Leo, Martin

Article

Operational resilience disclosures by banks: analysis of annual reports

Risks

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Leo, Martin (2020) : Operational resilience disclosures by banks: analysis of annual reports, Risks, ISSN 2227-9091, MDPI, Basel, Vol. 8, Iss. 4, pp. 1-15, https://doi.org/10.3390/risks8040128

This Version is available at:
https://hdl.handle.net/10419/258081

risks

MDPI

Article

Operational Resilience Disclosures by Banks: Analysis of Annual Reports

Martin Leo

The Department of Finance, S P Jain School of Global Management, 10 Hyderabad Road, Singapore 119579, Singapore; martin.dbaon01009@spjain.org

Received: 3 November 2020; Accepted: 23 November 2020; Published: 1 December 2020

Abstract: An array of developments impacting the financial services industry, such as increasing complexity, interconnectedness, third party dependencies and digitalization, means operational resilience will remain a significant area of concern for policy makers, investors and customers. The purpose of this study is to evaluate if banks are disclosing information on their operational resilience risk. The study initially reviews the regulatory landscape for operational resiliency. The recent annual reports of the GSIB banks are reviewed to identify if they have made references to operational resilience. Through text mining, a frequency analysis of terms related to operational resilience was done, followed by an evaluation to understand the existence of relationships between these terms. The study shows that the regulatory guidance for operational resilience is still evolving with much of the current impetus on cybersecurity. There is a notable gap between banks that have reported on operational resiliency and those that have not, with a few patterns visible. Research in the area of operational resilience is relatively new and limited, and this research for the first time analyses the disclosures related to operational resilience in annual reports. Further, for policymakers, it highlights the disparity in disclosures around this relatively new area of risk, thus calling for additional regulatory guidance.

Keywords: operational resilience; operational risk; bank; GSIB

1. Introduction

The financial services sector as a whole is becoming more complex, with the larger firms providing a significantly large number of services to clients. The delivery of these services is supported by a very significant amount of operational infrastructure. There is also an increasing demand for digital services, with customers coming to rely more heavily on digital channels. Customer and market participant expectations regarding the availability of financial services have dramatically changed with 24 h access to services being the expectation. This has brought the resilience and availability of the delivery channels into sharper focus as even a brief service disruption could cause significant concern (European Commission 2019).

Resilience is broadly defined as "the capacity of a system to avoid disturbance and reorganize while undergoing change so as to still retain essentially the same function, structure, identity, and feedbacks" (Walker et al. 2004). It is a concept with a multidisciplinary pedigree that focuses on the dynamic capacity of a complex, adaptive, nonlinear system to self-repair in response to stress or transition to a new stable equilibrium. The tendency of the globally integrated financial system to oscillate from one crisis to another makes resiliency an essential concept for the financial system. This term has come to feature prominently in regulatory and supervisory discourse and documents since the financial crisis (Dowell-Jones and Buckley 2016).

The Regulators are starting to closely supervise operational risks and resilience. Regulators explained that "a resilient financial system is one that can absorb shocks rather than contribute to

them", and defined operational resilience as "the ability to prevent, adapt and respond to, and recover and learn from, technology, cyber-related and any other operational incidents". Operational resilience is now considered a priority issue, both from a regulatory perspective and within the financial services sector (European Commission 2019).

In 2019, the UK's financial regulators, the Bank of England (BoE), Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), published a series of consultation papers (CPs) on their proposed approach to operational resilience in the financial sector. The publication was on the back of much scrutiny around IT failures and breaches occurring in the financial sector. As stated in the foreword of the discussion paper titled 'Building the UK financial sector's operational resilience,' operational disruption can "impact financial stability, threaten the viability of individual firms and FMIs or cause harm to consumers and other market participants in the financial system".

The focus of post-financial crisis reforms has been on the resilience of the financial system to 'withstand, re-route and recombine in the wake of a potentially catastrophic event to maintain systemic operability' so that it can 'withstand, recover and bounce back from crisis'. In November 2011, the FSB published an integrated set of policy measures to address the systemic and moral hazard risks associated with systemically important financial institutions (SIFIs). In that publication, the FSB identified as global systemically important financial institutions (G-SIFIs) an initial group of Global Systemically Important Banks (GSIB), using a methodology developed by the BCBS. The FSB, in consultation with the BCBS, issued the revised list of GSIBs in November 2019 (FSB 2019).

The 2018 list of GSIBs together held more than $50 trillion in assets accounting for more than one-third of the global banking system's total assets and loans. These institutions play an essential role in international capital market services, international financial infrastructure and international lending activities. The collective dominance of these institutions makes them central to the provision of global financial services and the stability of the global financial system (Caparusso et al. 2019).

BCBS' operational risk principle 12 specifies that a bank's public disclosures should allow stakeholders to assess its approach to operational risk management and its operational risk exposure. It further expects that the amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations, and evolving industry practice. Corporate disclosure documents, such as annual reports and SEC 10-Ks, are a prime source of information for shareholders and markets. These documents are required to provide not only a backward-looking analysis of year-on-year profitability but also forward-looking information. The annual reports are important channels of shareholder communication, particularly about the company's business strategy and significant risks. It is therefore expected that important messages around risks—including risks and strategies related to operational resiliency—would be highlighted in these communications.

With the increasing attention on the topic of operational resilience, this paper studies whether banks, as part of annual reports, have made disclosures about operational resilience.

The research focused on the GSIBs and the risk disclosures made in their annual reports. Text analysis was conducted on the most recently available annual report of the GSIB to evaluate the following research questions:

1. Is operational resilience, and its related terms mentioned in the annual report and the frequency these terms are mentioned with
2. Is there any relation between the terms related to operational resilience
3. Is there any relation between the terms related to operational resilience and the operational expense of the bank

Section 2 of the paper includes a review of available literature and regulations on operational resilience in the banking industry. Section 3 explains the method for the research. Section 4 provides an analysis with conclusions of the research captured in Section 5.

2. Review of Literature and Regulations

Business models are becoming increasingly digitalized, complex and inter-connected. Technology has advanced a lot over the last many decades, and increasingly in recent times has created a deeply interconnected world. This is notably so in the financial system as no financial institution can survive on its own, isolated from the complex web of financial market infrastructures it is a part of and underpinning its day-to-day business (Lautenschläger 2018; KPMG 2019; Infosys Ltd. 2019).

Disasters, natural or man-made, can potentially cripple or impair an organization's ability to achieve its many business objectives. Firms run the risk that the costs of mitigating and redressing disruptive operational risk events may be compounded by the potential damage to reputation and customer confidence, resulting in loss of business. Organizations must be able to manage these events to be always available. Operational risk events such as cyberattacks, severe weather, health pandemics and power outages drive organizations to develop sophisticated availability measures to ensure uninterrupted business operations. This requires organizations to work with their internal business units, supply chains and business partners. The organization, additionally, must work with external stakeholders also—customers, government bodies, investors and the media. Organizations are required to implement a new paradigm of operational resilience to achieve a comprehensive and continuous level of availability. A firm's enterprise resilience can be divided into strategic resilience, financial resilience and operational resilience. Through the elevation of operational resilience at par with strategic and financial resilience, firms should be able to align the resiliency approach with the strategic goals, thereby holistically anticipating and navigating operational and financial risks (Tapper 2013; KPMG 2019).

Operational resilience is usually defined as "the ability of an organization to adapt rapidly to changing environments". Table 1 provides a list of operational resilience definitions available from various sources. There are a few commonalities between the various definitions available. Key attributes common in the definitions are—the ability of the firm to:

- Prevent the occurrence of a crisis event
- Protect itself from an adverse event
- Responding to and recovering from a crisis event
- Sustain business services in the event of a disruption

Table 1. Definitions for operational resilience available from various sources.

Source/Origin	Definition
Principles for operational resilience (BCBS)	The ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations through disruption.
Building the UK financial sector's operational resilience	The ability of firms, financial market infrastructure (FMI) and the system as whole to prevent, adapt and respond to, recover and learn from operational disruption.
KPMG (2019)	Operational resilience is usually defined as the ability of an organization to adapt rapidly to changing environments. This includes resilience of systems and processes and more generally, the ability of the organization to continue to operate its business in the event of disruptive events.
Carnegie Mellon's Resilience Management Model CERT-RMM	An emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption
(Bradenburg et al. 2019)	Operational resilience is the ability of an organization to continue to provide business services in the face of adverse operational events by anticipating, preventing, recovering from, and adapting to such events.
(Lebaka et al. 2016)	Resilience can be defined as the ability of a system to prevent the occurrence of a crisis and the capacity to absorb the impact and recover to the normal state rapidly and efficiently when a crisis does occur
(PWC 2019)	An organization's ability to protect and sustain the core business services that are key for its clients, both during business as usual and when experiencing operational stress or disruption.
(Finextra and IBM 2016)	The ability to rapidly adapt and respond to dynamic changes—opportunities, demands, disruptions, threats—with limited impact to the business, and with a scope that spans people, process and IT

Operational resilience has become an essential agenda item for boards and senior management. Operational resilience—different from traditional business continuity (BC) and disaster recovery (DR)—focuses on the firm's adaptability to emerging threats, dependencies for providing critical business services end-to-end, and the broader economic as well as firm-specific impact of adverse operational events. Operational resilience includes both the resilience of systems and processes and in general, the ability of the organization to continue to operate its business in the event of disruptive events.

While operational resilience has been a critical topic within the financial services sector ever since banking began, the emergence of digitalization, an increase in the complexity of financial instruments and the expansion of regulations has brought this topic increasingly to the fore. Contributing to these risks is the increasing complexity in the delivery of financial services resultant from the proliferation of innovative products and services. This is concurrent with the existence of legacy IT systems that may not be eliminated as more layers are added on to the technology stack, and these may not all be compatible and adaptable. Change management control procedures could potentially also not be appropriate for an environment that is dynamically transforming, making it more difficult for banks to manage and control operational risk. New concerns related to privacy, customer protection, cybercrime and interconnectedness of the financial systems have led regulators to be increasingly concerned in ensuring that all the participants in the financial services ecosystem are operationally resilient. The likelihood of disruptions has increased with the increasing complexity in operational processes, technology, dependence on third parties (through outsourcing or fintech partnerships), interconnectedness and data sharing within the economy, and sophistication of malicious actors. The impact of these events has also become more severe. The increase in the technological interdependencies among market players and infrastructures could cause an IT risk event to rapidly escalate into a systemic crisis, especially where there is a concentration of services with one or a few dominant players. These factors that are all in play simultaneously could make it more difficult for banks to manage operational risk (Infosys Ltd. 2019; Bradenburg et al. 2019; Hernández 2019; Finextra and IBM 2016).

The importance of operational resilience in the financial industry is greater now than ever, driven by client expectations of 24/7 'always on' service and regulatory regimes that are less tolerant of operational failures. It is an essential underpinning for the achievement of business goals and ensuring that the confidence and trust of the customer and regulator can be satisfactorily retained. Market-leading operational resilience could enable banks to turn the areas most impacted by operational resilience failures into areas for positive differentiation. Resources and attention for resilience compete with similar demands from other business priorities. With retail and commercial banks under threat from disruption and digitally-driven new entrants, the money and focus required to meet operational resilience expectations will be a challenge.

Many firms are embarking or expected to embark on transformational programs to strengthen their resilience to disruption. The strengthening is expected to be across all operational resilience domains—technology, data, third parties, facilities, operations and people. The business benefits are expected to form an inherent part of a firm's proposition, going beyond pure risk and compliance. Operational resilience can enable a firm to achieve a positive outcome to the firms' financial performance and reputation through different sources—(1) avoiding unexpected financial losses from adverse events (2) the ability to serve the client continuously and seamlessly resulting in increased revenues (3) increased revenues (profits) translating to increasing stakeholders' and investors' confidence and the resultant gains (4) ability to avoid potential regulatory fees and losses (PWC 2019).

Carstens (2017) highlights the rapid technological change in financial services as one of the three risks to financial stability from the current perspective. Vigilance is required on the part of the supervisors and regulators for the protection of the depositors and investors. The central role of the financial services industry in society and the wide-ranging impact of a disruptive event has resulted in regulators across the globe increasing their scrutiny of firms' ability to adapt to and recover from operational disruptions. The G20 Finance Ministers and Central Bank Governors noted that "the

malicious use of information and communication technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence, and endanger financial stability" (Basel Committee on Banking Supervision 2018).

Operational resilience has always been an important area of focus for financial institutions and their regulators/supervisors. However, this focus has been limited to a narrow set of risks—IT security and outsourcing. The recent and emerging approach of regulators, in particular the UK regulators, is to take a broader view of operational resilience, covering all risks that could impact the provision of key business services. The range and depth of regulatory requirements are varying across the different regulatory jurisdictions. The focus is increasingly on the response and recovery to an operational disruption and ensuring that the continuity of business services can be preserved in the event of a disruption occurring. This is a fundamental shift towards 'operational resilience' and will have implications for financial institutions globally.

Financial regulators have started to lay out expectations around the management of resilience. The Basel Committee on Banking Supervision (BCBS) introduced its Principles for the Sound Management of Operational Risk in 2003 subsequently revising them in 2011 to incorporate the lessons from the financial crisis. In 2014, the Committee conducted a review of the implementation of the Principles. In August 2020 the BCBS issued a consultative document 'Revisions to the principles for the sound management of operational risk'. Recognizing that the 2011 principles did not cater to risks arising from information and communication technology, a new and specific principle has been introduced in the 2020 version.

The 2011 version has a section on business resiliency and continuity which is revised to just Business Continuity Planning in the 2020 consultative paper. The consultation paper includes a section on Information and Communication Technology (Principle 10). This principle requires that "Banks should implement robust ICT governance that is consistent with their risk appetite and tolerance statement for operational risk and ensures that their ICT fully supports and facilitates their operations." By having a principle specific to ICT, its significance in the context of operational risk is recognized. However, the principle remains tilted more towards the more legacy business continuity management and information security controls as opposed to setting a more ambitious direction for operational resilience. It also does not appear that the risks of newer technologies (e.g., robotics, distributed ledger technology) have been considered.

The BCBS, in August 2020, issued a consultative document titled "Principles for Operational Resilience" citing the need for further work in strengthening a bank's ability to absorb operational risk-related events which could cause significant operational failures or wide-scale disruptions in financial markets. The BCBS believes that operational risk-related events such as pandemics, cyber incidents, technology failures or natural disasters could cause significant operational failures or wide-scale disruptions in financial markets. There is, therefore, the need to strengthen the banks' ability to absorb these risk events increasing their resilience and thereby provide additional safeguards to the financial system. The BCBS seeks to promote a principles-based approach to improving operational resilience through the publication of the consultative document.

The document builds on the Committee's updated principles for the Sound Management of Operational Risk, previously issued governance principles, as well as outsourcing, business continuity and relevant risk management related guidance. The document acknowledges that the most predominant operational risks banks face are from vulnerabilities related to the rapid adoption and dependency on technology infrastructure for the provision of financial services and intermediation. The sector's growing reliance on technology-based services provided by third parties is also acknowledged as a predominant contributor to operational risks.

The focus of the document appears to be more on business continuity, outsourcing though there is a principle related to ensuring 'resilient ICT, including cybersecurity'. There are principles related to 'Mapping interconnections and interdependencies' and 'Third-party dependency management' that are not in the earlier principles document. The consultative document does not take a creative and revised

approach to deliver a more forward-looking and comprehensive set of principles for banks to adopt in the relatively new area of operational resilience. This is, to an extent, acknowledged in the document as it mentions that the principles are 'largely derived and adapted from existing guidance'. Given the changing technology landscape and the increasing digitalization of financial services and emerging technologies, there should have been more effort in providing a refreshed set of principles as opposed to solely adopting the existing guidance. Even in the area of cybersecurity, or what should have been addressed as cyber resilience, the principle falls short. The extensive text around remote-access makes it appear that this has been influenced by the COVID-19 situation where large numbers of employees and contingent workers are operating from home through remote access. A principles document should be addressing a more expansive slate of past, present and emerging risks.

The European Commission (EC) issued a consultative document on digital operational resilience in the area of financial services in December 2019. The document focuses on strengthening the digital operational resilience of the financial sector, in particular as regards the aspects related to ICT and security risk. The EC has noted the need for a dedicated approach to enhance what can be referred to as the digital operational resilience of financial institutions in the context of the increase in outsourcing arrangements and third-party dependencies (e.g., through cloud adoption) (European Commission 2019).

The European Central Bank (ECB) has issued 'Cyber resilience oversight expectations for financial market infrastructures' defining the Eurosystem's expectations in terms of cyber resilience based on global standards.

Recognizing that operational disruption can impact financial stability and potentially impact firms, market infrastructure or consumers the Prudential Regulatory Authority (PRA), the Financial Conduct Authority (FCA) and the Bank of England jointly issued a discussion paper titled "Building the UK financial sector's operational resilience". The paper lays out an expansive approach addressing how the continuity of the services that firms provide can be maintained regardless of the cause of the disruption. Operational disruptions to the products and services that firms and FMIs provide can negatively impact consumers, market participants, threatening the viability of firms or the market infrastructure, potentially impacting the stability of the financial system.

Operational resilience of firms and the financial market infrastructure is a priority for the supervisory authorities and is being viewed as no less important than financial resilience. The discussion paper is among the most comprehensive regulatory publications documents around the topic of operational resilience. Operational resilience is more effectively managed by focusing on business services and therefore, central to the document is the firm's understanding of business services and the prioritization of these services. The risk and control areas the paper addresses are around cyber risks, business continuity and contingency planning, outsourcing and critical service providers.

The Office of the Superintendent of Financial Institutions (OSFI) Canada, an independent federal government agency, issued a discussion paper titled 'Developing Financial Sector Resilience in a Digital World' in September 2020. The paper touches on several technology-related themes, including the priority risk areas of—(a) cybersecurity (b) advanced analytics (c) third party ecosystem (d) digital data. The OSFI has observed that the increasing number of incidents, shifts in the severity of the risk and emerging risks require a better understanding among institutions and regulators. Technology and its risks weigh heavily in the discussion paper with the OSFI also seeking to hear, from respondents, the prevailing view regarding the relationship between operational resilience, operational risk management and technology risks.

The global financial sector continues to transform through rapid technological advancement and digitalization. Financial institutions, markets and infrastructures are more tightly-linked than before, and there is high interdependence on the resiliency of the sector's players and their processes. The forces, namely innovative financial technologies, that are shaping the change in the business models and risk profiles, while known, are generating new non-financial risks and amplifying risks in

the traditional areas. Technology is a crucial enabler for the industry; its widespread use poses risks across the business.

Operational resilience is not entirely a novel concept. ORM requirements include expectations that financial institutions can withstand, recover and maintain continuity of critical operations through a disruption. However, traditional ORM practices tend to be more process-oriented with business continuity management practices, a sub-category of operational risk, not broad enough to capture all the nuances required. Operational resilience is expected to take a more outcomes-based approach to a given adverse event and is based on the premise that disruptions will occur (Canada Office of the Superintendent of Financial Institutions 2020).

The Hong Kong Monetary Authority (HKMA) has issued a framework, the Cybersecurity Fortification Initiative (CFI), to enhance the cyber resilience of regulated institutions. The framework is built around through three elements (a) Cyber Resilience Assessment Framework (b) Professional Development Programme (c) Cyber Intelligence Sharing Platform.

Reserve Bank of New Zealand, in October 2020, issued a consultation document "Guidance on Cyber Resilience". The guidance draws on leading cybersecurity standards and guidelines. The guidance recommends principles for cybersecurity governance, cybersecurity capabilities, information sharing and third-party risk management.

3. Method

This research focussed on the GSIBs. These are large, complex, internationally active banks whose failure could create cross-border spillover risks. Table 2 lists the GSIBs per the FSB (2019).

The primary source of data for this research is the annual reports of the banks. For the research, the most recent annual report available on the website of the GSIB was downloaded. The annual report was downloaded in pdf format.

Based on the literature reviewed, a list of terms related to resilience were determined. These terms were then grouped to have similar terms classified together. As an example, terms related to technology such as 'data', 'automation', 'digital' and 'technology' were grouped under 'technology'. For better search results, for some of these search terms a manual stemming approach was taken. The search term was determined as 'automat' to capture all variations such as 'automation', 'automated'. The search terms and the group they were put in can be found in Table 3. Through text mining, the frequency of the words in each annual report was determined. Frequencies related to the search terms were then summed to arrive at the frequency of terms for the group. The operating expense was manually read from the annual report and added to the data set for further analysis.

It was noted that the term 'operational resilience' or 'operational resiliency' were not explicitly mentioned; therefore an additional analysis was done to extract the text around the word "resilien" (to capture all variants such as 'resilience', 'resiliency'). This text was manually analysed to narrow down to operational resilience references only excluding references to financial resiliency. This was used as the count of the term 'operational resilience' for each bank. The approach ensured a better count of the term instead of just mining the frequency of the word resiliency or resilient. The text extracted, only related to operational resilience, was then processed to plot a word cloud to visualize the word associations.

The data of the terms and their frequency was analysed to determine:

1. Frequency of the terms
2. Correlation between the terms
3. Correlation between the operating expense of the bank and the terms
4. Analysis of the terms in reference to the region of the bank
5. Terms most associated with the text that mentions resilience

Packages in R were used for the text mining and analysis. The functions available in the package *pdfsearch* were primarily used to mine for the keywords within the pdf files. Functions in the packages

tm have been used to prepare the data for plotting the word cloud, followed by functions in the package *wordcloud* for plotting. For charting the data functions in the packages *PerformanceAnalytics*, *ggplot2*, *scatterplot3d* have been used.

Table 2. List of G-SIBs (Source: FSB 2019).

G-SIBs (in Alphabetical Order)
Agricultural Bank of China
Bank of America
Bank of China
Bank of New York Mellon
Barclays
BNP Paribas
China Construction Bank
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
Groupe BPCE
Groupe Crédit Agricole
HSBC
Industrial and Commercial Bank of China
ING Bank
JP Morgan Chase
Mitsubishi UFJ FG
Mizuho FG
Morgan Stanley
Royal Bank of Canada
Santander
Société Générale
Standard Chartered
State Street
Sumitomo Mitsui FG
Toronto Dominion
UBS
UniCredit
Wells Fargo

Table 3. List of terms mined for from the annual reports and the resilience term that they are grouped as.

Search Terms	Resilience Term
data	technology
automat	
digital	
technolog	
technology	
operation	operation
process	
bcp	bcp
business continuity	
disaster recovery	
drp	
cyber-security	security
cyber	
cybersecurity	
data security	
information security	
It security	
resilien	resilience
It resilien	
operational resilien	
system resilien	
outsourc	outsourcing
third-party	
third party	
cloud	-
pandemic	-
system failure	-

4. Analysis

4.1. Occurrence of the Terms

Table 4 shows the descriptive statistics for the various terms, related to resilience, that were mined from the annual reports.

All the banks have made extensive mentions of technology and operation in their annual reports with the relevant terms being mentioned on average 146 times for technology and 273 for operations. While all the banks have made extensive mentions of technology and operation, only 16 (62%) of them made specific mention of operational resilience in their annual reports. The term was mentioned on average at least seven times with the outlier being one bank that mentioned the term nearly 81 times in their annual report. While the extensive mention of the term 'technology' across all banks is reflective of the trend towards digitalization at banks, it appears that operational resilience has not universally been considered a risk despite the growing attention from regulators.

The banks that have mentioned operational resilience have done so in reference to the areas closely related with the analysis showing that of the 16 banks that mentioned operational resilience 5

of them were in the context of outsourcing, 12 in the context of information technology, 7 in the context of business continuity planning and 12 in the context of security. It does show that outsourcing and business continuity planning are not adequately mentioned in the context of operational resilience though they are essential components of operational resiliency as per the regulatory publications.

Table 4. Descriptive statistics for the terms studied from the annual reports of the GSIBs.

	Size (n)	Average	Minimum	Median	Maximum	Standard Deviation	Number of Banks that Have Mentioned the Term at Least 1 Time	% of Banks Mentioning the Term
technology	26	145.77	32	138	300	59.61	26	100%
operation	26	273.46	24	227	808	169.44	26	100%
bcp	26	2.88	0	3	9	2.44	21	81%
security	26	15.42	0	11	45	13.35	25	96%
resilience	26	7.77	0	1	81	16.82	16	62%
outsourcing	26	21.38	0	22	51	15.77	25	96%
cloud	26	2.92	0	2	17	3.57	19	73%
pandemic	26	4.08	0	1	32	6.84	15	58%

Nearly 96% of the banks mentioned security, with the term being mentioned on average at least 15 times in the annual report. This is in line with the heightened attention around cyber security threats and increased activity of malicious actors. Outsourcing was another term reported by 96% of the banks with the term being mentioned nearly 22 times on average. This is reflective of the trend towards outsourcing and engagement of third parties. Banks appear to be treating both as significant topics with outsourcing appearing to be the more significant one. Business continuity planning terms were found in the reports of 21 banks (81%) with the term being mentioned approximately three times. Though outsourcing as a term was mentioned by 96% of the banks, indicating the extent of communication around the topic, in the context of operational resilience, only 5 of 16 banks mentioned outsourcing. Security, however, was mentioned in the context of operational resilience by 12 of the 16 banks. This may indicate that while security is viewed as core to operational resilience by most banks, outsourcing is possibly still not viewed as a significant risk contributor to operational resilience.

Thirteen banks (50%) had mentioned all the terms in their annual reports, namely operational resilience, security, outsourcing and business continuity. These banks have provided comprehensive coverage of reporting by covering all the areas related to operational resilience.

While not directly related to resilience, terms related to cloud were analysed in the context of outsourcing, and increasing usage of cloud services. Cloud was found mentioned in at least 19 of the annual reports with the term appearing three times on average. This indicates the adoption of emerging technologies such as cloud services by banks with widespread implications for operational resilience that could be researched further.

In light of the current situation of the Coronavirus pandemic (COVID-19) the frequency of the term pandemic was also analysed, and it was found that nearly 15 banks had made a mention of it. This term was mentioned on average four times with one bank mentioning it nearly 32 times. Of the four banks that had mentioned pandemic more than 10 times in the recent annual report, only one had also mentioned it last year. A review of the previous year's annual report for the other three banks showed no mention of pandemic. The timing of the report issuance may have had an influence on the mention of pandemic.

Figure 1 shows the banks, by region, that have reported on operational resilience in their annual reports. 100% of the UK banks in the analysis have mentioned operational resilience. On the other extreme, none of the Asian banks analysed had a mention of operational resilience. 75% of the European banks and 88% of the North American banks studied mentioned operational resilience. This can be explained by the limited regulatory guidance issued in the jurisdictions of these Asian GSIBs.

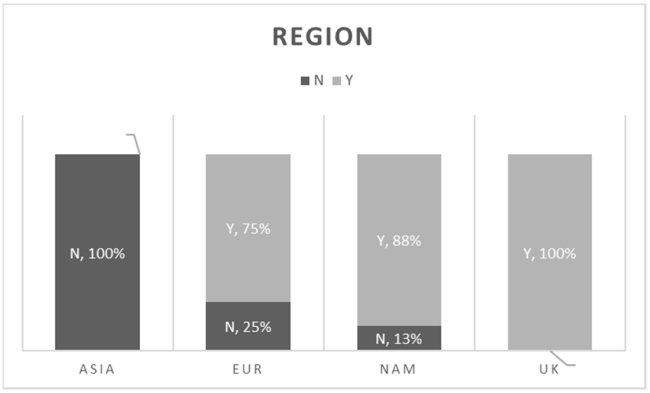

Figure 1. For each region, the percentage of banks (shown as 'Y') that have mentioned operational resilience in the annual report.

Figure 2 plots the frequency of the occurrence of the term resilience against the frequency of technology and operation as it appears in the annual reports. As seen in Figure 2, the UK banks also have a higher frequency of reference to operational resilience. This can be explained by the more advanced regulatory guidance available in the UK.

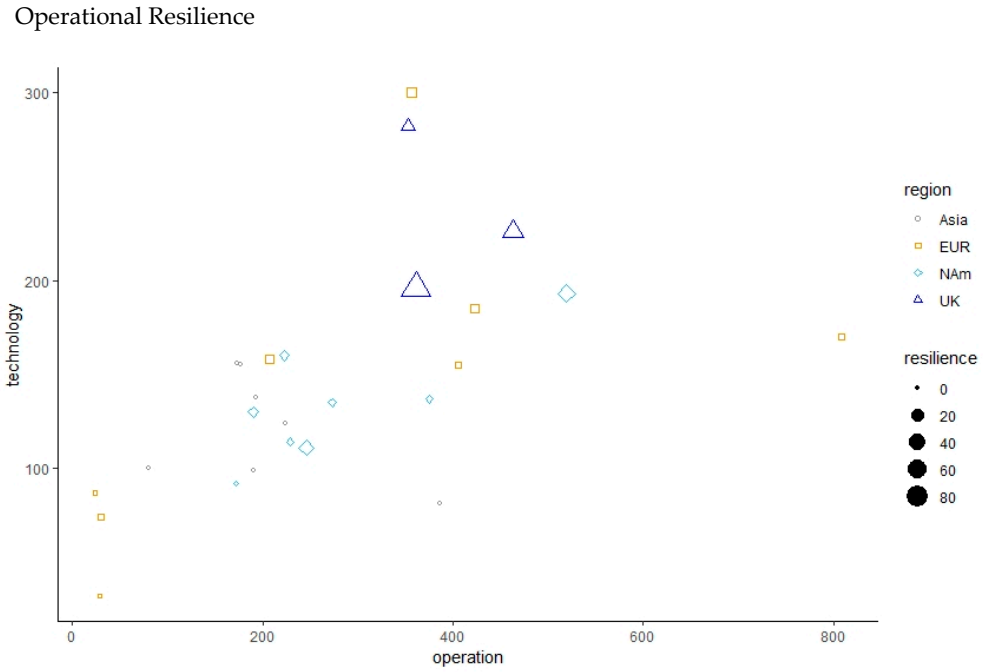

Figure 2. Occurrence of the term resilience (operation resilience) plotted against the frequency of technology and operation as found in the annual reports.

4.2. Distribution of Resilience Terms by Region

Figure 3 shows a distribution of the various terms related to resilience—outsourcing, business continuity, security—by the region of the bank. The disparity in the mention of the three topics is quite evident in the chart, with some banks standing out versus the others. The UK banks are positioned in the centre, with balanced coverage of all three topics. The Asian banks have the lowest numbers amongst the regions with very low counts for the three areas, with business continuity showing comparatively better numbers. The North American banks have better coverage of security and business continuity in comparison to outsourcing. The European banks also have lower numbers in the three areas.

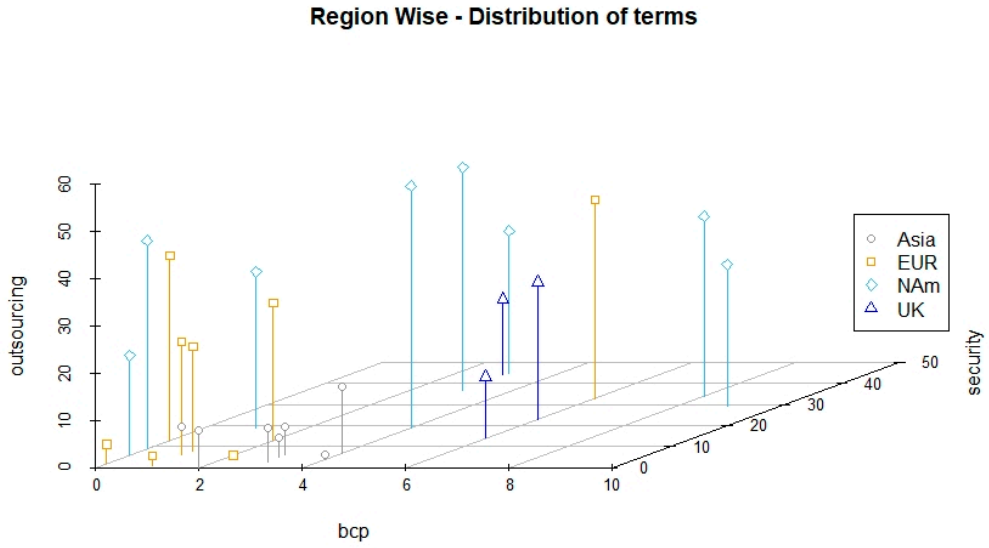

Figure 3. Distribution of resiliency terms by region of the GSIB.

4.3. Relationship between the Terms

Figure 4 is the correlation chart for the different terms, frequencies of which were mined from the annual reports of the GSIB. In the correlation chart below

(a) the distribution of each variable is shown on the diagonal
(b) the bivariate scatter plots with a fitted line are displayed on the bottom of the diagonal
(c) the value of the correlation plus the significance level as stars is shown on the top of the diagonal
(d) each significance level is associated to a symbol: *p*-values (0, 0.001, 0.01, 0.05, 0.1, 1) <=> symbols(***, **, *, .).

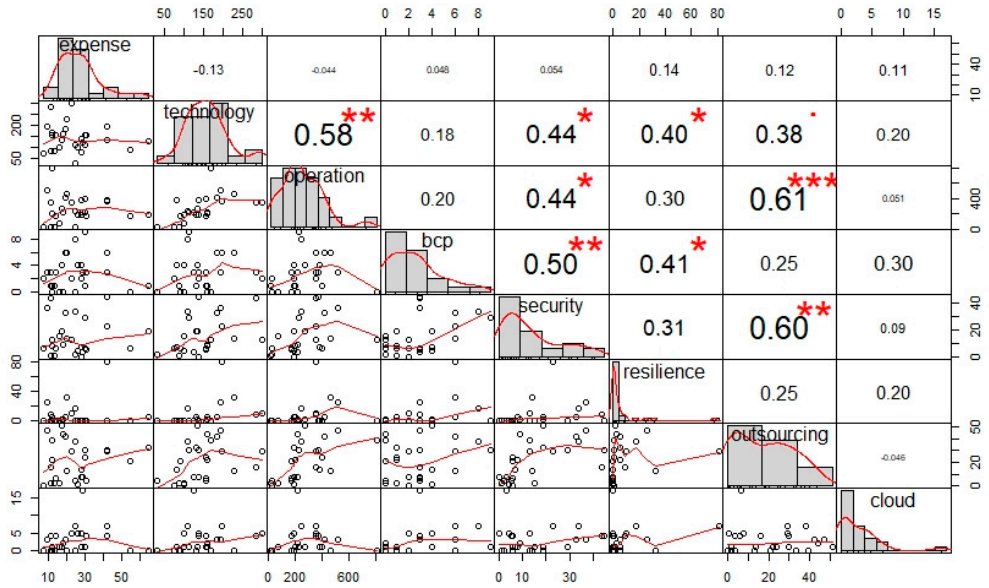

Figure 4. Chart showing the correlation between the frequency of the variables related to resilience as measured from the annual reports. Each significance level is associated to a symbol: *p*-values (0, 0.001, 0.01, 0.05, 0.1, 1) <=> symbols (***, **, *, .).

The chart shows there is sufficient evidence to conclude a significant linear relationship between the following variables mentioned in the annual reports:

1. Technology and operation: Positive correlation, r = 0.58, $p \leq 0.001$
2. Technology and security: Positive correlation, r = 0.44, $p \leq 0.01$
3. Technology and resilience: Positive correlation, r = 0.4, $p \leq 0.01$
4. Operation and security: Positive correlation, r = 0.44, $p \leq 0.01$
5. Operation and outsourcing: Positive correlation, r = 0.61, $p = 0$
6. Bcp and security: Positive correlation, r = 0.5, $p \leq 0.001$
7. Bcp and resilience: Positive correlation, r = 0.41, $p \leq 0.01$
8. Security and outsourcing: Positive correlation, r = 0.6, $p \leq 0.001$

The research shows that there exists a significant relationship between the mention of resilience and technology, though the correlation is only 0.40. The correlation between resilience and operation was found to be only 0.30 and not significant enough to accept that a linear relationship existed.

The study sought to evaluate whether there was a relationship between the bank's operating expense and the mention of operational resilience to understand if banks with higher operating expenses were more focussed on operational resilience. The analysis showed a low correlation of 0.14 (p-value > 0.05) between expense and resilience, showing that no relationship existed between the mention of the term resilience and the expense of the bank.

The text adjoining the word resilience (only related to operational resilience) was extracted, and a word cloud was created to visualize the associations. Figure 5 shows the word cloud and the associations of the words frequently appearing with operational resilience.

Figure 5. Word cloud for the text around operational resilience.

The research focused only the GSIB banks, and due to file formats and language, the analysis could be done on only 26 banks. The APAC region has many countries and banking regulators and the GSIBs are concentrated only in two countries, which would have had an impact on the regional analysis. While due care has been taken in identifying the terms for the search and analysis, some variants could have been missed. To search for terms related to cybersecurity, 'security' was not used as this may have also captured references to financial security. This exclusion may have resulted in a few terms not being mined.

5. Conclusions

After the events of 2007–2008 provided evidence that significant systemic risks could emerge and escalate from within the financial system, there was extensive regulatory guidance from the regulators to ensure financial resilience. Regulators have moved earlier in the area of operational resilience, recognizing the rapid digital transformation at banks and the parallel advancing threat landscape. Many regulators have recently issued consultative documents for enhancing non-financial

resilience. The extent of regulatory guidance for operational resilience still lags behind what is available for financial resilience. The BoE, PRA and FCA have been the front runners, issuing a comprehensive document for operational resilience; the BIS has only recently issued a dedicated document on operational resilience. Most of the regulatory publications on resiliency are more focused on cybersecurity. While this is the most significant threat, operational resiliency is much deeper and complex, and there is a need to have more comprehensive regulatory guidance to ensure a truly operationally resilient bank and consequently an operationally resilient financial system. Comprehensive regulatory guidance will ensure that the efforts are not overtly focused on one threat area, resulting in siloed control capabilities, defeating the intended objectives of resilience. Regulatory publications should also include guidance to manage risks from new and emerging technologies and operating models. While a few regulators have addressed cyber resiliency testing, the area of operational resiliency testing would benefit from further guidance.

This paper analyses the extent to which banks, namely the GSIBs, have made disclosures, in their annual reports, with regards to operational resilience on whether and, if so, the extent to which companies make disclosures around operational resilience within their annual reports. The analyses of GSIB annual reports show that the extent to which operational resilience is reported on is limited. There are disparities in the reporting of operational resilience in terms covered, the number of times referred to and the extent to which the various topics are covered. While all the banks analysed had a broad mention of technology and operation in the annual report, operational resilience was mentioned only by 62% of the banks. Security and outsourcing were mentioned in annual reports of 96% of the banks. The reporting by banks in certain regions is far better than other regions, and this can be attributed to the extent of regulatory guidance available in the respective regions. A significant relationship was found between the pairs—technology and operation; technology and security; technology and resilience; operation and security; operation and outsourcing; security and outsourcing. There did not appear to be a significant relationship between the operating expense of a bank and the mention of operational resilience.

There needs to be better guidance for disclosure by banks who have an obligation to disclose the risks related to operational resilience to their external stakeholders such as investors, clients, business partners. Standards for disclosures should enable an investor to compare the resiliency risks between different banks. The industry, especially banks that operate globally, would greatly benefit from harmonization of the regulatory requirements related to operational resiliency across jurisdictions. A more consistent way to measure and report operational resiliency risks would benefit the stakeholders of the banks by providing a comparative view of the resiliency risk of the bank. Regulators, through a harmonization of the guidance around operational resilience, can drive better standardization of practices such as disclosures and reporting, ensuring a framework that is more efficient and effective in compliance.

The area of operational resiliency will also benefit from additional research, especially around areas of measuring and reporting operational resilience and comprehensive operational resiliency testing. This study highlights the disparity in disclosures on operational resilience and also provides a basis for future empirical research on operational resilience in banking.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

Basel Committee on Banking Supervision. 2018. *Cyber-Resilience: Range of Practices*. Basel: Bank for International Settlements.

Bradenburg, Rico, Tom Ivell, Evan Sekeris, Matthew Gruber, and Paul Lewis. 2019. *Striving For Operational Resilience*. New York: Oliver Wyman.

Canada Office of the Superintendent of Financial Institutions. 2020. *Developing Financial Sector Resilience in a Digital World*. Ottawa: Canada Office of the Superintendent of Financial Institutions.

Caparusso, John, Yingyuan Chen, Peter Dattels, Rohit Goel, and Paul Hiebert. 2019. *Post-Crisis Changes in Global Bank Business Models: A New Taxonomy*. IMF Working Papers. Washington, DC: International Monetary Fund. [CrossRef]

Carstens, Agustín. 2017. The Nature of Evolving Risks to Financial Stability. Paper presented at the 53rd SEACEN Governors' Conference/High-Level Seminar and 37th Meeting of the SEACEN Board of Governors, Bangkok, Thailand, December 15–17; Bangkok: BIS, pp. 13–14.

Dowell-Jones, Mary, and Ross Buckley. 2016. Reconceiving resilience: A new guiding principle for financial regulation. *Northwestern Journal of International Law & Business* 37: 1.

European Commission. 2019. Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More. Available online: https://ec.europa.eu/info/publications/finance-consultations-2019-financial-services-digital- (accessed on 9 August 2020).

Finextra, and IBM. 2016. *How to Get Ahead on Operational Resilience: Strategies for Financial Institutions*. London: Finextra Research Ltd.

FSB. 2019. 2019 List of Global Systemically Important Banks (G-SIBs). Available online: https://www.bis.org/bcbs/publ/d296.htm (accessed on 16 September 2020).

Hernández, Pablo. 2019. Financial Technology: The 150-Year Revolution. Paper presented at the 22nd Euro Finance Week, Frankfurt, Germany, November 18–22; Frankfurt: BIS, pp. 1–11.

Infosys Ltd. 2019. Designing for Operational Resilience. In *Blast Effects on Buildings*. London: ICE Publishing. [CrossRef]

KPMG. 2019. *Operational Resilience in Financial Services*. Honkong: KPMG.

Lautenschläger, Sabine. 2018. Sabine Lautenschläger: Cyber Resilience—Objectives and Tools. In *Euro Cyber Resilience Board for Pan-European Financial Infrastructures*. Frankfurt, BIS central bankers' speeches.

Lebaka, L., J. Hernantes, and J.M. Sarriegi. 2016. A holistic framework for building critical infrastructure resilience. *Technological Forecasting & Social Change* 103: 21–33.

PWC. 2019. Operational Resilience: Your Swiss Army Knife to Survive the next Crisis. In *The Art of Organisational Resilience*. London: Routledge. [CrossRef]

Tapper, David. 2013. *Lack of Operational Resilience Will Undermine Enterprise Competitiveness: A Strategy for Availability*. Framingham: IDC.

Walker, Brian, Crawford S. Holling, Stephen R. Carpenter, and Ann Kinzig. 2004. Resilience, adaptability and transformability in social–ecological systems. *Ecology and Society* 9: 2. [CrossRef]