Operational Risk Information Sensors for Unstructured Data

Abstract

Banks and financial institutions use social media extensively and therefore need complex risk detection tools to monitor and understand the various operational risks. Sophisticated tools are required, in particular for identification of security risks such as non-compliance with operating procedures, that are inherent and escape easy detection. Social media can, however, also be leveraged to develop rare and high impact scenarios, build on risk repositories and add to loss data repositories to help strengthen the operational risk management capability.

Detection of operational risk in unstructured data forms would require complex algorithms and high performance data processing capabilities to derive meaning from voluminous unstructured data. Fortunately, advances in complex event processing techniques using sophisticated rules and statistical model driven algorithms has imparted considerable reliability to such detection engines. Further, a big jump in data crunching capability enabled by Big Data analytics has made it possible to conceive 'in time' or even 'real time' operational risk information sensors.

This whitepaper analyzes the issue of operational risk in unstructured data, more specifically social media, and proposes a comprehensive solution for detecting, processing and managing the operational risk information embedded there in.

Introduction

The growth and ubiquity of modern communication technologies like emails, social media networks, telephone calls and messaging services have created opportunities as well as challenges. Banking and financial services organizations have been using these communication tools for operational and business purposes such as customer interaction, marketing, customer service, promotions and public relations as well as for customer acquisition and loyalty programs.

Many organizations use internal social networks such as online discussion forums for internal communication. This helps speed up processes through increased employee collaboration that boosts productivity and improves corporate culture. However, not many institutions are fully prepared to manage the potential operational risks associated with these highly evolved communication tools in use.

The Federal Financial Institutions Examination Council (FFIEC) issued elaborate guidelines for managing risks, specifically covering operational risk. The FFIEC guidance states that a risk management program in a financial institution should be able to identify, measure, monitor, and control the risks related to social media taking into account the breadth of its social presence[1].

Nature of Operational Risk Information in Social Media

Social media has two categories of embedded operational risk information. The first deals with incident detection in relation to the financial institution. As shown in Figure 1, information here can be of three types depending on its origin, either from authorized business uses, unauthorized misuse or triggered by external agents.

[1] Federal Financial Institutions Examination Council, Social Media: Consumer Compliance Risk Management Guidance, 11th December 2013

The first two (reference to incident detection aspects) are inherent to internal unstructured data like call logs and emails. The latter is typical of social media networks.

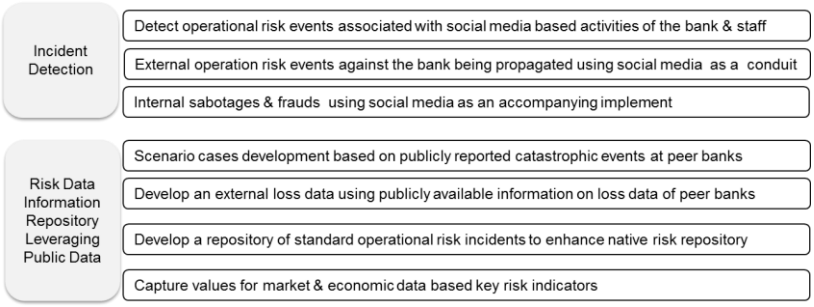

Figure 1: Operational Risk Information from Social Media (Source: Internal Research)

Social media information that can help strengthen the operational risk management capability of the bank forms the second category. This is achieved by developing an elaborate risk information system based on peer banks' experiences. Also, as is the norm in operational risk management, external loss event data would be helpful for banks using Advance Measurement Approaches to calculate regulatory operational risk capital.

Characteristics of an Operational Risk Information Sensor

A high performance analytics engine is required to process information embedded in voluminous, unstructured data mass with reasonable precision. An operational risk information sensor should have the following characteristics:

- Capability to process large data in real time
- Rule based complex event processing models
- Data driven pattern recognition models
- Closed loop feedback mechanism for embedding artificial intelligence

Complex event processing technology with built-in artificial intelligence and big data analytics capabilities has emerged as a powerful solution for detecting operational risk information embedded in unstructured data.

Architecture of Operational Risk Information Sensors

A schematic architecture of an Operation Risk Information Sensor is outlined in Figure 2.

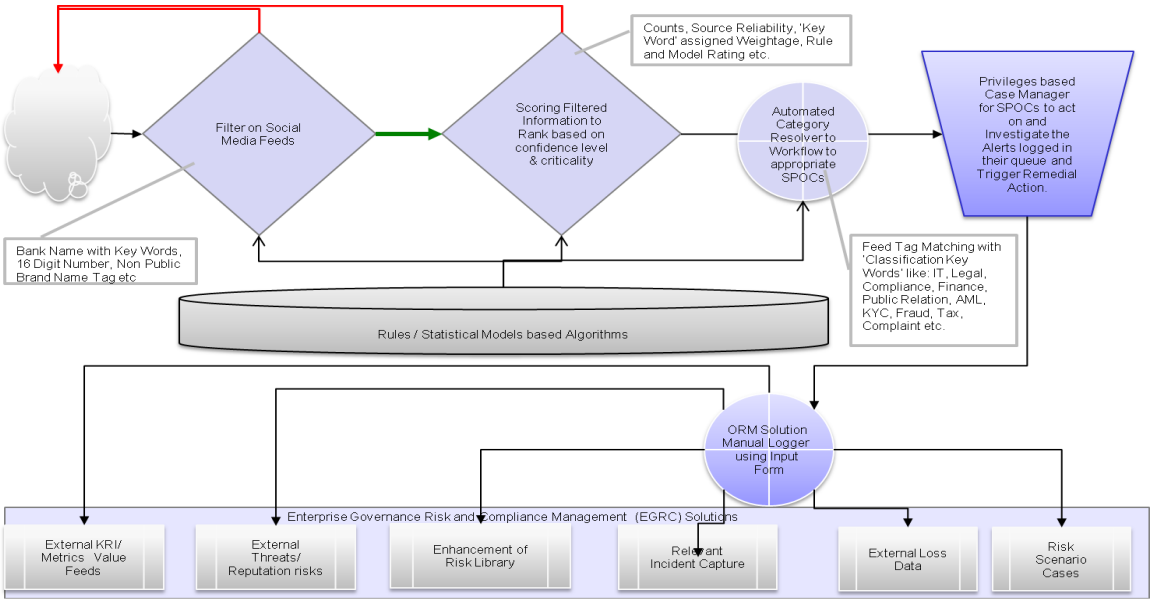

Figure 2: Operational Risk Information Sensor Architecture (Source: Internal research)

The following table 1 describes the six essential components of an operational risk information sensor:

Component	Function
Feed Listener & Text Mining	• Feed listener: Crawls through social media feeds, news feeds, emails, call logs, call scripts and messages. • Text mining: Scans sundry sources of unstructured data including documents and file dumps.
Feed Analyzer Engine	• Uses complex event processing techniques involving both rule based engine and statistical model based pattern detection engines to detect the desired information from voluminous data. • Uses Big Data analytics techniques to process the detected information to generate structured data sets. • Comes embedded with closed loop feedback mechanism to reduce occurrences of false positives and false negatives.
Automated Scoring Engine	• Helps collate, score, aggregate and prioritize the detected information. Similar to feed analyzer, scoring algorithms is embedded with made outcome sensitive using a closed loop feedback mechanism.
Routing Engine	• Uses business rules to classify the information and route it appropriately as per the built-in workflow rules. • Closed loop feedback mechanism helps improve the routing accuracy of this tool over time.
Case Manager	• Provides an interface for comprehensive analysis of operational risk information that allows manual intervention to enable manual cognizance of operational risk information.

	• Transmits message to preceding automated components like feed analyzer, automated scoring engine and router engine through an in-built feedback mechanism to improve their performances.
ORM Bridge	• Helps appropriate modules of the operational risk management system to incorporate operational risk information so that both operational risk information sensors and operational risk management system are in synch with each other. • Helps automatically populate information in relevant fields in the appropriate form,

Table 1: Essential components of Operational Risk Information Sensor (Source: Internal Research)

Benefits of an Operational Risk Information Sensor

The operational risk information sensor can be used to monitor phishing posts, malicious tweets, inadvertent or deliberate disclosure of account information, adverse comments, leakage of privileged or confidential information, and information leaks by insiders about operational risk incidents in the bank. Furthermore, it can also help garner posts or tweets on major operational risk events, catastrophic occurrences, high severity and rare incidents encountered by peer organizations that can be used for building scenarios.

However, a bank may not have experienced certain risks and may therefore lack sufficient data for risk modelling. In such cases, a bank can use experience data of peer banks sourced from social media to build scenarios and adapt them to suit its own requirements. Infrequent incidents of a high degree of severity encountered by peer banks can be processed to identify possible risks. Information related to data loss caused by rare events captured from social media, after due validation, can be used as external data input for rare event modelling. Similarly, key risk indicators such as interest rate forecast by leading research agencies or early warning of an impending systemic crisis can be gleaned from social media and news feeds.

Most importantly, operational risk information sensors would help detect the build-up of rumours that can potentially trigger disruptive events such as a run on the bank. These sensors must have the ability to detect reputation risk events such as negative or adverse posts and risks arising from the social media activity of non-stakeholders and other external entities. In fact, operational risk information sensors should detect all types of incidents irrespective of the type of impact— tangible or non-tangible.

Conclusion

Risk management programs are commonplace for the data-driven financial world that spends billions every year on managing all kinds of risks. But, the reality is that comprehensive solutions dealing with operational risks caused, carried or cascaded by social media are either limited in scope or difficult to implement. With the number of social media platforms multiplying day by day, risk mitigation measures covering all aspects are no longer an option. As a result, organizations are looking for solutions that take into account technological and regulatory factors to minimize their operational risk woes.

Detecting operational risk in unstructured data has emerged as an imperative for banks given the proliferation of and preference for social media. Technological advances such as complex event processing, artificial intelligence and big data analytics have made it possible to do so in real time., . The solution overview suggested in this paper provides typical components and architecture of sensors to extract operational risk information embedded in social media feeds ‘in time’ and process it using a typical operational risk management framework.

About the authors

Dwarika Nath Mishra, an MBA and B Tech, has wide ranging experience spanning 16 years across Manufacturing, Software, Investment Banking, Finance & Insurance sectors in leadership positions. Has been a risk management consultant and risk solution architect of 10 year standing, during which he has opportunity to architect multiple Risk Management platforms, namely D'RisK and MORSE among a number of other specific purpose solutions while working with different organizations. He has also managed complex Basel II implementation program involving multiple banks, some having presence in multiple jurisdictions. He is currently working as a Risk Management Consultant with TCS BFS Risk Practice.

Vijayaraghavan Venkatraman (Vijay) is a Global Lead for Tata Consultancy Services Ltd (TCS Ltd) Banking Risk Management Practice. He has approx 16 years of experience in the IT industry with focus on banking, risk management and regulatory compliance. Vijay has worked in several global risk and compliance engagements for various banking clients. In his current role, his key responsibilities include offering development, thought leadership initiatives, pre-sales support, Go to Market strategy, enhance domain competency and consulting. Vijay holds a master's degree in business administration and a bachelor's degree in electrical and electronics engineering. He is a GARP certified Financial Risk Manager (FRM), holds CFA charter from ICFAI and a Project Management Professional (PMP). Vijay has co-authored White papers on Basel & Enterprise Risk Management architecture.

A.N. Jayaraman (ANJ) is the Head of the Center of Excellence for the BFS risk and compliance practice in Tata Consultancy Services (TCS). He has over 17 years of experience in the banking industry and over nine years of experience in the IT industry focusing on banking, risk management, assurance and compliance. His current responsibilities include management of the CoE which involves the activities of solution/offering development, pre-sales, and consulting in the risk management space. He is a certified associate of the Indian Institute of Bankers and a graduate in commerce.