Bigdata For Enterprise Risk Management

Shreelakshmi C.M[1], Padmaja Kunda[2]
[1, 2] Department of CSE
[1, 2] GSSSIETW,Mysuru

Abstract- *Bigdata is a term used to describe massive amounts of structured and unstructured, yet digital, data sets many of which are too large or complex for traditional dbms applications[5]. With the integration of technologies like Big Data analytics, cloud computing, governance, risk, and compliance (GRC) and Enterprise Risk Management (ERM) applications, and parallel-processing platforms, in the near future, risk managers will be able to gain even greater advantages from capturing, extracting, transforming, and using legacy databases to perform risk assessments, stress tests, and risk scenario analysis[6]. Bigdata For Enterprise Risk Management(BFERM) provides standards that operates in an organization in which the governing board and executives formally accept responsibility for managing enterprise risks, and agree to adhere to generally accepted risk management standards.*

Keywords- Bigdata, ERM, GRC, Parallel-processing platform, risk assessment, dbms.

I. INTRODUCTION

Executives of organization recognize Enterprise Risk Management (ERM) as a much-needed core competency that helps organizations deliver and increase profit value over time. ERM is viewed as an essential tool for helping management for creation, sustainment, and delivery of values. An ERM program can be effectively used for processes, and technologies the program uses[3]. As executives focus on risk management as an emerging core competency, many also see the need for better data and information, so that the organizations can take action on an ever-evolving inventory of risks. One challenge risk managers face, however, is risk data scattered across the organization and not shared across business unit silos. Equally challenging is that many risk management functions lack the tools they need to capture and use risk information more effectively. So, to be truly effective, risk management teams must facilitate and encourage the capture, analysis, and delivery of current and forward-looking (predictive or directive) risk information. Predictive risk information can give management a leg-up in making better informed decisions and help them take actions that produce more reliable outcomes[10]. Leading organizations realize risk management is fundamental to good organizational governance because managing risks effectively requires management to connect and align the organization's assets, people, activities, and goals, and it does that by focusing attention on the achievability of the organization's important objectives. Yet, many ERM programs also fall short when it comes to having skilled "risk aware" resources, analytical processes, and tools. Many risk programs can also do a better job identifying, collecting, and analyzing risk data and preparing to respond to risk scenarios, as evidenced in root cause analyses done after the occurrence of an unexpected loss event. But, the good news is that evolutions in computing and risk technology, and related developments in new technologies that exploit Big Data, analytics, mobile applications, cloud computing, enterprise resource planning (ERP), and governance, risk, and compliance (GRC) systems[20].important for risk management. These technical advancements offer risk managers and those in management or outside the organization engaged in improving existing risk management programs with better abilities for enhancing risk management effectiveness[15].

This report was written for risk professionals and CPAs engaged in operating, managing, and evaluating the effectiveness of risk management functions and their investments in risk information technology (IT). This report contains general information on current trends in technology tools (those becoming more visible to risk managers) and covers simple and more sophisticated risk applications and explains how they can be useful in enhancing the maturity of risk management overall[16].

1.1 The Evolving Use of IT

Almost all organizations these days would say they are critically dependent on IT as the enabler of their continued success. This is especially true if one considers the potential impacts from a data breach or network outage, as demonstrated recently in the Sony attack and data theft. As IT and related technologies continue to evolve, organizations see more uses for leveraging technology to do the following[1]:

- More accurately and securely connect, communicate, and process business transactions with customers, suppliers, and other stakeholders
- Support human resources management and talent attraction and sustainment

- Handle detailed logistics activities across globally-integrated business operations or supply-chain processes
- Support execution of business strategies and objectives and assign the accountability for execution and achievement of these strategies and objectives with key managers.

One interesting recent development in the evolution of IT is the introduction of viable cognitive computing applications, which represent a giant leap in computing capabilities from traditional, highly programmed applications. This evolution is the next step in computing that originally began with large computational machines that calculated complex mathematical problems, which then evolved into programmable computers that executed millions of pre-defined commands to solve more complex problems[5]. The theoretical next step in the evolution of computing has been described as "artificial intelligence," in which computers are able to ingest and organize massive amounts of facts and data points and be programmed to apply natural language programming and complex algorithms to self-learn, apply logical thinking, and apply knowledge to problem solving. One interesting development in this regard was the introduction of the IBM Watson computer on the U.S. television show *Jeopardy*. As a test to see whether a computer could ingest massive amounts of data, and after some time in preparation, the Watson computer beat the top two all-time Jeopardy champions, proving that this next evolution of natural language computing applied to massively large, big data repositories can have very practical applications to real world problems[3]. Although this paper is not about this emerging shift in computing technology, the application of this game-changing technology to risk management will also fundamentally transform the risk technology used in the future.

II. ERM

Generally accepted risk management principles and standards articulate that an effective risk management program is one that operates in an organization in which the governing board and executives formally accept responsibility for managing enterprise risks, and in doing so, agree to adhere to generally accepted risk management standards. Standards such as the Committee of Sponsoring Organizations' (COSO) ERM(Enterprise Risk Manamgement) Framework (COSO ERM) and the International Standards Organization's ISO31000 are considered acceptable ERM frameworks and recognize the connection between good governance and effective risk management[5]. These standards also prescribe that to be effective, an ERM program should integrate "risk informed" or "risk aware" decision making into an entity's formal governance structures and processes. So, an effective risk program should provide management with an enhanced ability to continually capture, evaluate, analyze, and respond to risks arising from changing internal operations, external markets, or regulations[9]. Not managing these changes effectively can produce financial losses, negative publicity, and affect the achievement of the organization's objectives or mission. Therefore, effective risk programs consider, evaluate, and provide input to an organization's planning and performance measuring and support the evaluation of potentially negative events and their impacts from changes to an organization's established risk appetite and tolerance-setting processes. ERM framework standards, such as COSO ERM, also note that information and communication are essential framework components, but more importantly, feedback tools[12]. Risk information is key to delivering an effective ERM program, and information about emerging, yet critical, new risk events and causal factors are key to effective risk management processes. These days, many ERM programs maintain an inventory or listing of the organization's critical enterprise-wide risks. Moreover, from a technological perspective, these risk inventories can be fairly well managed with spreadsheets, tables, or, in more sophisticated situations, using commercially available "off the shelf" ERM or GRC software. Risk managers in many organizations use these tools to capture, categorize, organize, evaluate, track, and prioritize the organization's inventory of risks[17]. Many of these systems come pre-configured and can be further configured to apply risk prioritization schemas to risk inventories. Because risk prioritization helps management focus attention on the most critical risks, then a risk inventory generally captures data about the following:

2.1 The types and categories of risk

- The types and various categories of risk like human resources, financial, market, operational, counter-party, regulatory and others.
- The probability of occurrence for a specific risk loss event.
- The potential impact and severity of the most probable risk events, including the potential for loss of life or asset values and the potential costs required to recover from a loss event or loss scenario
- The strength of the organization's risk management process and related risk mitigation and control activities (that is, the ability and readiness of the organization to react and respond to risk loss events and optimize potential recovery costs)
- The names of the individuals responsible and accountable for monitoring and managing each critical risk

III. TRADITIONAL RISK MANAGEMENT SYSTEM ARCHITECTURE

A traditional risk system management architecture includes the big repository. Daily sensitivity and scenario data based on which the portfolio is re-priced to reflect the impact of various risk factors. Static Data that includes trade details, business organization and other hierarchical information Reference Data that includes historical prices, risk parameters, etc. Calculation Results Repository that stores the history of risk analysis related information Traditional risk systems use large extract-transform-load (ETL) sub-systems for loading data into these data warehouses and employ a battery of data processing rules to clean, standardize, validate and approve the required data[7]. Such an environment includes numerous automatic and manually triggered workflows to move information from one stage to the next. Large distributed clusters employ modular applications to determine various risk measures and other report processing infrastructure. These applications may employ load balancing for report processing and grid compute infrastructure for some calculations involving large amounts of simulation. These applications are built in-house, and developed and enhanced by applying additional business processing logic over a period of time. GUI applications and other end user compute infrastructure help in maintaining, querying and consuming data[3].

Figure 1 depicts a typical application infrastructure layout for risk management.

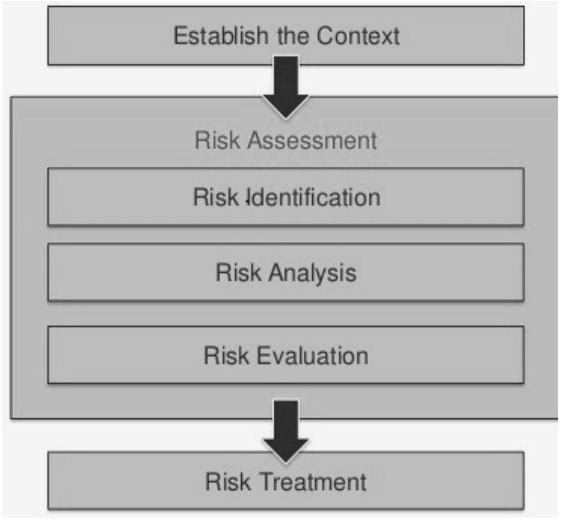

Figure1: Traditional Risk Management System.

The context that establishes the risk for the particular area is studied first. The risk assessment is made by identification of the risk ,risk analysis and then the evaluation of risk is made. After the risk evaluation risk treatment is done by identifying various methods to resolve the risks.

IV. BIG DATA ANALYTICS IN RISK MANAGEMENT

Big data analytics in Risk Management includes the following[7]:

- **Risk Assessment and Measurement**
  Risk modelling
  Scenario analysis
  Development of risk policies
  stress testing.
- **FrontOffice and Risk Operations**
  Front Office decision support
  Collateral management
  Capital allocation and liquidity management
  Risk based pricing.
- **Risk Control and Monitoring**
  Fraud detection and prevention
  Counterparty risks
  Positions limits monitoring
  monitoring g risk parameters.
- **Risk reporting and Governance**
  Dashboards and reports
  Response to data requests
  Regulatory reporting
  Model validation

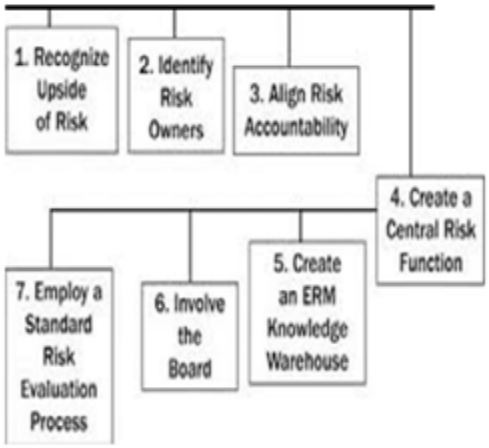

Figure2: Risk Management Using Bigdata

Figure2 provides the architecture of Risk management system using bigdata. The system first recognises the main cause for t he risk and then identifies the source which has caused the risk .Then maintains the accountability of risk causing sources. Creation of centralized risk management system is done[10].A ERM Knowledge Warehouse is created and risk handling centralized board is been maintained.The system employs standard risk evaluation process, which effectively manages the risks.

V. CONCLUSION

Risk management using Bigdata is proved to be more efficient than the traditional approach of risk management.Risk management using bigdata creates an ERM Knowledge database which effectively manages the risks in the organization which includes huge amount of resourses.The proposed system easily recognises all categories of risks and manages them in a efficient manner.

REFERENCES

[1] D. L. Olson and D. Wu, Enterprise Risk Management Models. Heidelberg, Germany: Springer, 2010.

[2] D. Wu, D. L. Olson, and C. Luo, "A decision support approach for accounts receivable risk management," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 12, pp. 1624–1632, 2014.

[3] D. Wu, D. L. Olson, and A. Dolgui, "Decision making in enterprise risk management: A review and introduction to special issue," Omega, vol. 57, pp. 1–4, 2015.

[4] M. Baucells and F. H. Heukamp, "Probability and time tradeoff," SSRN working paper, 2009.

[5] P. Jorion, "Risk management lessons from the credit crisis," Eur. Financial Manage., vol. 15, no. 5, pp. 923–933, 2009.

[6] D. Wu, "Introduction to the special SERRA issue," Stoch. Environ. Res. Risk Assess., vol. 25, no. 3, pp. 301–304, 2011.

[7] Tom Patterson,"The Use of Information Technology in Risk Management",September 2015 Whitepaper.

[8] Alok Bisni,"Manaaging Enterprise Financial Risk using Bigdata technologies", whitepaper

[9] Desheng Wu and John R. Birge," Risk Intelligence in Big Data Era: A Review and Introduction to Special Issue", IEEE TRANSACTIONS ON CYBERNETICS, VOL. 46, NO. 8, AUGUST 2016.

[10] James Joshi, Balaji Palanisamy " Towards Risk-aware Policy based Framework for Big Data Security and Privacy**"** (Position Paper).

[11] H. V. Jagadish, Johannes Gehrke, Alexandros Labrinidis, Yannis Papakonstantinou, Jignesh M. Patel, Raghu Ramakrishnan, Cyrus Shahabi, "Big Data and Its Technical Challenges," Communications of the ACM, Vol. 57 No. 7, Pages 86-94

[12] H. Takabi, and James B. D. Joshi. Semantic Based Policy Management for Cloud Computing Environments. International Journal of Cloud Computing, Vol. 1, No. 2, 2012.

[13] H. Takabi, James B. D. Joshi, and Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security and Privacy, Vol. 8, No. 6, 2010.

[14] Min Chen, Shiwen Mao, Yunhao Liu, "Big Data: A Survey," April 2014, Mobile Networks and ApplicationsVolume 19, Issue 2, pp 171-209

[15] Lei Jin, James B. D. Joshi, Mohd Anwar: Mutual-friend based attacks in social network systems. Computers & Security 37: 15-30 (2013)

[16] Matt Blaze, Sampath Kannan, Insup Lee, Oleg Sokolsky, Jonathan M. Smith, Angelos D. Keromytis, Wenke Lee: Dynamic Trust Management. IEEE Computer 42(2): 44-52 (2009)

[17] Michael Chuang, Suronapee Phoomvuthisarn, James B. D. Joshi, "An Integrated Framework for Trust-Based Access Control for Open Systems," CollaborateCom 2006, GA, USA

[18] Nathalie Baracaldo, James Joshi "An Adaptive Risk Management and Access Control Framework to Mitigate Insider Threats" Computers & Security. 2013.

[19] Nathalie Baracaldo, James Joshi "Beyond Accountability: Using Obligations to Reduce Risk Exposure and Deter Insider Attacks" ACM Symposium on Access Control Models and Technologies (SACMAT), Amsterdam, The Netherlands. 2013.

[20] Suroop M Chandran, Korporn Panyim, James B. D. Joshi, "A Requirements-Driven Trust Framework for Secure Interoperation in Open Environments", The Fourth International Conference on Trust Management, (iTrust-06)

[21] Weitzner et. al, "Consumer Privacy Bill of Rights and Big Data: response to White House Office of Science and technology Policy Request for Information," April 4, 2014.