The term Fintech is a 21st century phenomenon which refers to Financial Technologies. Fintech has given a new paradigm to financial services delivery and execution processes where technology is driving innovation in financial services industry. The financial institutions are taking cognizance of benefits of Fintech and are offering varied products and services using information technology. Leong and Sung (2018) defined Fintech as *"any innovative ideas that improve financial service processes by proposing technology solutions according to different business situations, while the ideas could also lead to new business models or even new businesses".*

Fintech is now accorded as a game changer which can disrupt the whole spectrum of financial markets (Lee & Shin, 2018). The banks can effectively comprehend the magnitude of operational risk when they consider the emerging changes in business models and associated risks so that different operational risks can be prioritized and consequences may be mitigated (Chiclana, Gongora, Pena, Bonet, & Lochmuller, 2018).

A Fintech Ecosystem comprises of Demand (E&Y, 2016), Fintech startups, Technology developers and Policy, and they all collaborate to provide innovative solutions (Nicoletti, 2017a).

BCBS (2011) in principles for sound operational risk management guidelines recommended that "In general, a bank's operational risk exposure is increased when a bank engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems". Since the Fintech ecosystems are a simultaneous interaction and collaboration of various financial and non-financial entities, it works in untraditional way and takes unusual paths to follow the execution process, hence prone to attract new risks.

BCBS (2018a) have categorized technology and innovation driven financial services into two main categories; i.e. sectoral innovations related to banking products and services and market support services.

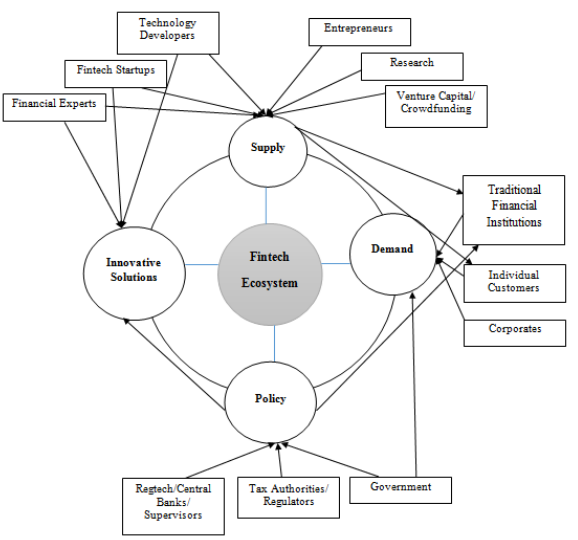

Figure I: The Fintech Ecosystem

Source: E&Y (2016); Lee and Shin (2018), elaborated by author

Basak and Buffa (2017) stated that surge of adoption of sophisticated systems of Fintech among financial institutions, has highlighted prominence of operational risk and not surprisingly, during current decade, literature on operational risk has grown drastically, focusing mostly on measurement and statistical characteristics of operational losses. The effective operational risk management process includes the identification and measurement of operational risk, which should lead to an understanding of the specific causes and events embedded in adoption of Fintech, which may expose a bank to operational risk (Gomber, Kauffman, Parker, & Weber, 2018).

Sectoral Innovations			
Credit, deposits and capital raising services	*Payment, clearing and settlement services*		*Investment management services*
Crowdfunding	**Retail**	**Wholesale**	High frequency trading
Lending marketplaces	Mobile wallets	Value transfer networks	Copy trading
Mobile Banks	Peer to peer transfers	FX wholesale	E-trading
Credit scoring	Digital currencies	Digital exchange platforms	Robo- advice

Table I: Source: BCBS (2018a)

This work is focused on identifying operational risk events, entrenched in Fintech, with respect to main categories of operational risk i.e, processes, people and systems, because the adoption of Fintech by banks is prone to attract new risks. On the basis of experts' opinions, the study will document Fintech driven OR events and their individual validity in identification of overall operational risk of banks.

2. Fintech and Operational Risk Identification

Operational risk identification and management is usually conducted to create operational risk profiles, causal relationships of events and to measure the risk exposure based on frequency and severity of OR events (Teker, 2005). Li, Allan, and Evans (2017) elaborated that the complex systems invite evolving and emerging risks and exhibit advance signals of a significant change process, and knowing how to detect and analyze those signals is the pivotal in developing and robust and scientific emerging risk process.Woods, Dekker, Cook, Johannesen, and Sarter (2017) stated that the complexity of operations is major contributor to human performance issues, incidents, and failures, implying that well intended changes that increase complexity are bound to produce new forms of failure. The collaboration of Fintech firms and banking industry includes new players into the system which have limited experience and expertise in managing bank specific risk (BCBS, 2018b).

One issue when measuring operational risk is that operational risk data is not that frequent when compared with other types of risk. The quantification of other risks uses statistical data, however, quantifying operational risk is regarded as complex as the historical loss data on every business process is not readily available within the bank (Alaoui & Tkiouat, 2017). Therefore, the field experts and researchers face hindrances in identifying and modeling various risks under the ambit of operational risk (Tarantino & Cernauskas, 2009). Moreover, León (2009) argued that the operational risk sources are more context dependent, diverse and complex and this is why, the supervisors expect the banks to consider qualitative methods for identifying, measuring and managing operational risk (Girling, 2013).

Fintech being an emerging trend is rapidly making its way into banks, however, its proliferation is inviting operational complexity and risks (BCBS, 2018b). Therefore, it is high time for banks to identify the core elements inbuilt in Fintech services which may expose the banks to operational risk in an untraditional way (Blakstad & Allen, 2018) . It is expected that banks' operational risk management framework is efficient enough to identify Fintech driven operational risk triggers for responding in timely manner to stop any developments that may significantly change existing OR or invoke new risk (BCBS, 2018b).

It is not simple to identify these new risks and it may be done by defining possible attacks and evaluating the defense mechanisms in place and the availability of relevant expertise is crucial (Nicoletti, 2017b). The identification of key risk sources and triggers with the help of experts' opinion and judgment is an effective way to foresee changes in OR exposures and to enable risk managers act proactively in anticipating operational problems and losses (Scandizzo, 2005).

3. Detecting the Fintech driven OR triggers

BCBS (2018b) elaborated in detail the Fintech driven operational risk events which may expose the banks to ultimate risk outcome as "a proliferation of innovative products and services may increase the complexity of financial services delivery, making it more difficult to manage and control operational risk. Legacy bank IT systems may not be sufficiently adaptable or implementation practices, such as change management, may be inadequate. As such, some banks are using greater numbers of third parties, either through outsourcing (e.g, cloud computing) or other Fintech partnerships, thereby increasing complexity and reducing the transparency of end-to-end operations". This implies that the banks are exposed to operational risk from varied sources including, but not limited to innovative solutions, complexity of business models, IT risks, change management process, outsourcing and reduced transparency of operations.

The traditional method of measuring OR is based on cause and effect relationship which gives OR exposure (Tattam, 2017).

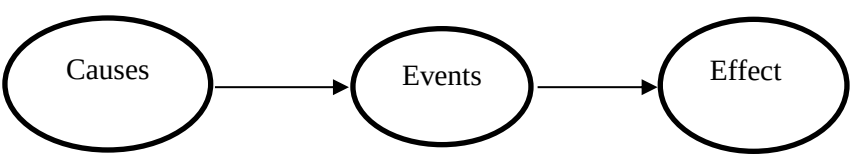

Figure II: OR events identification framework Source: Tattam (2017)

There are two ways for identification of potential risks. The evidence based approach, which uses historical data or checklists on risk events from risk database or existing literature (British Standard, 2010). The other method is called systematic team approach, which uses set of structured contextual questionsto identify risks for seeking imagination based holistic view for detecting new risks and solutions, contrary to evidence based approach (ARMS, 2010). Using systematic team method, this study employed approach proposed by Lawshe (1975) for ascertaining Content Validity Ratio.

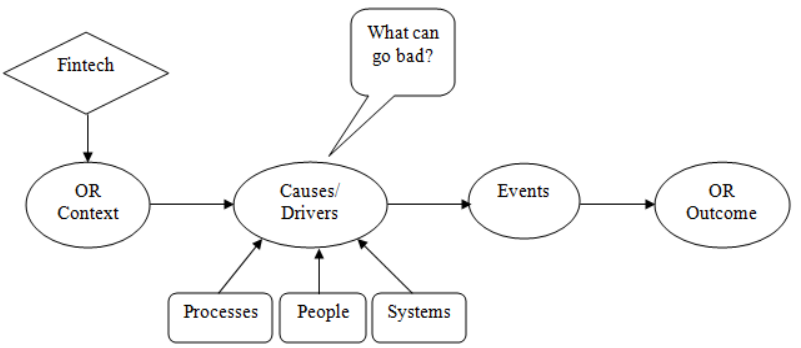

Figure III: Author's elaboration: proposed context based OR events identification framework

The proposed Fintech driven OR identification process takes into account the context as the first step, as a major contribution. This step involves establishing a background and perspective for which OR management is to be conducted (Tattam, 2017), as without understanding of context the identification process may not give desired insight. Another contribution of this study is to identify the potential Fintech driven OR triggering events in a novel manner based on Lawshe's approach. For this purpose, the study summarizes Basel II OR main categorizes as risk drivers within the context of Fintech related services and divides these into operational dimensions of OR i.e processes, people and systems. This will ensure thecontent validity of each OR dimension and respective potential Fintech driven OR triggering events, besides bridging insufficient findings in existing literature and meeting practical needs(Huang, Lin, Chiu, & Yen, 2017).

4. Research Design and Methodology

This study uses the Basel II OR drivers i.e level I and their mapping with OR triggering events i.e level II (Ibrahimovic & Franke, 2017). The study takes into account Basel II defined broad and main categories of OR instead of event types, to have an initial and more detailed specification of OR triggering events.

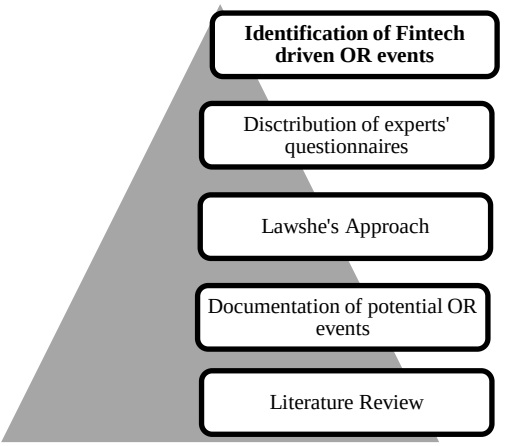

Figure IV: Research design

The purpose of this study is to ascertain the Fintech driven OR events and their capability of exposing the banks to operational risk, using of filed experts' judgments. Firstly, the main OR categories, i.e. OR drivers and mapped events are documented and discussed with Bank Fintech and operational risk experts. As per State Bank of Pakistan 2017, out of total 45 commercial banks operating in Pakistan, 26 banks are offering Fintech related services, so principally, the population comprises of 26 banks' risk managers and banks' Fintech/ alternate delivery channels experts who are responsible for formulating, planning and execution processes of technology based banking services, and are well conversant with study attributes.

Basel II Categories/ OR Drivers Level-I	**Definitions**	**Source of Definition**	**OR Triggering Events Level-II**	**Source**
Process	The risk of loss due to deficiencies in an existing procedure or absence of a procedure. This relates to execution of bank transactions and their maintenance, varied aspects of running a business line. Process related OR may be systematic in an	Dickstein and Flast (2008) Mohammed Rezaul (2012)	1. Bank's internal control and auditing mechanism were not upgraded 2. Fintech related OR events were not well identified and incorporated in Bank's system. 3. Process of launch of Fintech service took long time than planned, causing increase in cost due to inaccurate	Author Author Author (BCBS,

	entity or in-built in a process.		decisions 4. Fine imposed by regulators for not following laid down laws 5. Bank was exposed to legal proceedings/ actions. 6. Sound processes of new product approval were not in place before launching new Fintech products/ services. 7. Product/services were flawed. 8. The change management process was not in place/ updated to address technology and business activities changes when Fintech services are launched.	2018b) Author (BCBS, 2018b)
People	The risk of loss caused by employees who may intentionally or without intention make errors, mistakes or fail to follow prescribed processes and procedures.	Dickstein and Flast (2008)	1. Branch employees lack of information about Fintech services 2. Employees failed to follow internal process 3. Negligence or carelessness of employees during Fintech services process execution and delivery. 4. Man in middle attacks/ Employees frauds. 5. Lack of task definition and authorities 6. Communication gap within Bank 7. Unauthorized activities 8. Poor working conditions	Author Author Author Ochuko (2013) Author Author Author Author
System	The risk caused by automated processes and underlying	Dickstein and Flast (2008) Mohammed Rezaul (2012)	1. Programming errors, wrong data inputs and programming	Author Author

	technologies, privacy, theft, failure, breakdown or other disruption in technology, IT infrastructure.		incapability. 2. Bank's system was not capable of processing and delivering Fintech services. 3. Account compromises 4. Loss of data integrity 5. Loss of Fintech service availability 6. Loss of confidentiality 7. inefficient disaster recovery and business continuity	Ochuko (2013) --do-- --do-- --do-- Author

Table II: Level I & Level II OR triggering events

The data are collected through face to face and email survey. The experts have given their opinion on level-I and level-II risks based on their knowledge in the field of study and experience in the banks. The results of the study will establish as if the main OR drivers and events are valid in posing OR to the banks offering Fintech services or not.

4.1. Lawshe's Approach –Experts' judgment questionnaire

The concept of measuring relevant essentiality and validity of an item towards testing a broader content with the help of experts' opinions and judgments was introduced by Lawshe (1975). Content Validity Ratio (CVR) is a static useful in making decision for rejection or retention of an item and its validity in an instrument as judged by experts (Gilbert & Prion, 2016). The experts in the domain of test content establish content validity by design, further evaluated by rationale behind their judgment (Wilson, Pan, & Schumsky, 2012). The responses received from all experts are then pooled and frequency count of "essential" responses is used to determine if an individual item is representative of the test content (Lawshe, 1975), in the light of following basic rules;

CVR is negative if less than half experts accord an OR event as "essential"

CVR is zero, if half of experts say an OR event is "not necessary".

The calculation of CVR is done as follows;

$$CVR = \frac{ne - N/2}{N/2}$$

Where, *ne* refers to number of experts who accord an item as "essential" and *N* denotes total number of experts. The CVR of each item shall indicate its relevant validity in the content under study. The content validity index (CVI), on the other hand is computed for the whole set of items of test content. It shows the mean value of CVR of all items retained in the set (Lawshe, 1975).

There are other statistical methods to measure content validity of experts' judgment like Cohen's kappa, *k* (Cohen, 1960), the Tinsley Weiss index (Tinsley & Weiss, 1975), *rWG* and *rWG (J)* indexes (James, Demaree, & Wolf, 1993), and *r*WG(J)* indexes of Lindell, Brandt, and Whitney (1999), however, those have more focus on inter-rater agreement instead of individual item validity as "essential" (Wilson et al., 2012). Contrary to alternate alternative methods, the Lawshe's approach is simple, straightforward and user friendly, involving simple calculation and giving table of critical cutoff value (Lindell et al., 1999).

For the purpose of this study, experts' judgments were gauged through questionnaire survey to identify Fintech driven OR events and to confirm their respective potential to trigger OR in banks. 26 filed experts are invited from banks offering Fintech services. The questionnaire is comprised of three parts. First part containing questionnaire explanation and articulation of study purpose, second part covering experts' information and third part comprising 23 potential OR events , requesting the experts to elicit their opinions. The experts are asked to respond to the questions in either of 3 ways, i.e. 1 for "essential" or 2 for "useful but not essential" or 3 for "not necessary".

5. Empirical Results - Lawshe's Approach

The 23 documented OR events were put in front of experts in form of questionnaire for provision of direct responses against each item. 26 operational risk experts from the banks offering Fintech driven services were contacted, who have considerable experience and know how in the area of content study to obtain robust and valid results.

20 experts accorded their opinion, entailing a response rate of 77%. For 20 experts, according to Lawshe (1975), the CVR of 0.42 is minimum cutoff value for retention of an item as valid. In the light of experts' opinion, 18 items having CVR>0.42 were retained as Fintech driven OR triggering events, eliminating 8 items having CVR values less than 0.42. The table III below is showing the results of study after applying Lawshe's Approach.

Against the main OR category of "process", out of 8 items, 7 items were identified as potential Fintech driven OR triggers. All experts agreed that "Non updation/ upgrade of Bank's internal controls and audit mechanisms before launch of Fintech services" and "Sound processes of new product approval not in place before launching new Fintech products/ services" were the most

OR Categories	Items	CVR	CVR > 0.42
Process	Non updation/ upgrade of Bank's internal controls and audit mechanisms before launch of Fintech services	1	Yes
	Non identification of Fintech related OR events for incorporating in Bank's OR management system	0.75	Yes
	Long procedural delays of launch of Fintech service causing increase in cost due to inaccurate decisions	0.8	Yes

	Likelihood of fine imposition by regulators for not following laid down laws for offering Fintech services	0.8	Yes
	Likelihood of Banks' exposure to legal proceedings/ actions due to offering Fintech services	0.6	Yes
	Sound processes of new product approval not in place before launching new Fintech products/ services.	1	Yes
	Flawed Product/services	0.2	No
	Change management process either not in place or not updated to address technology and business activities changes when Fintech services are launched.	0.9	Yes
	Branch employees lack of information about Fintech services	0.85	Yes
	Failure of employees to follow internal process	0.95	Yes
	Negligence or carelessness of employees during Fintech services process execution and delivery	0.7	Yes
	Man in middle attacks/ Employees frauds	1	Yes
	Lack of task definition and authorities	1	Yes
	Communication gap within Bank	0.1	No
	Unauthorized activities	0.1	No
People	Poor working conditions	0.15	No
	Programming errors, wrong data inputs and programming incapability	1	Yes
	Bank's system was not capable of processing and delivering Fintech services.	1	Yes
	Account compromises	1	Yes
	Loss of data integrity	1	Yes
	Loss of Fintech service availability	0.15	No
	Loss of confidentiality	1	Yes
Systems	Inefficient disaster recovery and business continuity plans	0.9	Yes

Tale III: Results of Lawshe's Approach

crucial as OR triggering events. "Non-identification of Fintech related OR events for incorporating in Bank's OR management system", "Long procedural delays of launch of Fintech service causing increase in cost due to inaccurate decisions", "Likelihood of fine imposition by regulators for not following laid down laws for offering Fintech services" and "Likelihood of Banks' exposure to legal proceedings/ actions due to offering Fintech services" were also retained as essential. Only 1 item "flawed products/ services" was eliminated due to being not necessary agreed by all experts.

Under the ambit of OR category of "people", 5 out of 8 items were retained as essential. "Man in middle attacks/ employee frauds" and "lack of task definitions and authorities" were the most crucial as all experts agreed upon their essentially being OR triggers. 3 items, "communication gap within the bank", "unauthorized activities" and "poor working conditions" were eliminated for being not necessarily OR triggers.

In "system" category of OR, 7 items were documented, out of which 6 items of "Programming errors, wrong data inputs and programming incapability", "Bank's system was not capable of processing and delivering Fintech services", "Account compromises", "Loss of data integrity", "Loss of confidentiality", "Inefficient disaster recovery and business continuity plans" were accorded essential by experts. Only 1 item "Loss of Fintech service availability" was eliminated for not meeting cutoff value of CVR.

6. Conclusion

The current regime is witnessing an unprecedented impact of new technologies on banking industry in terms of the speed of technology adoption by society as a whole and the amount of pervasiveness of technological knowledge among the population (BCBS, 2018b). Rapid surge of Fintech firms in financial institutions' products and services offerings for making processes unique and innovative, besides gaining competitive edge, has made the financial system more complex and subject to enhanced supervision. The adoption of complex systems also exposes the banks to new types of operational risk due to operational complexity and dependence on technology. The banks need to identify what new risks these innovative processes and resultant changes in business models may bring to their risk appetite and risk tolerance, making it difficult to measure and manage operational risk (Blakstad & Allen, 2018). Therefore, Basel Committee on Banking Supervision urged the banks that in Fintech regime, the banks' operational risk framework must be able to detect potential new risks for timely responding to any material changes in existing operational risk framework due to their emergence (BCBS, 2018b).

This study was an attempt to identify new operational risks with a contextual lens of Fintech, while most of prior studies give a generic view of cause, event and effect relationship for identification of operational risk in banks. For this purpose, Lawshe's approach was applied to ascertain the validity of individual events towards identification of Fintech driven operational risk. The field experts were selected to accord their opinion for identifying an event as potential OR trigger or otherwise. The experts suggested 18 OR events may possibly trigger operational risk in the banks having collaboration with Fintech firms. The results of this study are available for future research in this area.

7. Limitations of study

The study is aimed to identify the operational risk events in the banks having collaborations with Fintech firms and offering technology enabled products. The research considers only the validity of an item as an event in measuring operational risk profile of banks, rather than measuring inter-rater agreement and construct validity.

References

Alaoui, Y. L., & Tkiouat, M. (2017). Managing Operational Risk Related to Microfinance Lending Process using Fuzzy Inference System based on the FMEA Method: Moroccan Case Study. *Scientific Annals of Economics and Business, 64*(4), 459-471.

ARMS. (2010). The ARMS Methodology for Operational Risk Assessment in Aviation Organisations.

Basak, S., & Buffa, A. M. (2017). A Theory of Model Sophistication and Operational Risk.

BCBS. (2011). Principles for sound management of operational risk.

Sound Practices- Implications of Fintech Developments for Banks and Bank Supervisors (2018a).

BCBS. (2018b). Sound Practices: Implications of fintech developments for banks and bank supervisors

Blakstad, S., & Allen, R. (2018). *FinTech Revolution: Universal Inclusion in the New Financial Ecosystem*: Springer.

British Standard, I. (2010). IEC 31010:2009 : Risk management -- Risk assessment techniques.

Chiclana, F., Gongora, M. A., Pena, A., Bonet, I., & Lochmuller, C. (2018). An Integrated Inverse Adaptive Neural Fuzzy System with Monte-Carlo Sampling Method for Operational Risk Management.

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and psychological measurement, 20*(1), 37-46.

Dickstein, D. I., & Flast, R. H. (2008). *No excuses: a business process approach to managing operational risk*: John Wiley & Sons.

E&Y. (2016). UK Fintech: On the cutting edge: Ernst & Young.

Gilbert, G. E., & Prion, S. (2016). Making sense of methods and measurement: Lawshe's Content Validity Index. *Clinical Simulation in Nursing, 12*(12), 530-531.

Girling, P. X. (2013). *Operational risk management: a complete guide to a successful operational risk framework*: John Wiley & Sons.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems, 35*(1), 220-265.

Huang, S. Y., Lin, C.-C., Chiu, A.-A., & Yen, D. C. (2017). Fraud detection using fraud triangle risk factors. *Information Systems Frontiers, 19*(6), 1343-1356.

Ibrahimovic, S., & Franke, U. (2017). A probabilistic approach to IT risk management in the Basel regulatory framework: A case study. *Journal of Financial Regulation and Compliance, 25*(2), 176-195.

James, L. R., Demaree, R. G., & Wolf, G. (1993). rwg: An assessment of within-group interrater agreement. *Journal of applied psychology, 78*(2), 306.

Lawshe, C. H. (1975). A quantitative approach to content validity 1. *Personnel psychology, 28*(4), 563-575.

Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons, 61*(1), 35-46.

León, C. (2009). Operational risk management using a fuzzy logic inference system.

Leong, K., & Sung, A. (2018). FinTech (Financial Technology): What is It and How to Use Technologies to Create Business Value in Fintech Way? *International Journal of Innovation, Management and Technology, 9*(2), 74-78.

Li, Y., Allan, N., & Evans, J. R. (2017). A nonlinear analysis of operational risk events in Australian banks.

Lindell, M. K., Brandt, C. J., & Whitney, D. J. (1999). A revised index of interrater agreement for multi-item ratings of a single target. *Applied Psychological Measurement, 23*(2), 127-135.

Mohammed Rezaul, K. (2012). *Strategic and Pragmatic E-Business: Implications for Future Business Practices: Implications for Future Business Practices*: IGI Global.

Nicoletti, B. (2017a). *The future of FinTech*: Springer.

Nicoletti, B. (2017b). The future of FinTech: Springer.

Ochuko, R. E. (2013). *E-banking operational risk assessment. A soft computing approach in the context of the Nigerian banking industry.* University of Bradford.

Pena, A., Bonet, I., Lochmuller, C., Chiclana, F., & Góngora, M. (2018). Flexible inverse adaptive fuzzy inference model to identify the evolution of operational value at risk for improving operational risk management. *Applied Soft Computing, 65*, 614-631.

Scandizzo, S. (2005). Risk mapping and key risk indicators in operational risk management. *Economic Notes, 34*(2), 231-256.

Tarantino, A., & Cernauskas, D. (2009). *Risk management in finance: Six sigma and other next generation techniques* (Vol. 493): John Wiley and Sons.

Tattam, D. (2017). *A short guide to operational risk*: Routledge.

Teker, D. (2005). *Comparative analysis of operational risk measurement techniques.* Paper presented at the International Trade and Finance Association Conference Papers.

Tinsley, H. E., & Weiss, D. J. (1975). Interrater reliability and agreement of subjective judgments. *Journal of Counseling Psychology, 22*(4), 358.

Wilson, F. R., Pan, W., & Schumsky, D. A. (2012). Recalculation of the critical values for Lawshe's content validity ratio. *Measurement and Evaluation in Counseling and Development, 45*(3), 197-210.

Woods, D. D., Dekker, S., Cook, R., Johannesen, L., & Sarter, N. (2017). *Behind human error*: CRC Press.