatory environment, governance and compliance becomes cumbersome, costly and time consuming. People alone cannot cope with the sheer volume of data, or process the amount of work required for comprehensive compliance, despite an organization's best intentions.

RegTech: The Use of Technology To Solve Regulatory Problems

- Encryption and other technologies will ensure secure transport of open data to the appropriate destination.
- Data-masking solutions will protect data that is classified as personally identifiable and sensitive data, or commercially sensitive data.
- Technologies such as blockchain will modernize the maintenance of an immutable ledger audit system.
- Content indexing, data classification and the application of metadata will be automated, driven by increasing data management requirements.
- The time- and resource-intensive regulatory reporting process will increasingly be automated for efficient adherence to deadlines and requirements as well as cost savings.

Applications of automation, blockchain, artificial intelligence and machine learning will enable organizations to identify patterns and behaviors in data, implement protocols and automate controls to comply with an increasingly complex compliance regime. RegTech will assist organizations to manage and identify the sheer amount of data they have, effectively apply governance policies, and ensure that critical procedures, systems and controls are correctly implemented within organizations.

Use of RegTech doesn't mean turning over all responsibility for compliance to technology. Rather, your intellectual human capital behind data governance and compliance policies, and behind the selection, implementation and oversight of RegTech solutions is critical.

Step 5. Realize the Value of Compliant Data

Good-quality, clean, compliant data that has been indexed, classified and governed can be used to:

- Improve the customer experience.
- Generate insights for competitive advantage.
- Inform and enable innovation.
- Assist the organization to apply change more quickly, both to correct when something has gone wrong and to expand and scale when a success has been realized.

Obviously, data is not just something you use for compliance purposes. Employees and customers demand access to it anytime, anywhere, from any device. Properly managed, governed and analyzed, data is a significant strategic asset that can yield actionable insights and even new revenue streams.

Regulatory compliance is often considered a cost center: a time-, money- and resource-consuming annoyance. It's time to change that perspective. An organization that ensures it has the good-quality, clean data required for regulatory compliance now has reliable, precious data to monetize and drive value for the business and meet market and economic challenges head on.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact

May 2020