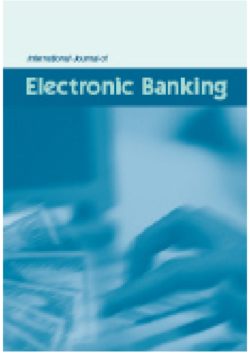
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Electronic Banking

ISSN online: 1753-5247 - ISSN print: 1753-5239
https://www.inderscience.com/ijebank

Does higher capital help to mitigate failure of digital technologies and systems in banks?

Anjan Roy

DOI: 10.1504/IJEBANK.2024.10062443

Article History:

Received:	17 January 2023
Last revised:	19 January 2023
Accepted:	18 June 2023
Published online:	22 February 2024

Does higher capital help to mitigate failure of digital technologies and systems in banks?

Anjan Roy

National Institute of Bank Management,
Kondhwa Khurd, Pune 411048,
Maharashtra, India
Email: aroy@nibmindia.org

Abstract: Bank regulators in different countries have responded variedly to failures of digital technologies and systems in banks under their jurisdiction. Some have prescribed higher capital while others have levied fines and penalties, or issued warnings and reprimands. This study examines whether imposition of higher capital could prompt appropriate mitigation action in banks. Technological malfunctions and breakdowns are operational risk events, classified as business disruption and systems failure, which have lower frequency of occurrence as well as lower severity of impact. Their material insignificance leads to their acceptance as part of business risk. With banks transitioning to digital mode of operations, such risks may be higher, but capital charge imposition may have limited direct impact on their mitigation. Instead, by imposing penalties, regulators may elicit mitigation actions such as investment on technology capacity and enhanced controls. The study finds that regulatory penalties lead to lower operational risk capital with lag of one year and therefore may be better alternative action.

Keywords: operational risk; loss distribution; digital technologies; regulatory penalties; business disruption; system failure.

Reference to this paper should be made as follows: Roy, A. (2024) ‘Does higher capital help to mitigate failure of digital technologies and systems in banks?’, *Int. J. Electronic Banking*, Vol. 4, No. 2, pp.85–98.

Biographical notes: Anjan Roy teaches post-graduate courses and conducts executive training on business strategy and banking operations at National Institute of Bank Management, Pune. He has undertaken sponsored research and consulting assignments for banks and financial institutions on strategic repositioning, organisational restructuring, mergers and acquisitions, sustainable finance, etc. He graduated with the Bachelor of Technology degree from the Indian Institute of Technology (Indian School of Mines), Dhanbad and has a Doctoral degree the Fellow in Management from the Management Development Institute, Gurgaon.

1 Introduction

In February 2022, the Monetary Authority of Singapore imposed an additional capital charge on a certain bank following the widespread unavailability of their digital banking services for several days in November 2021.[1] The regulator noted deficiencies in the bank’s incident management and recovery procedures to restore its digital banking services to a normal state, resulting in the prolonged duration of the disruption. It required the bank to apply a multiplier of 1.5 times to its risk-weighted assets for operational risk leading to an additional amount of approximately S$ 930 million in regulatory capital.

Few years back, in December 2020, the Indian banking regulator, Reserve Bank of India (RBI) asked one of the largest private bank facing frequent technology problems of outage in data centres, to take actions such as freezing the issue of new credit cards, holding their digital strategy and new product launches, third-party audit of IT system, etc.[2] The curbs lasted for more than a year. The regulator also imposed monetary penalties on the bank and prescribed third party audit of bank's technology systems, but did not prescribe higher capital for operational risk.

Similar incidents in other countries indicate to varied responses by the banking regulators. In December 2020, a large U.S. Bank and few of its peers, were reported to have incorrectly charged overdraft and related fees to their customers owing to certain software glitch.[3] They were not penalised by the regulator but only issued letters of reprimand. Similarly, a large bank in Japan, following several events of technology outages in September 2021, received administrative actions and directions for formulating business improvement plans from the regulator.[4] In May 2022, the Bank of England instructed banks to build up resilience from major disruptions to their business operations.[5]

The context of these banks may be dissimilar as they belong to different banking and financial systems, regulatory jurisdictions, or level of sophistication of risk management systems. According to their latest bank reports on Pillar III disclosures, U.S. based banks determined operational risk weighted assets as per Basel III advanced approach using internal models, while banks in Singapore have adopted the standardised approach to computing the operational risk regulatory capital. Banks in India as well as Japan still report operational risk weights using the BI approach. The observed differences in regulatory actions still lead to the question whether the imposition of higher capital charge could lead to better mitigation of operational risk due to failure of technology, particularly digital technologies and systems, or whether other actions, such as imposition of penalties, reprimands or directives for affirmative actions, are more suitable.

Operational risk, under Basel II, is defined as 'the risk of loss from inadequate or failed internal processes, people and systems, or from external events'. The definition incorporates a wide variety of loss events and causes attributable to different business lines and functions. These include cases which can be linked to internal causes such as unauthorised activity leading to theft or fraud, external frauds (EF) such as market manipulations or product mis-selling, process failures such as during execution of transactions or documentation, disaster events such as failure of technology hardware or software, etc. Amongst these, the risk of systems disruption encompassing events from accidental systems blackouts to deliberate attacks have occupied the highest rank amongst information and technology (IT) risk by Baker Makenzie for the last two years (Risk.net, 2020, 2021). Importantly, though the frequency of operational loss events attributable to outages were fewer, there have been high-profile technology failures at a number of banks, technology vendors and trading platforms that led to chaos and volatility in several markets such as futures and foreign exchange trading. The report highlighted that the largest banks were highly reliant on few large cloud providers whose failure could 'plague multiple institutions at once', causing a large-scale shock.

This study examines whether higher capital charge would be effective for mitigation of operational risk due to failure of digital technologies and systems in banks. The layout of the paper is as follows. Section 2 traces the evolution of Basel guidelines and approaches for measurement of operational risk capital and the criticisms received on their effectiveness for risk mitigation. Section 3 reviews the literature on loss characteristics of various types of operational risk events. Section 4 discusses facts and features of operational risks and losses related to failure of digital technologies and systems. Section 5 highlights few reasons as to why higher capital may not be effective for mitigating risks due to technology and systems failure. Section 6 reports observations of empirical relationships between alternative actions for regulators, and points to recourses available other than imposing capital charge upon banks for operational risk mitigation. Section 7 concludes.

2 Basel guidelines for operational risk capital: evolution and criticisms

Management of operational risk, included within the Basel II guidelines in 2004, were founded upon three pillars. Amongst these, the Pillar I provided the standards for measurement of operational risk and determination of capital estimate for protection against expected and unexpected future losses from risks taken in the conduct of business. The measure of capital also formed the basis for performance management of banks and their business lines. Pillar II and III addressed the adequacy of systems and processes for risk management and disclosures to be made in regards of risk performance respectively.

Approaches to measurement of operational risk under Pillar I have been evolving to meet the emerging challenges and incidences of risks, and banks can be found to be in various stages of adoption today. From the basic indicator (BI) to the standardised (TSA) and the advanced management approach (AMA), the evolution signified increasing sophistication and risk sensitivity in the measurement process. The BI approach determined bank level capital requirement for operational risk as a fixed percentage of positive annual gross income (which included net interest income and non-interest income) averaged over the previous three years. The gross income serves as proxy for scale of scale of operational risk while the fixed factor serves as proxy for the industry-wide relationship between the operational risk loss experience for bank and the aggregate level of gross income in the industry.

In TSA approach, banks' activities were divided into eight business lines: corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency services, asset management, and retail brokerage. Operational risk capital is calculated upon the gross income of the business line multiplied by a beta factor assigned to the business line. This beta factor serves as a proxy for the industry-wide relationship between the operational risk loss experiences for the business line, while the aggregate level of gross income for its size. Allocation of capital charge to business lines thus became an integral mechanism for operational risk management.

Sands et al. (2018) criticised these operational risk methodologies for their lack of transparency, poor predictive power and being disconnected with managerial actions. They observe the methods to be backward looking, complex and with potential side effects. Despite requiring significant level of capital, they argue, banks still do not have the ability to absorb the operational risk losses. More importantly, the approaches are ineffective for creating the appropriate incentives for risk taking. Earlier, Kuritzkes and Scott (2005) had argued that instead of holding capital, operational risk should be dealt by other means such as better controls, loss provisions or insurance. Hain (2009) mentioned about incentive conflicts in reporting and disclosing operational risks by managers, while Behlaj (2010) examined whether the capital charge creates any incentive to reduce exposure to operational risk and found that it does not create incentive to exert effort for risk prevention. Ames et al. (2015) also observed the absence of incentives to invest in and improve business control processes through granting of regulatory capital relief. Doff (2015) pointed that modelling of operational risk needs to contend with lack of data in the tail of probability distributions and may be prone to inverse incentives leading to use of special statistical techniques or shared external data. He therefore suggested that institutions and regulators should focus more on operational risk mitigation and avoidance of large losses.

In following, the AMA approach came up, with the measurement of operational risk capital becoming more nuanced and based on various quantitative and qualitative criteria. In this approach, losses are classified in a matrix comprising of the eight business lines as well as seven event types such as: internal frauds (IF), EF, clients, products and business practices (CPBP), employment practices and work safety (EPWS), damage to physical assets (DPA), business disruption and system failures (BDSF) and execution, delivery and process management (EDPM). Determination of capital is based on four data elements such as: internal loss data (ILD), external loss data (ELD), scenario analysis (SA) and Business environment and internal control factors (BEICFs). Calculation of capital charge is based on difference between Value at Risk at the 99.9th percentile of the distribution of potential aggregate operational losses over a 1 year time horizon as made by the bank and its expected loss. Banks under AMA are allowed to recognise risk mitigating impact of insurance and reduce up to 20% of their operational risk capital charge.

Measurement of operational risk and capital charge under AMA, however, has also remained challenged due to availability of loss data. Operational risk events in individual banks and financial institutions are by far and few, and hence internal loss data may be inadequate. Deployment of data from external and other sources may be required, but such data must be scaled and adjusted to reflect institutional differences in business unit mix, activity level, geography, and risk control mechanisms across firms (Allen et al., 2004). An associated challenge remains about aggregation of such data. Data from different sources carry their own biases such as from size, sample selection, reporting, etc. Aggregation problems also emerge from the different nature of operational risk event types and their loss distributions.

In order to address the above concerns, the non-model based new standardised approach (NSA) was developed. This approach determines operational risk capital as a product of a business indicator component and an internal loss multiplier. The former is a measure of baseline capital requirement depending on the size of bank while the latter is a scaling factor depending upon the loss experience of the bank.

Migueis (2019), however, found that while the AMA was complex, vulnerable to gaming, and lacking comparability, the NSA lacked risk sensitivity and was insufficiently conservative for US banks. Grimwade (2021) has pointed out that the latter is backward looking and consequently blind to emerging risks particularly linked to changes in bank business models such as with increased usage of artificial intelligence and machine learning.

3 Loss characteristics of operational risk event types

Incidents of risk have certain statistical features known as loss distributions, which are modelled upon the estimation of their frequency of occurrence and their severity of impact viewed at particular level of confidence. Depending on the event type, the shape of the loss distributions vary from being normal or skewed while having thin or fat tails signifying the size of extreme losses (Li et al., 2013). For example, the loss distribution of a loan portfolio, caused due to default in repayment of principal or interest amount, is represented by a skewed distribution with asymptotic tail, assuming the portfolio to be granular, homogeneous and fully diversified. On the other hand, market risks losses, caused due to adverse movements in prices and fall in economic value of a portfolio of traded assets, may exhibit normal or logistic distribution (Olson and Wu, 2013). Operational risk events are characterised by their frequency of occurrence modelled as Poisson or negative binomial distribution, whereas their severity or impact modelled as lognormal, Pareto, or Weibull distribution (Galloppo and Rogora, 2011). Such distributions are observed to be skewed and kurtotic, with concentration of data points in the lower loss ranges and with extreme data points signifying large losses at several standard deviations away from the mean.

As previously noted, under the AMA, operational risks are classified into different types of risk events. These event types have varying loss characteristics and predictability. For example, Rachev et al. (2006) reported their findings from an operational loss data collection exercise conducted in 2002 and observed varying levels of operational loss severity and frequency not only between the eight business lines but also for the seven event types. Tables 1(a) and 1(b) reports the loss severity and frequency data for the event types from several studies including Chernobai et al. (2009) who observe similar findings in a study of operational loss data for 157 financial institutions in the U.S. during the period 1980 to 2003. Other studies, such as by Anghelache and Olteanu (2011), Moosa and Li (2013), Tandon and Mehra (2017) and more recently Aldasoro et al. (2020), also make similar observation. In most of these studies, BDSF events were found to be having one of the lowest loss severity and probability of occurrence.

De Fontnouvelle et al. (2006) analysed two vendor-provided operational loss datasets, SAS's OpRisk global data and fitch OpVar loss database with information on operational losses exceeding $1 million and found that the event types with the most losses were IF and CPBP, while those with the fewest losses were DPA and BDSF. More recent studies of U.S. bank holding companies, such as by Berger et al. (2022) for the period 2002 to 2016 and Scott Frame et al. (2020) for the period 2001 to 2018, found that the event type under discussion had the lowest allocation for operational risk losses.

Other studies, such as by Medova and Berg-Yuen (2009) have observed that risk events leading to extreme losses contribute the most to operational risk. Accordingly, they advocate the use of extreme value theory to model such losses. In a study using data from the 2008 Loss Data Collection Exercise for Operational Risk (LDCE, 2008), Milkau and Newmann (2012) found .that there exists correlation between the severity and frequency for operational risk events leading to extreme losses. Such correlation can be fitted with a power law distribution which indicates that frequency of such events depends on their severity.

Table 1a Loss severity (%) and frequency (%) by operational risk event type

S. no	*Event type*	*Rachev et al. (2006)*		*Chernobai et al. (2009)*		*Moosa and Li (2013)*	
		S	*F*	*S*	*F*	*S*	*F*
1	Internal fraud	3.50	7.58	5.6	15.5	15.7	22.4
2	External fraud	43.94	16.09	3.4	9.5	1.6	7.2
3	Employment practices and workplace safety	7.99	5.51	2.1	9.0	0.9	7.9
4	Clients, products and business practices	7.11	10.88	52.9	47.4	57.8	47.1
5	Damage to physical assets	0.85	29.03	10.6	1.9	20.7	7.7
6	Business disruptions and systems failure	1.02	0.70	1.4	2.9	0.5	1.6
7	Execution, delivery and process management	35.40	29.54	2.6	7.3	2.8	6.2

Note: S = severity; F = frequency.

Table 1b Operational risk loss (in %) by event type

S. no	*Event type*	*De Fontnouvelle et al. (2006)*	*Berger et al. (2022)*	*Scott Frame et al. (2020)*
1	Internal fraud	23.0	1.0	0.98
2	External fraud	16.5	3.0	5.15
3	Employment practices and workplace safety	3.0	2.7	3.09
4	Clients, products and business practices	55.5	78.3	74.35
5	Damage to physical assets	0.4	0.9	0.71
6	Business disruptions and systems failure	0.3	0.5	0.67
7	Execution, delivery and process management	1.2	13.6	15.06

4 Operational risk from failure of digital technologies and systems

The banking industry across the world has been increasingly embracing digital technologies, applying them to various parts of value chain processes and operations. There has been a rapid rise in digital transactions in banks, which have often exceeded their capacity leading to frequent breakdowns and service outages. Besides, with evolution of banks' technological architectures from mono-lithic to micro-service based systems, and increasing adoption of application program interface (API) and cloud based applications, there is greater inter-connectedness and dependence on third-party service providers. Events of systems failure and downtime now impose bigger risk of disruption and immense cost on the banking system. Gartner has estimated[6] the average cost of network downtime for a bank to be around USD 5,600 to USD 9,000 per minute in 2016.

The actual amount of loss can be staggering considering the fact that the amount of downtime has been increasing. Study by Ponemon Institute (2016) indicates that business disruption contributed to the highest cost of unplanned outages of 63 data centres studied. According to Statista[7], the average cost per hour of server downtime for the banking and finance industry worldwide stood at USD 9.3 million, which was the highest amongst all industries in the year 2017.

The rising cost of system outage is also contributed by the increasing duration of outage. According to a report released in 2018 by the Uptime Institute[8], prolonged downtime is increasingly becoming common among public reported outages. The Ponemon Institute (2016) report also discerned a linear relationship between the cost and duration of outage. In their Annual Sectors Report of 2020, UK's Financial Conduct Authority (FCA) expressed concerns about service interruptions undermining consumer confidence, causing inconvenience and financial loss to them. Clearly, the recent experiences suggest that both the frequency and severity of failures of digital technologies may not be that rare or mild as found out in the studies on BDSF event types made earlier.

With increasing dependence on vendors for digital technologies, system failures may also occur at sites external to banks. According to the Uptime Institute Global Data Centre Survey Report published in 2022, due to increasing use of cloud technologies and growing deployments of software defined and hybrid distributed architectures, there has been significant rise in complexities of systems. Almost 63% of the publicly reported outages since 2016 were caused due by external and third party IT service providers which include a variety of services such as cloud, hosting, co-location, telecommunication, etc. Another significant cause of failures was power cuts and uninterrupted power supply system failures that resulted in 43% of outages. Networking related problems are recognised as the single biggest cause of IT problems.

5 Effectiveness of capital for mitigating risk of technology and systems failure

The discussion in Section 3 characterised the incidents of technology malfunctions as BDSF type operational risk event, which occur with lower frequency and lower severity. Accordingly, such failures may be accepted as part of business risk and addressed by making provisions or providing capital. However, as Section 4 informed, the occurrence of such event types in digital operating systems seem to be more frequent as well as impacting severely and widely. These observations indicate that imposition of higher capital for BDSF type risk events, particularly in digital banking, may not be effective for bringing about the required mitigating actions by banks. The associated concerns are further elaborated as follows.

First, BDSF events may be different from other event types in regards of the underlying causes, as Grimwade (2021) described, in their nature of inadequacies and failures. Other operational risk event types such as internal or EF or employment practices and workplace safety, etc., may relate to intended or wilful actions of agents or people internal and external to the institution. The occurrence of these events may follow certain patterns, for example, product mis-selling may increase at the time of high credit growth or incidences of rogue trading may rise during times of market volatility, etc. Indeed, tail operational risk events have been found to be positively related to growth

(Scott Frame et al., 2020). But BDSF event types such as digital technology failures may stem from causes such as system or component failure, lack of training, inadequacy of capability, etc., which may occur with banks failing to make the requisite investments in re-architecting, upgradation or maintenance of their legacy technological infrastructure.[9] These events are more idiosyncratic with little systematic external connect, such as with growth in financial market. Thus, being uncorrelated with the market, their beta factor, or the measure of systematic risk reflecting the sensitivity of their return to variation in the market return, is likely to be zero (Guo et al., 2021).

Such feature of technology failures may imply upon the effectiveness of capital allocation for their risk management. Allocating capital to a business unit per forces ownership and internalisation of losses due to risk and enables setting up of market based cost targets, or hurdle rates, leading to assignment of responsibility for their optimal use. Business units assigned with higher capital may increase their earning asset portfolio or pursue higher yields on their exposures for their viability. But, for risks with beta factor value as zero, markets may not provide the appropriate benchmark returns. Such types of risk therefore remain as downside loss rather than variability of outcome (Herring, 2002) with limited effect of market discipline for their management. Therefore, as Sands, et al. (2018) point out, capital deployed against such risk weighted assets to meet capital ratio may be essentially 'dead' capital, incapable of being used for purpose of risk management.

Second, as studies by Cummins et al. (2011) and Sands et al. (2018) point out, there are negative externalities and spill over effects of operational risks leading to higher magnitude of losses. Li et al. (2013) have observed significant correlation between operational risk and credit or market risk losses wherein the occurrence of the former may lead to the latter under certain circumstances. For example, mistakes in loan documentation may lead to losses if and only if the counterparty defaults. Such effects can be observed for technology failure as well. Mittnik et al. (2013) found BDSF events to be highly correlated with other events of high frequency and high severity such as CPBP and EDPM. Recently, a UK based bank, suffered malfunction in digital operations after which some of their customer accounts were accidentally subject to double payments[10]. One bank in India reported that customers received added credit to their accounts during the introduction of a software patch as part of maintenance activity[11]. Another reported that technology glitches led to disbursement of loans in customer account accounts without their consent[12]. All these incidents led to consequential effects of reputational harm, customer churn and loss of business to the banks. These are business risks that may not be mitigated by allocation of higher capital. At an extreme, the impact of technology and systems failure may create significant market uncertainties and even threaten a bank's survival. The failure of Knight Capital in August 2012 occurred due to a software error in its automated market operations, which led to unintended buying of a large number of securities within a very short time.

Third, operational risks are featured by other time related dimensions such as detection (Grimwade, 2021) and velocity (Chaparro, 2013; Parkin, 2022). There are often instances of 'near misses' (Muermann and Oktem, 2002; Kelliher et al., 2020) when a risk event may not immediately crystallise due to favourable prevailing conditions. Materialisation of operational risk may be delayed until the formation of unfavourable circumstance, such as hidden losses at Barings became revealed only after the Kobe earthquake, leading to failure of the bank. Aldasoro et al. (2020) observed that, on average, it took more than a year for operational losses to be discovered and recognised in the books of banks. Chernobai et al. (2021) also pointed out that operational risk externalities may not be immediately evident but may carry huge impact with increasing size and complexity of banks. Grimwade (2021) reported lags, not only between occurrence and detection, but also between the detection and settlement of operational risk losses. However, his study indicates that for BDSF type risk events, such lags were one of the lowest. This may imply that technology failure risk events occur with higher velocity with a shorter time gap between their exposure and occurrence of impact.

Due to the above reasons of network externalities and second order effects, rapidity of loss impacts becoming material and limited effect of market discipline, imposition of capital for ex-post mitigation of operational risk due to digital systems failure may just be a reactive action. Instead, there would be need for infrastructure and organisational capital to prevent such risk from happening in the first place. Regulators may need to ask banks to invest adequately on technology capacity and enhance their control systems for ex-ante mitigation.

6 Other regulatory actions as alternative to capital charge

Regulatory actions for mitigation of operational risk in banks vary from issuance of instructions such as ceasing operations in certain business lines, to enhancing risk weights and raising capital levels or imposing penalties. Asser (2001) described several categories of regulatory actions such as enforcement, corrective or taking control. Enforcement actions aim at preventing failures by taking preventative actions before occurrence of any serious problem. For example, the regulator may require banks to cease and desist from some operations. In this regards, regulatory penalties as enforcement actions, may impose substantial and prolonged damage to banks on their reputation risk (Armour et al. 2017), and therefore induce good behaviour. Corrective actions are taken for repairing any damage caused and return back to regulatory health. For example, interventions such as prompt corrective action (PCA) taken under more serious structural and performance problems for banks. Control actions could lead to replacement of management and placement of the bank under receivership.

The actions of the regulator may depend upon the severity of prudential violations in regards of their impacts on an individual bank and the need to protect the creditors from any fall in value of assets to addressing the emerging requirement for maintaining stability of the banking system. Regulatory actions, though often intended to be gradual or progressing sequentially, may not occur as such. Regulator have the discretion to make their intervention gradual or precipitated. Study by Hill (2012) informs that bank regulators may require individual banks to maintain more capital than required by regulation if the latter are found to be operating in an unsound manner. However, the study also noted that such enforcement actions are not consistent between regulators or uniformly applied to different banks.

While taking such action promptly and adequately, regulators may also face dilemmas to find the balance between imposing any overbearing condition and avoiding impairment of ability for innovations. Banks, particularly the older and larger ones, may operate with a variety of technological handicaps such as legacy systems, outdated coding language, shortage of knowledgeable IT staff, etc., which need to be overhauled (Risk.net, 2021). Actions of regulators must, therefore, conform to certain principles of proportionality keeping in view the nature of risk, and the likelihood of occurrence and severity of impact at the bank or system level

7 Research question, model variables and analysis

The research question that follows from the above discussion is: 'what may be the preferred regulatory action to mitigate the risks of technology and systems failure in banks?' The answer to this could depend upon the regulator's view of the effectiveness of its different actions, such as issuance of warnings or directions, imposition of penalties or higher capital charges. If they determine the latter two actions as positively related, then these could be considered as equal alternatives with similar mitigating effect. However, if monetary penalties lead to mitigating actions by banks which ultimately to lower capital requirements, then regulators may choose the former action than the latter.

The hypothesis, therefore, is that imposition of monetary penalty for operational risk events is related but leading to lowering of operational risk capital in banks. Actions of monetary penalties for operational risk events in banks are independent of the bank's decisions of maintaining the level of operational risk capital, which are based on the Basel approach adopted by them. The empirical model for the hypothesised relationship is as follows:

$$LORC = a_1 + a_2 . RPEN + a_3 . RPEN^{-1} + e$$

Table 2 describes the variables in the model, their measures and descriptive statistics. The hypothesis has been tested with data from five largest private sector banks in India (HDFC Bank, ICICI Bank, Axis Bank, Kotak Mahindra Bank and IndusInd Bank). The values of operational risk capital have been obtained from the Basel Pillar III disclosures made the banks for the period between and including the years 2010–2011 and 2021–2022. The data on penalties imposed by the regulator have been obtained from the section on corporate governance found in the annual reports of the banks for the same period. Regulatory penalties here relate to various reasons apart from technology glitches, such as mis-selling of products, deficiency in meeting KYC norms, etc., which are part of operational risk events in banks.

Table 3 provides the results of the random effects multiple regression (Hausman Test p value = 0.784) conducted to test the hypothesis. Although based on a small set of observations, the results are robust and significant at 1% level. It suggests that the level of operational risk capital in banks may be related to the number of regulatory penalties imposed on them, affected with lag of one year. However, the direction of the relationship does not lend support to the hypothesis that the effect of more number of penalties would be to increase the level of operational risk capital. As matter of fact, the money value of the penalties are much lower and insignificant as compared to the change in level of capital for risk. On the contrary, it is observed that the number of penalties is inversely related and hence has a negative effect upon the level of operational risk capital. The findings suggest that imposition of regulatory penalties may lead to elicitation of internal risk mitigation action in banks, which may ultimately benefit by lowering their operational risk capital requirements.

Table 2 Model variables and descriptive statistics

S. no.	*Variable*	*Measure*	μ	σ
1	LORC	Operational risk capital (as percentage of Tier-I capital)	6.465	0.968
2	RPEN	Number of penalties imposed in the current year	0.685	0.772
3	RPEN^{-1}	Number of penalties imposed in the previous year	0.666	0.800

Table 3 Effect of regulatory penalties on operational risk capital

	LORC	
	Coefficient	*T stat*
Constant	6.897***	29.04
RPEN	–0.279	–1.99
RPEN_{-1}	–0.377**	–2.83
Overall R^2	0.173	
Wald chi^2	16.69	
Significance	0.0002	
N	54	

Note: *** $p < 0.000$; ** $p < 0.01$.

8 Conclusions

Operational risk due to technology and systems failure, termed as BDSF events, are reported to have loss distributions with low frequency of occurrence and low severity of losses. Therefore, such type of risk events may be viewed as causing lower material loss in comparison to other events, and hence their acceptance as part of business risk. With banks transitioning to digital operations with replacement of legacy systems and dependence on third party services, these risks may be high with systemic implications. Banks are participants in financial networks and market infrastructure provide payment, clearing and settlement services and operate as essential utilities. Their operational resilience and business continuity are important and hence the occurrence of digital technologies and systems failure must be prevented and also arrested fast when they happen. The paper has argued that capital charge may have limited direct impact on mitigation action by banks and regulators may, instead, require banks to invest on technology capacity and enhanced control systems. The study finds that regulatory penalties lead to lower levels of operational risk capital with a lag of one year, and hence may be a better alternative to imposing higher capital charge for digital system failures.

References

Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2020) *Operational and Cyber Risk in the Banking Sector*, BIS Working Paper No 840.

Allen, L., Boudoukh, J. and Saunders, A. (2004) *Understanding Market, Credit and Operational Risk: A Value at Risk Approach*, Blackwell Publishing, MA, USA.

Ames, M., Schuermann, T. and Scott, H.S. (2015) Bank capital for operational risk: a tale of fragility and instability', *Journal of Risk Management in Financial Institutions*, Vol. 8, No. 3, pp.227–243.

Anghelache, G. and Olteanu, A. C. (2011) 'Operational risk modelling', *Theoretical and Applied Economics*, Vol. 18, No. 6, pp.63–72.

Armour, J., Mayer, C. and Polo, A. (2017) 'Regulatory sanctions and reputational damage in financial markets', *Journal of Financial and Quantitative Analysis*, Vol. 52, No. 4, pp.1429–1448.

Asser, T.M.C (2001) *Regulatory Intervention: Common Issues*, Chapter in book titled Legal Aspects of Regulatory Treatment of Banks in Distress, International Monetary Fund.

Behlaj, M. (2010) *Capital Requirements for Operational Risk: an Incentive Approach* [online] https://shs.hal.science/halshs-00504163 (accessed 18 July 2022).

Berger, A.N., Curti, F., Mihov, A. and Sedunov, J. (2022) 'Operational risk is more systemic than you think: evidence from U.S. bank holding companies', *Journal of Banking and Finance*, Vol. 143, No. 106619, https://doi.org/10.1016/j.jbankfin.2022.106619 (accessed 31 July 2022).

Chaparro, M.R. (2013) *A New Dimension to Risk Management*, Centre for Mathematical Sciences, Lund University [online] https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=4330718&fileOId=4330725 (accessed 18 July 2022).

Chernobai, A., Jorion, P. and Yu, F. (2009) 'The determinants of operational losses in U.S. financial institutions', *Journal of Financial and Quantitative Analysis*, Vol. 46, No. 6, pp.1683–1725.

Chernobai, A., Ozdagli, A. and Wang, J. (2021) 'Business complexity and risk management: evidence from operational risk events in U.S. bank holding companies', *Journal of Monetary Economics*, January, Vol. 117, pp.418–440.

Cummins, J.D., Wei, R. and Xie, X. (2011) *Financial Sector Integration and Information Spillovers: Effects OF Operational Risk Events On U.S. Banks and Insurers*, DOI:10.2139/ssrn.1071824.

De Fontnouvelle, P., Dejesus - Rueff, V., Jordan, J.S. and Rosengren, E.S. (2006) 'Capital and risk: new evidence on implications of large operational losses', *Journal of Money, Credit and Banking*, Vol. 38, No. 7, pp.1819–46.

Doff, R. (2015) 'Why operational risk modelling creates inverse incentives', *Journal of Financial Regulation*, Vol. 1, No. 2, pp.284–289.

Galloppo, G. and Rogora, A. (2011) 'What has worked in operational risk?', *Global Journal of Business Research*, Vol. 5, No. 3, pp.1–17.

Grimwade, M. (2021) *Ten Laws of Operational Risk*, Wiley and Sons, West Sussex, UK.

Guo, Q., Bauer, D. and Zanjani, G.H. (2021) 'Capital allocation techniques: review and comparison', *Capital Management*, Vol. 14, No. 2, pp.1–32.

Hain, S. (2009) 'Managing operational risk: creating incentives for reporting and disclosing', *Journal of Risk Management in Financial Institutions*, Vol. 2, No. 3, pp.284–300.

Herring, R.J. (2002) 'The Basel II approach to bank operational risk: regulation on the wrong track', *Journal of Risk Finance*, Vol. 4, No. 1, pp.42–45.

Hill, J.A. (2012) 'Bank capital regulation by enforcement: an empirical study', *Indiana Law Journal*, Vol. 87, No. 2, pp.645–708.

Kelliher, P.O.J., Acharya, M., Couper, A., Maguire, E., Nicholas, P., Pang, N., Smerald, C., Stevenson, D., Sullivan, J. and Teggin, P. (2020) 'Operational risk dependencies', *British Actuarial Journal*, Vol. 25, No. 5, pp.1–21.

Kuritzkes, A.P. and Scott, H.S. (2005) 'Sizing operational risk and the effect of insurance: Implications for the Basel II capital accord', in *Capital adequacy beyond Basel: Banking, Securities and Insurance*, Scott, H.S. (Ed.), pp.258–283.

Li, J., Zhu, X., Lee, C-F., Wu, D., Feng, J. and Shi, Y. (2013) 'On the aggregation of credit market and operational risk', *Review of Quantitative Finance and Accounting*, Vol. 44, No. 1, pp.161–189.

Medova, E.A. and Berg Yuen, P.E.K. (2009) 'Banking capital and operational risks: comparative analysis of regulatory approaches for a bank', *Journal of Financial Transformation*, Vol. 26, pp.85–96, Capco Institute.

Migueis, M. (2019) 'Evaluating the AMA and the new standardized approach for operational risk capital', *Journal of Bank Regulation*, Vol. 20, No. 4, pp.302–311.

Milkau, U. and Neumann, F. (2012) 'The first line of defence in operational risk management: The perspective of the business line', *Journal of Financial Transformation*, Vol. 34, pp.155–164, Capco Institute.

Mittnik, S., Paterlini, S. and Yener, T. (2013) 'Operational risk dependencies and determination of risk capital', *Journal of Operational Risk*, Vol. 8, No. 4, pp.1–22.

Moosa, I. and Li, Q. (2013) 'The frequency and severity of operational losses: a cross-country comparison', *Applied Economics Letters*, Vol. 20, No. 2, pp.167–172.

Muermann A. and Oktem, U.G. (2002) 'The near-miss management of operational risk', *Journal of Risk Finance*, Fall, Vol. 4, No. 1, pp.25–36.

Olson, D.L. and Wu, D. (2013) 'The impact of distribution on value-at-risk measures', *Mathematical and Computer Modelling*, Vol. 58, Nos. 9–10, pp.1670–1676.

Parkin, R. (2021) 'What has time got to do with risk? A preliminary communication', *New Zealand Journal of Employment Relations*, Vol. 46, No. 2, pp.26–30.

Ponemon Institute (2016) *Cost of Data Centre Outages*, Data Center Performance Benchmark Series.

Rachev, S.T., Chernobai, A. and Menn, C. (2006) 'Empirical examination of operational loss distributions', in Morlock, M., Schwindt, C., Trautmann, N. and Zimmermann, J. (Eds.): *Perspectives on Operations Research*, DUV, https://doi.org/10.1007/978-3-8350-9064-4_21 (accessed 23 July 2022).

Risk.net (2020) *Top 10 Op Risks 2020*, Baker Mckenzie, UK.

Risk.net (2021) *Top 10 op Risks 2021*, Baker Mckenzie, UK.

Sands, P., Liao, G. and Ma, Y. (2018) 'Rethinking operational risk capital requirements', *Journal of Financial Regulation*, Vol. 4, No. 1, pp.1–34, Oxford University Press.

Scott Frame, W., McLemore, P. and Mihov, A. (2020) *Haste Makes Waste: Banking Organizational Growth and Operational Risk*, Working Paper No 2023, Research Department, Federal Reserve Bank of Dallas.

Tandon, D. and Mehra, Y.S. (2017) 'Impact of ownership and size on operational risk management practices: a study of banks in India', *Global Business Review*, Vol. 18, No. 3, pp.795–810.

Notes

[1] https://www.mas.gov.sg/news/media-releases/2022/mas-imposes-additional-capital-requirement-on-dbs-bank.

[2] https://www.moneylife.in/article/hdfc-bank-rbi-appoints-external-firm-for-special-audit-of-the-banks-it-infrastructure/62829.html.

[3] https://www.propublica.org/article/jpmorgan-chase-bank-wrongly-charged-170-000-customers-overdraft-fees-federal-regulators-refused-to-penalize-it.

[4] https://www.reuters.com/business/finance/rare-move-japan-regulator-oversee-computer-system-troubled-mizuho-source-2021-09-21/.

[5] https://www.finextra.com/newsarticle/40325/bank-of-england-sounds-warning-to-banks-over-operational-resilience.

[6] https://www.ponemon.org/research/ponemon-library/security/2016-cost-of-data-center-outages.html.

[7] https://www.statista.com/statistics/780699/worldwide-server-hourly-downtime-cost-vertical-industry/.

[8] https://uptimeinstitute.com/data-center-outages-are-common-costly-and-preventable.

[9] https://www.ey.com/en_uk/banking-capital-markets/why-banks-can-t-delay-upgrading-core-legacy-banking-platforms.

[10] https://www.thesun.co.uk/money/17956242/tsb-customers-technical-glitch-payments-taken-twice/.

[11] https://timesofindia.indiatimes.com/city/chennai/tech-glitch-hdfc-bank-customers-turn-crorepatis-in-chennai/articleshow/91877478.cms.

[12] https://www.telegraphindia.com/business/indusind-bank-admits-technical-glitch-in-disbursing-loans/cid/1837656.