Gresham

Banking in the dark

Data control framework for the new risk era

Gresham Guide

November 2015

Regulatory Compliance | Internal Risk Control | Financial Control | Transition Management

Contents

During the first, frantic days of the financial crisis in 2008, banks and financial institutions across the world scrambled to assess their exposure to Lehman Brothers and other casualties of the market crash.

It soon became clear that a significant number were operating inadequate and outdated data architecture, which left them unable to aggregate the necessary information quickly enough to take action on the risk.

The issue was compounded for many by entirely siloed functions and processes; banking divisions were dealing with their own levels of exposure, while foreign exchange, fixed income, and multiple other departments were too. The result was wholesale fragmentation, and a near impossible task to collate relevant information across numerous legal entities.

BCBS 239, 'Principles for Effective Risk Data Aggregation and Reporting' was published by the Basel Committee in January 2013 as a response to the crisis, with the aim of ensuring banks could monitor risks properly and report on them quickly and efficiently.

Applying to Global Systemically Important Banks (G-SIBS) initially, BCBS 239 comes into force in January 2016, by which time these larger institutions should be ready to meet the regulations.

Executive Summary

The individuals responsible for managing operational risk in large banks are firefighting multiple challenges; external and internal threats, disjointed systems, departments and processes, and new regulation that needs implementing to tight timescales.

Robust and agile control frameworks are critical.

In this Gresham Guide we assess the impact of some of the latest directives designed to combat banking risk, cut through to the critical requirements for safe, transparent data management, and provide practical advice on getting your systems compliant, operating with greater efficiency and implementing risk controls that can power innovation.

What does BCBS 239 hope to achieve?

The aim is a stronger marriage between data accuracy and timeliness, with the robustness to handle everyday data requirements, as well as flag and mitigate risks during times of crisis.

With clarity and better quality information, the Committee argues, banks will be better placed to facilitate informed – and fast - decision making.

It's certainly an argument that needs little selling into the banks, whose bruises from the financial crisis are far from healed.

Alongside the issues highlighted by the crash, the case for improved data transparency has assumed even greater urgency over recent years as a result of high profile criminal cases involving concealed insider trading.

While significant political and public pressure remains on the financial industry to prove its integrity, banks know they need to take the matter seriously. BCBS 239 provides an industry standard and an impetus for banks to get their data houses in order.

But though the regulation is well intentioned, it brings with it two critical problems:

1. It's a guideline only.

There are no metrics provided, no prescriptive rules. Instead banks are advised that reports 'should be comprehensive', that the frequency 'should reflect the needs of recipients', that risk data should be generated 'in a timely manner'.

But what works for one bank will be wholly different for another. If financial institutions are unable to follow the letter of this law, can they be relied on to follow the spirit of it?

Is there a chance that banks could pay lip service to the principles, and won't reposition to place strategic risk management at the heart of their operations – as is the new regulation's intention?

2. Not enough time.

The timescale to implement BCBS 239 has been far too short. For the majority of global banks, whose operations are often widely spread and whose data is held in disparate formats, in multiple locations and managed via myriad systems, the task of re-working long-standing processes can be immense. Though the aim of the legislation is to be applauded, in order to implement it properly and effectively, banks need more time. There's a very real chance that in order to meet the deadline, even the most well-intentioned institutions will refer to quick fixes and sticking plasters – and sticking plasters come off over time.

Changing mindsets

Until now, banking data risk has been viewed as a tactical function, passing between IT and operations. For BCBS 239 to be successful, and in order for banks to validate the importance of data risk it needs to become a business change issue and involve every functional department as well as the highest level of management.

But in order to achieve buy-in, it needs a change in mindset – one that re-evaluates data risk as a strategic investment, rather than a cost.

And this investment has the potential to pay dividends way beyond risk. It could in fact ignite a new era of smarter banking. One in which the data that is harvested to analyse risk is used to extract more meaningful predictive analytics – not only to identify potential areas of concern, but also trends and opportunities. While data remains a homogenous mass for banks, not only is the risk higher, but opportunities are hidden.

With a holistic approach to realigning internal culture, this could be the start of a new era of proactive risk management and better banking.

The cost of doing nothing has the potential to be far too great.

Improving data control frameworks – what's the issue?

From front office trading to product sales, OTC products to exchange based assets, FX, fpML and internet and mobile transactions across multiple territories and time zones, the amount of data being processed and collected by banks has grown exponentially over recent years.

As a result, banking IT has become far from linear, and instead a patchwork of different systems, offshored processes and complex data feeds. Nothing is joined up.

The consequence is a lack of control. Exceptions are missed. Risk reporting is hit and miss. And while management reports take weeks to produce, the data is almost immediately out of date.

Aside from an inability to identify and manage external risk, the uncomfortable truth is that poor risk structures make discrepancies easier to hide – opening them up to internal abuse.

FCA fines:

2013 - £474m, 2014 - £1.47bn, 2015 - £900m

www.fca.org.uk

What happens when the right controls aren't in place?

In a recent high profile case, a rogue trader cost a major global bank $billions by concealing illicit and reckless ETF trades across multiple systems and spreadsheets.

Without a stringent control framework, the trader was able to keep his activity off the radar of his supervisors, entering false information into the bank's systems, while tracking his secret deals offline. Because reconciliations were handled in batch mode, rather than real-time, his behaviour was able to go unnoticed for several months.

Aside from extensive financial losses, when the trading was revealed, the bank suffered a serious decline in its share price, while several of its senior management were forced to resign. The final, painful sting in the tail was a £29 million fine from the FCA in lieu of the bank's lack of internal controls.

Though extreme, this is a scenario that many banks could find themselves in – and it was perhaps simply a matter of time before any one of them received this particular wake up call.

Many banks know that there are holes in their systems that are open to abuse. But instead of dealing with the problem head on, it's clear that a significant number are still more likely to plan for the aftermath of a breach, instead of shoring up their defences in advance. Many even have funds set aside in anticipation of regulatory fines and loss due to unscrupulous internal practices – funds that could be invested in implementing controls and measures to prevent these practices from happening in the first place.

Those who have attempted to deal with the issue have often turned to end-user computing solutions – applications developed by the end user because their bank's existing IT infrastructure is unable to on-board new, robust controls quickly enough.

The result is more patching.

But imagine if it wasn't just a case of filling in holes? If there was a new way of on-boarding controls quickly and with little disruption? And if these controls could extend beyond trade information and data to monitor trader behaviour?

In the case highlighted here, if the bank had been able to review historical data on the trader's entry access to the building and match against his social media activity, they would have been able to highlight discrepancies in his behaviour and red-flag an area of risk.

Banks pay out £166bn over six years:

'The global banking industry racked up more than £166bn in fines, settlement fees and provisions between 2009 and 2013'.

www.theguardian.com

What do banks need?

In short, new control frameworks that reflect the realities of modern banking. Creaking legacy infrastructures, disparate locations and offline working are simply serving to increase risk, just at a time reducing it should be the front and centre focus of every banking business.

As banking continues to evolve at a rapid rate, bringing with it a vast number of new datasets and more stringent regulation, the ability to provide accurate, frequent risk aggregation reports – as well as red-flag any exceptions in real-time – has become business critical. For senior management, for whom risk is no longer just an organisational issue, but could see them held personally liable for any breaches, it's even more important.

The only way to keep pace is with a flexible, adaptable control framework. One that can on-board new regulation and implement it across multiple data feeds simultaneously. One that isn't constrained by complex data structures – that can process big data; not just talk about it. One that can adapt to new controls without a heavy reliance on IT and provide the capacity to integrate deep-dive analytical capabilities.

A system to meet the risks of modern banking

The Basel Committee has thankfully acknowledged that the timeframe for BCBS 239 compliance is particularly tight and that adherence to all of the stringent criteria may be a step too far for some of the G-SIBs included in the first wave (the D-SIBs who were spared the Committee's full attention this time around are likely to follow on shortly, with national supervisors already advised to include them in scope). Evidence of action by the January deadline will be enough in some instances to satisfy the regulator – but this free pass won't last for long.

For those banks who haven't had the time to properly achieve BCBS 239 the roadmap for full compliance should be as follows:

1. **Tick the boxes**
2. **Adapt over time**
3. **Get the regulations to work for you**

> The question for banks to ask themselves is whether 'good enough for compliance' will actually be 'good enough'.

The vagueness of the legislation is an open invitation to push control as far as the banks see fit. How far they decide to go in meeting the spirit of the principles is a matter of their willingness to place risk at their heart of their business.

The good news is that technology is available to help. Ten, or even five years ago, a change in procedure like this would have been akin to redirecting an oil tanker – a sluggish process requiring every legacy system and dataset to be modified and reworked.

Now, flexible 'plug in' data integrity platforms, like CTC from Gresham, are designed specifically to provide the agility banks need to change quickly.

Within CTC, controls are stringent, but the flexibility that has been baked into the core architecture means the roadmap to implementation (and compliance) can be reduced to a matter of weeks.

$34.64BN lost to rogue traders in just 5 years
Gresham Research 2015

Fit the data, not the technology

Designed to match multiple feeds, importantly, it can match data in multiple formats of any width and structure. Instead of the data having to work with the technology, the technology accommodates the data, so there's no need for banks to change their labelling and processes using expensive and time consuming ETL tools.

Integrity meanwhile, is baked in. Regulatory controls and capacity are catered for, so not only are the boxes pre-ticked for BCBS 239, but further legislation can be accommodated quickly and efficiently.

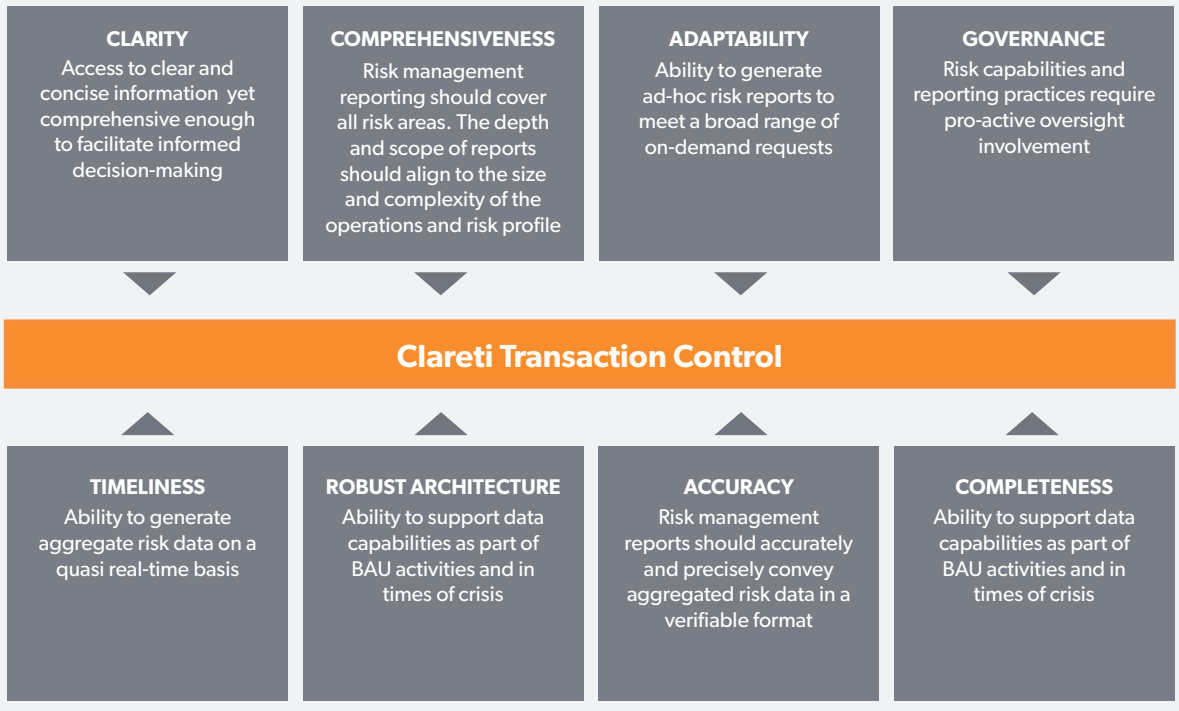
The impetus for change that BCBS 239 and other regulations force upon the banks offers much more than a tick in the compliance box. With aggregation, transparency and visibility, data becomes more useful.

Banks can better marry risk control with risk taking. Much trade risk analysis is currently completed after the trading day. If risk decisions can be made in real-time, via a holistic view of all relevant information, aggregated quickly, exposures can be identified and acted on more quickly.

Only the right technology can provide the smarter foundation that can support this more agile banking era.

Do you have your control framework in place?

Key principles of BCBS239



Checklist: what's your risk exposure?

Interrogate the robustness of your data aggregation and reporting facilities by answering the following questions:

1. Can new controls be implemented quickly and efficiently across every relevant dataset?
2. Is capacity built in to handle new regulations?
3. Can the LEI be integrated easily and efficiently?
4. Are exceptions red-flagged quickly and clearly?
5. Can data be aggregated in real-time and presented in an easy-to use structure?
6. Are reports consistent and valid across every different feed and data format?

Conclusion – better control is an investment in opportunity

For too long, banks have been afraid to invest in data risk management from a fear of what lies under the hood. But good data risk protection can be about augmentation, instead of wholesale replacement.

As we head into 2016, the technology is available to help. When new regulations like BCBS 239 are announced, the availability of smarter, plug and play data handling platforms removes the need for wholesale process change. New legislation can be implemented quickly, while strategic controls can be introduced in a matter of days.

As a consequence, processes are safer, more robust, and better aligned with the speed of modern banking.

But beyond a reduction in risk, they're also better aligned to opportunity.

The front office of banking will always be more innovative, creating new products and services and solving customer challenges (before someone else does). Failure to implement a flexible control framework is a barrier to innovation. When new controls can be added as a simple change to an agile framework, the opportunities for banks are exponential.

2015 will be the worst year in history for UK bank fines:

'Conduct and litigation charges are now a 'way of life' for British banks'.
www.telegraph.co.uk

Technology alone is not enough

In the post-crash era, integrity must lie at the heart of any banking strategy, but in order to effect this cultural change, data risk management has to be viewed as a strategic investment.

Technology like CTC can accelerate this change, but it works best when introduced hand-in-hand with a proactive approach to risk.

With proactivity, banks can stop looking over their shoulders in fear of the regulator, and instead spend time focusing on business growth.

How easy is it to control risk with your existing systems?

CTC from Gresham is the enterprise data integrity platform. With regulatory compliance built-in and the ability to match multiple feeds in multiple formats, it provides a quick-to-install data control framework that can be implemented across your financial institution in a matter of weeks.

Take a free demo of CTC using your live data and discover where the risks in your control systems currently lie.

Whether you're BCBS 239 ready, or need some help fulfilling your obligations, if you would like a session with our product experts to identify integrity gaps and opportunities within your control framework please get in touch at greshamtech.com/contact.

UK
+44 (0)20 7653 0222

Europe
+352 691 358 277

North America
+1 646 943 5955

Asia Pacific - Singapore
+65 6832 5166

Asia Pacific - Sydney
+61 (0)2 8514 7007

greshamtech.com @greshamtech #InternalRisk