Bank Governance
Leadership Network

November 2021

BGLN

SUMMARY of THEMES

Developing effective data strategies in banking

On November 3, 2021, Bank Governance Leadership Network (BGLN) participants met virtually to discuss evolving challenges, risks, and opportunities in how banks collect, store, analyze, and use data. Participants were joined by guests including Christophe Tummers, group chief data officer, UBS; Kim Crider, former chief data officer, US Air Force; and John Bottega, president, EDM Council.

Banks can be fast followers, assuming they get some basics right

Financial institutions maintain huge swaths of valuable data, and most have focused time and investment on upgrading systems and identifying ways to better use that information. In a previous discussion, a tech executive proclaimed, *“The name of the game is data. Whoever has the data and controls the data has the opportunity to do whatever they want.”* Some have suggested banks would have to compete with big tech companies and fintechs to be leaders in data and analytics. An executive shared a slightly different perspective on the competitive threat to banks and how they might respond: *“If we are very, very good at following, at looking at markets, trying things, not being hesitant when the time comes … You combine that with the knowledge and operational experience we have, I think banks can do quite well.”*

Participants discussed requirements to allow banks to be fast followers when it comes to data management:

- **Ensuring data is organized and accessible.** A participant said, *“Your data needs to be discoverable, actionable and usable, trusted and accessible, but also controlled.”* Large financial institutions have often struggled to leverage their data effectively due to the way they have gathered and stored data in silos across sprawling digital infrastructures pieced together across businesses. Banks are working toward a shared taxonomy across their businesses and across banks and providers. They are still in the process of categorizing the data they have and where that data resides to *“combine data into a single understanding.”* An executive said, *“Many banks have grown via a lot of mergers and acquisitions creating quite a distributed environment.”* Another participant said, *“For banks that have grown and have multiple environments, the notion of collecting all your data and making necessary data accessible is going to be a big game changer for firms to be fast followers.”* That allows banks to *“build an internal market for data,”* according to one participant, clarifying, *“We encourage people to publish data sets they feel are valuable and enable anyone at the* *firm to use that data and find it easily. You need to make sure that data is unambiguously defined, and then provide the ability access it, like an app store for data."*

- **Navigating regulatory compliance and leveraging new requirements.** Participants stressed the challenge of promoting agility, particularly with regards to significant data management upgrades, in the highly regulated banking sector. A director said, *"Any change we make, any new data systems we put in place, we have to meet stringent regulatory requirements. It's tough to do that efficiently."* For banks, any noncompliance can often lead to requirements that they address systems failures, distracting resources from business upgrades, but also offering potential to leverage required investment for multiple objectives. A participant observed, *"You need to remain compliant. The moment you go into noncompliance you are in the penalty box. Staying out of the penalty box allows you to be a fast follower, but once you are in it … it essentially means the board and management are focused on trying to get out of it, rather than focusing on proactive changes."* As regulatory requirements like GDPR, PSD2, state privacy rules, and BCBS939 come into effect, they can provide banks an opportunity to invest more broadly in improvements to data management. A participant said, *"GDPR was a great opportunity to finally look at our archives and modernize the technology. No one wants to make that investment to modernize archives, but the business case for it is fantastic, and the GDPR lens forced us to make that connection."* The same participant continued, *"We look at all of our regulatory programs, first from a compliance perspective but also a horizontal view and say, 'If this is connected, what's the business case?'"* Such upgrades can also make responding to future compliance demands easier and less costly.

- **Ensuring they have sufficient talent and expertise.** The growing importance of data management has resulted in a scarcity of talent, participants said. One said, *"Any emerging technology or emerging area of concern, there is always a battle for talent…There are some skills that are very scarce."* Banks may be able to differentiate themselves due to the huge amount of data they have, and unique institutional needs to better leverage it. An executive proposed, *"In banking, you have to present it as an opportunity to actually apply data science. I do think we will find good talent through that approach."* Although participants said that technical skills are often in short supply, the most desired skillsets are even more scarce: *"You can find a lot of people who know all the frameworks, have the technical skills, but then how do they take something that is academic in nature like a data management framework, and make it practically applicable to a bank and implement it at a speed the firm can absorb? That's where pragmatism comes into play as a skill, understanding it's not going to be perfect, but it can be good enough. That skillset is the hardest to come by in my opinion,"* noted one participant.

- **Retaining awareness of concerns about ethical use of data.** BGLN participants have consistently shared concerns about ensuring ethical uses of data and avoiding bias in outputs, particularly as AI and machine learning technology is employed. A director said, *"How do you ensure that your artificial intelligence and machine learning algorithms are not skewing off track based off bad or biased data?"* Stakeholders are increasingly focused on this issue. A participant said, *"Regulators want to know that data is being protected. And consumers want to know that the data is being collected and protected properly. Ethics is a major focus. With the advances of AI and machine learning … like every new technology, there is great stuff but, especially in this industry, we can misuse it in a major way if we're not careful."*

Data security is more critical than ever

Perhaps nowhere is it more important for banks to get the basics right than with regards to data security. Digitalization, remote work, and an expanding ecosystem of partners and providers have exposed firms to more risks as recent high-profile breaches have further underscored the importance of data security for all businesses, not just banks. An executive said, *"Information security is everybody's problem. It's not just third parties, it's not just banking. Look at the breaches that have occurred in the past several years that cut across industries."* Participants discussed key considerations as banks work to prioritize data security:

- **Security and accessibility require a careful balance.** As one director noted, *"Dealing with data access is a major challenge. The more you bring data together, the more you want people to access it. So, figuring out how to manage those restrictions effectively is a source of focus."* Another stated, *"The balance we should all be trying to strike is really about trying to maintain both optimum usability and optimum security in terms of accessibility by authorized users,"* which is not always straightforward. As banks continue to explore ways to leverage data, they must weigh the benefits of accessibility against protection. A participant observed, *"It really depends on how sensitive your data is, both to you as the owner of the data and also what would the consequences be if that data was misused or corrupted."* Data experts promote identifying and protecting the "crown jewels", the business processes and data that are most critical to the company and thus most important to protect. Another participant said, *"For the most part, people who really value their data are going to lean more towards security, making sure they have scalable, flexible, trust-based systems that will enable their data, but protecting that data is much as they possibly can."*

- **'Zero trust' architectures are becoming the accepted standard for data access.** To improve data security many banks are moving to a 'zero trust' model, which attempts to remove the concept of trust from an organization's network architecture, requiring continuous and thorough authentication processes for data access. A participant said, *"There has been an evolution in the use of data as data has moved into ecosystems where there are no walls. More data on the cloud, more data outside the perimeter, people working from home, but we want the data to be usable and accessible and secure. To deal with that, we must go to this new model of assuming anyone who needs to access the data* *is untrusted until they can be verified and validated. It enables a more fluid flow of information, more scalability, and much more effective ways to make sure you are getting the right data to the right people."* Another said, *"Zero trust really fundamentally comes down to the idea that no user, no server, no device, is trusted until verified."* Participants noted that implementation of zero trust can be a costly and time-intensive process and may be best done in pieces and select areas. For many businesses, it is still early days for the zero-trust model, a participant said, *"Data is everywhere, users are everywhere, and people are quickly waking up to the fact that we need a new model, so zero trust is moving quickly but most organizations are not there yet in terms of fully implementing it."* For bank boards, it is important to communicate with management regarding progress in this area. *"It's very important to look to your CIO, CDO, or CISO and ask where the users are and where is the data and what do we need to do to put in place more of these zero-trust models to ensure more effective, secure access to the data while verifying trust of individuals coming into the system."* recommended a participant.

- **Data risk should be managed like other well-understood risks.** The strategic importance of data, as well as the potential risks of mismanaging it, have made it increasingly critical to financial institutions and thus should be overseen like other strategically important risk areas, participants said. A director stated, *"Simply, data represents risk to the firm, and you have to, in some way or form, quantify that risk and establish what management is doing to manage that risk more effectively."* Another participant said, *"There is a big, big linkage between data management and operational risk. How is your data management framework integrated into your operational risk framework? In many cases, you will see people have not joined them up."* Like other risks, establishing a risk tolerance can be useful in this area: *"How do you benchmark data security? It kind of comes down to how much can you stomach? If there is a data breach, and there is a huge chance you'll have one, can you live with the time, energy, and cost it will take to clean it up? Are you willing to assume that potential risk?"*

Prioritizing investment in data management capabilities

As banks continue on the path towards digitalization, data management will continue to be an increasingly central focus of investment. Participants identified some ways to maximize those investments:

- **Management needs to help boards understand the costs and value of investments.** Boards need to understand how technology spend is being used to better assess additional investments in data management. A participant said, *"It's all about awareness. Too often in large organizations there is a lack of awareness of where the money is being spent to put that data in front of you. Once you understand that, it's easier to make the pitch on the investment side."* Though several participants agreed that the costs can be difficult to forecast, they insisted that a business case can and should be made. A participant said, *"I'm making this investment, I'm paying for better security and data management, so what is it going to do downstream for my ability to generate revenue? You want your management to be thinking of business purpose outcomes generating competitive advantage."* Boards should lean on management in this area. According to another participant, *"The CDO's role is identifying the crown jewels and directing spend to the most critical parts of the organization. That's how you not only build a business case but also make sure you are balancing other priorities."* Cost should also be weighed against potential risks associated with insufficient investments. A participant said, *"I've tried for years now to put a number value on this, I haven't been successful … But really, there is a benchmark of fines in the market if you don't get it right and it's quite public. At a big institution, there is definitely a big avoidance factor."* Another said, *"If you're doing it the right way, this is not a balance sheet destroying investment, this is just doing things smartly … The risks and the inefficiencies of getting the data wrong absolutely outweigh the investment."*

- **Firms must navigate challenges of competing board and management priorities.** One director said, *"It's not a reluctance to pay what it takes to govern data, it's more about the capacity to spend the money when you have so many competing programs in your discretionary spend portfolio."* Yet, another participant asserted that the strategic importance of effective data management means, *"Data cannot be considered discretionary spend, it's got to be part of the day-to-day activity spend of the company."* A director noted the challenge of balancing competing priorities: *"When you talk about one topic it all sounds so simple, but for the board it's never just one, and it's competing against so many things. We have to do these things, but it's more of a question of how to get it done rather than a lack of willingness to take action."*

- **Investment is necessary to enable deployment of emerging technologies.** Banks are increasingly turning to AI and machine learning to help unlock the value of the enormous swaths of data they maintain, particularly as they move more data to the cloud. Improving data management can fast track the deployment and effectiveness of new technologies, while also improving costs. A participant said, *"Most of the cost and lead time for AI goes into the extraction and cleanup of the data. Getting ahead of that now will allow you to leverage those technologies more effectively in the future."* Investing in emerging technologies will also permit banks to assume a more offensive posture with data management. *"The financial crisis brought a lot of attention to the defensive,"* according to one participant, *"We have seen a shift to offensive. How do you use data for good? To increase revenue? What about wallet share? From a social perspective, look at what is happening today; the data collected from cell phones, this is using data for public good. It doesn't mean you take the eye off the defensive. Boards need to be asking what management is doing to service both perspectives."*

- **New applications are making it easier to improve data capabilities.** While many banks have focused on creating "data warehouses" or "data lakes" to allow better analysis, one participant said, *"I think we have now reached a point where you can actually bring the computer to the data instead of the data to the computer. There are applications that allow you to create a layer across all your data sources. That obviously opens an entirely new set of opportunities and obviously some challenges."*

Ultimately, boards should expect *"a program of improvements and updates. Understanding that it's never going to be 100%, but asking, 'Is it good enough to make progress?'"*

The perspectives presented in this document are the sole responsibility of Tapestry Networks and do not necessarily reflect the views of any individual bank, its directors or executives, regulators or supervisors, or EY. Please consult your counselors for specific advice. EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. This material is prepared and copyrighted by Tapestry Networks with all rights reserved. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends. Tapestry Networks and the associated logos are trademarks of Tapestry Networks, Inc., and EY and the associated logos are trademarks of EYGM Ltd.

Appendix

The following individuals participated in this discussion:

Meeting participants

- Homaira Akbari, Non-Executive Director, Santander
- John Bottega, President, EDM Council
- Michael Cole-Fontayn, Non-Executive Director, JPMorgan Securities
- Kim Crider, Former Chief Technology Innovation Officer, US Space Force
- Tobias Guldimann, Audit and Risk Committee Chair, Edmond de Rothschild
- Brad Hu, Former Chief Risk Officer, Citigroup
- Phil Kenworthy, Non-Executive Director, ClearBank
- Marty Pfinsgraff, Risk Committee Chair, PNC Financial
- Sarah Russell, Audit Committee Chair, Nordea
- Mark Seligman, Senior Independent Director, NatWest
- Gavin Smyth, Chief Risk Officer, Nationwide Building Society
- Christophe Tummers, Managing Director, UBS
- Tom Woods, Non-Executive Director, Bank of America

EY

- Jan Bellens, Global Banking and Capital Markets Leader

Tapestry Networks

- Dennis Andrade, Partner
- Brennan Kerrigan, Senior Associate
- Tucker Nielsen, Principal