



CPG 235

Implementation

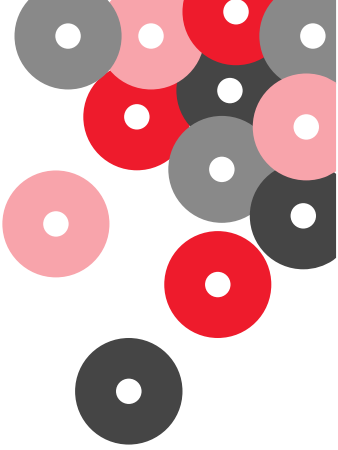
Fundamentals

How are you managing your data risk?

Do you understand the difference between data risk and risk data?

Learn how innovative regulatory guidelines are inspiring a new approach...





CPG 235 is a guideline focusing on data risk management, released in 2013 by the Australian financial industry regulator, but only now becoming a hot topic due to recent major data breaches across several high-profile companies.

Whether you have Australian interests or not, this guideline is of interest in the focus on *data risk* compared with the well-known BCBS 239, which looks at *risk data*. By contrasting the two perspectives, new insights can be gleaned.

The Challenge for Australian Banks, Insurers & Supers

The regulator for the financial industry, known as the Australian Prudential Regulation Authority (APRA), first issued its guidance for data-oriented risk management almost a decade ago in 2013. Still, until recently, the topic has not gotten a lot of attention. So, what's changed?

What's changed is that large companies who Australian consumers trust have recently suffered major data breaches by highly organised hackers. These companies span a range of industries, from healthcare to retail and telecommunications. The result of these breaches is that the private data of at least 100 million citizens is in the hands of bad actors. Suddenly, the veil of perceived low risk and readiness has been pierced. The stark reality has settled in that the Australian regulators and industry are all far behind and extremely exposed.

The United States financial industry experienced a shock during the 2008-2010 financial crisis that was borne of a lack of regulatory oversight of mortgage-backed securities and their derivatives. And while the housing crisis was not specifically related to data breaches, it resulted in sweeping regulatory reform aimed at risk management, including how data is managed.

The European Union had a similar season of regulatory reform in the mid-2000s while forming the laws and regulations of their new trading block; at the time, that reform turned on a key question: How could they protect the rights of individual country's citizens while streamlining the ability to work together across borders? The result was the formation of a regulator called the EU Commission and a proposal for a General Data Protection Regulation (GDPR), which was enacted into law.

Australia must act fast to close the risk gap that allows the existential risk and attack on their citizens and institutions. If there is a silver lining, they can move quickly by leveraging what the United States and EU have already learned.

Defining Risk Management and Data Risk

As basic as it may seem, we must share a common definition and understanding of data risk.

Data risk is a subset of risk management, so what is risk management? Risk management is an ongoing process for identifying risks, defining controls which are essentially actions for mitigating each risk, and providing evidence that the controls are used and working. All businesses in highly regulated industries have board-level risk subcommittees and C-level risk executives. Their governance authority and responsibility will be formally delegated to various teams for implementation. This delegation will include data management, including data governance, privacy and information security leaders, along with other specialised control functions in an organisation. Each leader is responsible for different aspects of the risk management process related to data.

That brings us to the definition of data risk.

As stated formally by the APRA:

"Data risk encompasses the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events impacting on data."

"The goal of data risk management is to ensure that the overall business objectives of a regulated entity continue to be met."

Notice that data risks emanate from both inside and outside the organisation. The stated goal makes sense for the financial industry, which is their scope of responsibility, but is too narrow a definition for all industries. Stated more broadly, data risk management aims to ensure that business objectives are met and that the corporation, employees, customers, and suppliers are protected.

History of the APRA and CPG 235

The APRA was established in July 1998 as an independent statutory authority that supervises institutions across banking, insurance, and superannuation, and is accountable to the Australian Parliament.

The APRA uses a three-pillar framework that consists of legally binding standards, guidelines, and reporting standards. CPG 235, released in 2013, is a guideline that is not legally binding or enforceable. Its focus is data risk management and the APRA's view of sound practices.

The APRA released CPG 235 as a Prudential Practice Guide (PPG) to target areas of weakness they have seen in their overall supervisory work. The APRA also states, "The PPG does not seek to provide an all-encompassing framework, or to replace or endorse existing industry standards and guidelines."

Interestingly, the APRA has publicly shared that PPG 235 content was informed by the industry standard known as the Data Management Capability Assessment Model (DCAM™) from the Enterprise Data Management Council (EDMC). We will fully introduce both after setting a bit more context.

BCBS 239 and CPG 235

BCBS 239 is the Basel Committee on Banking Supervision's standard number 239. The overall objective of the standard is to strengthen banks' risk data aggregation capabilities and internal risk reporting practices. It was published in January 2013, the same year as CPG 235, for Global Systemically Important Banks (G-SIBs). It has been legally binding since 2016. It's widely understood that BCBS 239 was a necessary reaction to the 2008-2010 financial crisis and near-total global economic collapse.

BCBS 239 includes 14 principles aimed at risk data instead of CPG 235's data risks. It is a subtle transposition of words with an important impact. BCBS 239 is focused on narrow financial system risks and having the data to report on those risks. CPG 235 is focused more broadly on all corporate data and the risks associated with managing that data.

So, why introduce BCBS 239 if they are so different? Consider principle #2:

BCBS 239 Principle #2:

Data architecture and IT infrastructure – A bank should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis, while still meeting the other Principles.

This principle and others forced the banks to rethink their data management operating models. It also forced them to assess whether their data management operating model met all the BCBS 239 requirements. As a result, CPG 235 and BCBS 239 emphasise that the data management and data governance controls apply to data quality and managing data through its entire lifecycle.

The Enterprise Data Management Council and DCAM

The EDM Council is a global association that was born in 2005 out of a common need for banks to elevate their Data Management practices to meet BCBS 239 and other regulatory requirements.

The EDM Council quickly attracted members from the global financial industry, formed sub-committees, and began work creating new data management standards.

Today, the EDM Council has over 350 member organisations from the US, Canada, UK, Europe, South Africa, and Asia-Pacific, with over 25,000 data management professionals as members. In addition to standards, it provides a venue for data professionals to interact, communicate, and collaborate on the challenges and advances in data management as a critical organisational function.

Arguably, the most important contribution of the EDM Council to the industry is a standard and assessment process that is well understood and trusted by regulators.

The DCAM framework was developed collaboratively by hundreds of EDM Council members and has become the industry standard framework for data management. DCAM defines the capabilities required to establish, enable and sustain a mature data management discipline. It addresses the strategies, organisational structures, operational best practices, and technology needed to drive data management across an organisation successfully.

APRA included elements of DCAM to create CPG 235, which is why Australian companies must leverage what has been learned about implementing it so they can quickly close the data risk gap.

DCAM Methodology & Implementation Fundamentals

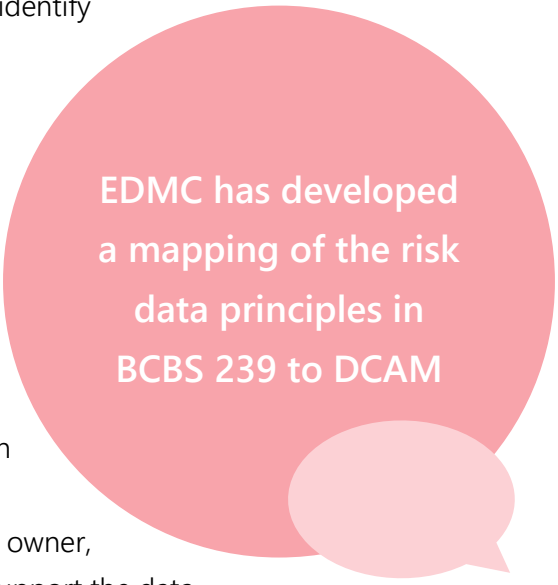
DCAM is a comprehensive target-state data management framework and capability assessment tool. The objective of completing a DCAM assessment is to first measure capability, and then identify and prioritise the capability gaps and develop a systematic capability uplift plan and roadmap.

DCAM is very process-oriented with a focus on auditability. The DCAM framework informs capability requirements for the processes, people, data, and technology required to control data, manage data risk, and create valuable opportunities for the business. The capability requirements are key to understanding what is needed for capability gap closure.

The EDMC has also developed a mapping of the risk data principles in BCBS 239 to DCAM. This mapping identifies the data management capabilities required to manage data risk successfully, as required by BCBS 239. Using the DCAM assessment scores to identify capability gaps and subsequent gap closure demonstrates the organisation's understanding and ability to manage data risk to a regulator. This approach becomes the basis for informing an organisation's regulatory narrative based on factual measurement of the capability to control the risk data and make it accessible for all uses, including managing data risk.

A core concept in DCAM is that the business process that creates the data must own the data it creates. That means the business process must define data as an input and output of each process step. This accountability is equally true for the data management function processes. The data management process owner, the Chief Data Officer, must define the requirements or data to support the data management process. This data is called metadata. Metadata is everything you need to know about your data to get it and keep it under control.

The focus on metadata from the data management processes leads to a direct technology requirement tied to a system to manage metadata (i.e. creation, implementation, maintenance, and monitoring activities). The system must also make metadata accessible to all data stakeholders. These requirements have elevated the role of a data catalog to the centre of modern data management; all focused on achieving data control.



EDMC has developed
a mapping of the risk
data principles in
BCBS 239 to DCAM

Controlling Data Risk

Much can be learned from how the heavily regulated finance industry has responded to the regulators' focus on risk data. These practices are sound guidance for all industries. OrtechA has worked with numerous organisations to introduce data risk into their risk management framework formally. Managing data risk should be an extension of managing data and data management issues. It is important to develop categories of data risk that assist in identifying the risk type and then aligning the risk to the data owner for resolution. Without classification and a method for engaging the data owner, chaos will ensue when data risk is added to the overall risk management process.

The key to managing risk lies in having data management processes that focus on metadata and incorporate risk identification as metadata in a data catalog to create transparency and organisation-wide awareness. The questions are: How do you do that? and Where do you start?

The adequacy of data controls in ensuring that an entity operates within its risk appetite would normally be assessed as part of introducing new business processes and then regularly after that (or following a material change to the process, usage of data, internal controls or external environments). The assessment would typically consider the end-to-end use of the data and related control environment, including compensating controls. Changes to the control environment would typically follow normal business case practices, considering the likelihood and impact of an event against the cost of the control.

To ensure that data risk management is not conducted in an ad-hoc and fragmented manner, an entity would typically adopt a systematic and formalised approach that ensures data risk is taken into consideration as part of its change management and business-as-usual processes. This approach could be encapsulated in a formally approved data risk management framework outlining the entity's approach to managing data risk that:



A data management framework could be defined at an enterprise-wide level, a business unit level, or as a component of other enterprise frameworks, as appropriate. The establishment and ongoing development of the data risk management framework would normally be:

- Directed by a data risk management strategy and supporting program of work with a clearly defined budget, resource requirements, timeframes, and milestones; and
- An integral part of a regulated entity's change management and business-as-usual processes. A data risk management strategy would align with the regulated entity's business, information technology, and security strategies.

The Role of a Data Catalog in Data Risk Management

A modern data catalog is a foundational component of a risk management program. It serves as the system of reference for all enterprise data and data-related assets. It maintains metadata that describes, classifies, and cross-references these assets, including the definitions of terms, governance policies, domains, and risk policies. In a risk management context, the catalog supports ongoing data management processes integral to risk, which include inventorying, assessing risk, assessing usage, and reporting.

The key is that Alation Data Catalog is far more than just a passive metadata repository. It provides automation and capabilities that help data management teams deal with massive data volumes in a rapidly changing enterprise data landscape.



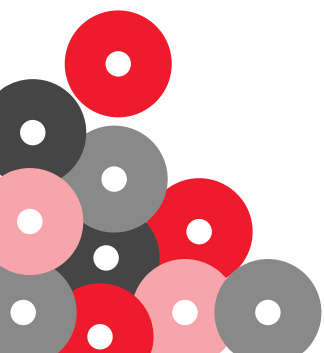
Ingestion & Behavior Insights – Alation uses scanners to continually extract metadata from all enterprise data sources. This scanning includes cloud, on-premise, and hybrid systems. The scanning process isn't only an extraction of technical details. Alation scanners provide human insights by examining how data is used and identifying its top users and popularity. The scanners also perform lexical naming of assets to make them more comprehensible.



Discovery & Classification – The Alation Data Catalog uses rule-based classifiers to examine all data assets and automatically associate them with domains, policies, and tags. For example, the catalog can find all elements of a name and place them in a personal domain, associate them with a given privacy policy, and classify them as PII so users are aware.



Owner & Steward Assignments – Alation supports the assignment of stewards using any number of approaches, including domains, source systems, risk category, etc. Stewardship assignments and progress can then be tracked and reported on using Alation's stewardship dashboard, which tracks risk assessment progress, as well as classifications and curation work and metadata maintenance.





Bulk Policy Assignment – The number of data assets a typical organisation must manage is in the millions. That makes performing operations in bulk an absolute necessity. Alation provides a stewardship workbench for doing exactly that. It allows a steward to identify assets that meet specific criteria, such as not having an owner assigned or an associated usage policy, and then manage them *en masse*.



Documenting Risk Assessment – Alation Data Catalog allows stewards to create a risk assessment review, document it, and associate it directly to the related assets. This becomes an important part of the risk management audit trail. It's also visible and used by all personnel responsible for providing access, sharing, and using the data.



Change Identification and Management – Alation automatically identifies changes to both physical data structures and logical metadata classification of assets. These changes trigger notification to the responsible stewards. The data catalog also tracks the relationship between assets and creates a lineage representation so stewards can run impact analysis reports and better understand how assets are linked.



Usage Understanding and Reporting – The Alation catalog continually analyses the usage of data assets by ingesting query logs with its scanners. The resulting usage data can be analysed with Alation Analytics to understand gaps between data usage and risk compliance policies.

Three keys to getting started

1. Engage a DCAM assessment partner, such as Ortech, and complete the assessment of the as-is state.
2. Create a strategic plan, including immediate actions for the regulator.
3. Establish a catalog program in support of processes and roles covered by the plan.

Authors



Mark McQueen is the Managing Partner-US at Ortecha, a data and analytics consultancy serving clients globally from offices in the US and UK. He leads the Data & Analytics Management practice focusing on leveraging industry standard best practices to optimise client data value. Mark has 25+ years of experience in business process design and data management and served five years as a Senior Advisor to the Enterprise Data Management Council responsible for DCAM product management.



John Wills is the former Field CTO at Alation and the founder & principal of Prentice Gate Advisors. He focuses on catalog adoption, governance, and automation and is a frequent writer and speaker on industry trends. John has 30+ years of experience in data management, holds numerous architecture certifications, and has authored several methodologies

Alation and Ortecha are Authorised Partners of the EDM Council for DCAM and the new Cloud Data Management Capability Model®

Disclaimer: This paper is not legal advice; users are encouraged to obtain professional advice about the application of any legislation or standards relevant to their circumstances.



the Data & Analytics enablers

www.ortecha.com