Journal of Global Information Management
Volume 31 • Issue 3

Application of Big Data Technology in Enterprise Information Security Management and Risk Assessment

Yawen Wang, School of Economics and Management, Xi'an University of Technology, China
Weixian Xue, School of Economics and Management, Xi'an University of Technology, China*
Anqi Zhang, School of Management, Shanghai University of International Business and Economics, China
https://orcid.org/0000-0002-5878-3728

ABSTRACT

Nowadays, the application of enterprise management information has been deeply rooted in daily business activities, and the management risk of enterprise information security (EIS) has also increased. The use of advanced means to provide security protection for it has become the top priority. To optimize the EIS management system, and carry on the risk assessment (RA), firstly, this study analyzes the current situation of the enterprise's internal information management and summarizes the shortcomings and security risks faced by the system. In the era of big data (BD), the security risks of database information systems show a diversified trend. Secondly, to explore the application of BD technology in EIS management, the characteristics of this technology and security control measures for risks are summarized to strengthen the enterprise's information management innovation and implement the application of data security technology.

KEYWORDS

Assessment System, Big Data Technology, Enterprise Management, Information Security Guarantee, Risk Assessment

INTRODUCTION: APPLICATION OF BIG DATA TECHNOLOGY IN ENTERPRISE INFORMATION SECURITY MANAGEMENT AND RISK ASSESSMENT

As information interaction becomes more and more convenient, the security of message data (MD) gradually becomes the focus of social groups. Among them, all kinds of enterprises in social communities place the highest requirements and importance on information security (IS) (Kong et al., 2018). IS risk refers to the possibility of information being damaged in the whole life cycle, which is a security event caused by the threat of system vulnerability and the degree of loss it may cause to the system. The three elements of IS risk include asset, danger, and vulnerability. The relationship among them is as follows. Threats exploit system vulnerabilities to lose or affect investments (El Mrabet et al., 2018). The ultimate purpose of the overall risk analysis and assessment of IS is to ensure the

DOI: 10.4018/JGIM.324465 *Corresponding Author

integrity, availability, confidentiality, and controllability of the information assets in the enterprise and determine the existing risks and their intensity. Thus selecting targeted security protection measures and reducing risks, so that the risks can reach an acceptable level (Zio, 2018).

Big data technology (BDT) is extensively used in enterprises and has rapidly become a vital technical guarantee means. Based on BDT, more enterprises have applied risk control management recently. Using big data is conducive to constantly improving the risk control system and establishing a good and lasting system (Choi et al., 2018). Compared with traditional technology, big data has added more dimensions and relevance analysis in risk control. BDT is widely applied to the field of the internet to carry sensitive personal data information of users. After cleaning the source data, it is adopted mainly in the call access of different business systems. Because this personal data is susceptible and valuable, the security construction of the big data platform has become an urgent task for enterprise information security (EIS) construction and risk management (Syafrudin et al., 2018).

Based on the above problems, the theoretical framework of big data and IS management systems is studied first. The ideas of data security construction of enterprise information under the background of big data are sorted out through the theoretical framework. Secondly, according to the characteristics of current big data, a risk assessment (RA) model of IS is implemented to evaluate and control the overall risk of EIS more accurately. Finally, the RA system is constructed by a decision tree (DT) algorithm. A set of assessment systems with platform universality is developed to carry out the RA of all aspects of EIS in the big data environment. Meanwhile, suggestions and solutions are put forward for the risk points, and the designed RA system of IS is tested, verified, analyzed, and improved. This paper can effectively improve the awareness and ability of EIS-RA and adequately carry out information system security RA and control.

LITERATURE REVIEW

As the essential work of information systems and information asset security, the RA of IS has been widely studied and applied in recent years. The evaluation process of the RA method proposed by Wangen et al. (2018) mainly involves five core steps: first, analysis and identification of risk points; second, determination of the attribute of the consequences of the risks; third, determination of the attribute value of the consequences; fourth, calculation of the threat index brought on by the dangers; and fifth, overall sensitivity analysis and optimization of the results. Based on the specific data analysis information of Qingdao Haier Group, Kure et al. (2018) analyzed the impact of data analysis (DA) on enterprise data management and proposed relevant strategies to promote the effective application of DA in enterprise risk management (ERM). By establishing a management platform for contract critical information collection and risk control systems, Mayer et al. (2019) realized the integration of risk information and data of construction contracts. Also, professional DA was formed using grid management of the system and intelligent screening of the multi-dimensional analysis module, which was helpful to improve the identification ability of contract implicit risk and provide support for the business decision and ERM (Mayer et al., 2019).

BDT has been applied in all walks of life, spawning a new operating model for enterprises. Vassakis et al. (2018) first introduced mining and DA of big data in their study. Then they analyzed the application of big data analysis techniques in financial investment risk management, which is expected to contribute to the following research. Taking various elements of RA as clues, Raguseo (2018) introduced risk parameters based on big data and constructed a new RA model by referring to industry characteristics and primary classification of evaluation items to solve the problem of the lack of pertinence in the risk rating of non-conforming items in grade protection assessment and achieved the effect of establishing a scientific and reasonable RA system. Saggi and Jain (2018) believed that the emergence and development of big data made it possible to extract, analyze, and predict the state of EIS through the big data model algorithm from massive data, which provided a comprehensive perspective and security guarantee for the IS management of large enterprises.

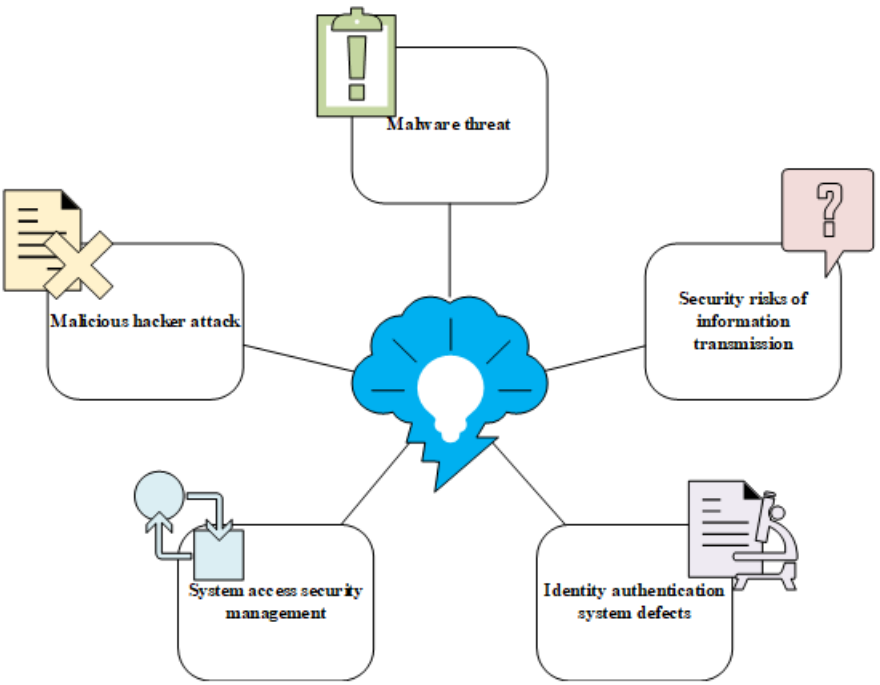
To sum up, recent scholars have conducted relevant evaluation work on the RA method of IS and the application of BDT, which has good guidance and practicability. However, the actual application of enterprise management has not been shown, and it is inconsistent with the adaptation environment and difficult to apply. This study mainly explores the RA system of EIS and designs and develops a set of relevant systems using the current swift growth of BDT. The existing research only focuses on improving theoretical approaches and technology, ignoring the evaluation of technology implementation. This study focuses on ensuring that the designed system has early reasonable risk warning capability. The purpose is to realize the input and management of EIS's assessment items and RA information, thus conducting RA on the collected information through a trained RA model and obtaining corresponding results.

Methods and Materials

Risk Management Status of EIS

With the continuous development of economic construction and the arrival of the knowledge economy model, domestic enterprises are committed to improving internal management quality and efficiency with unprecedented enthusiasm and realising office automation through information means. Network information system (NIS) becomes one of the infrastructures of enterprise offices (Bozkus Kahyaoglu & Caliyurt, 2018; Meng et al., 2022). The common characteristics of enterprises are complex organizations and a large amount of users, enormous loads of various application software systems, and large amounts of data. Enterprises often have higher construction goals, and they want to improve management and collaboration efficiency by implementing office automation, so they also put forward higher requirements for the NIS that carries this service (Paté-Cornell et al., 2018). At the present stage, IS risks mainly cover five aspects, as displayed in Figure 1.

Figure 1. IS risks



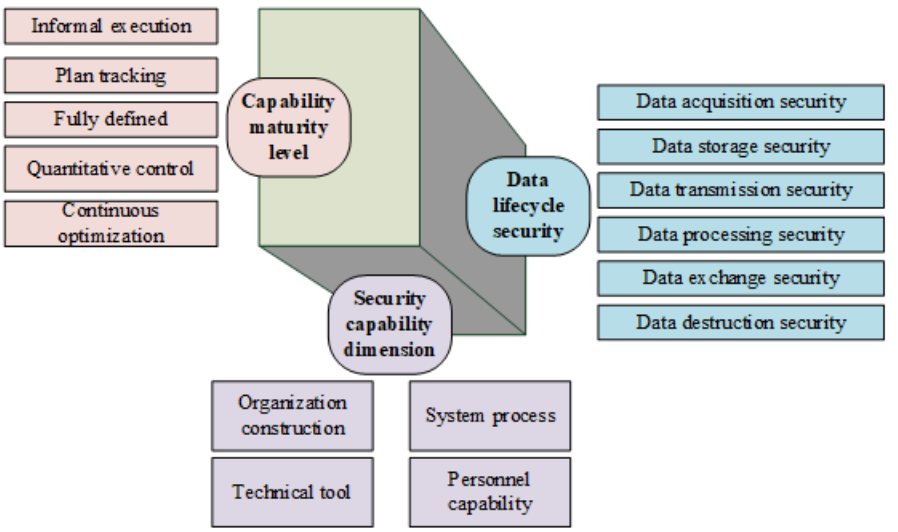
At this stage, the five aspects of IS risks include malicious software threats such as computer viruses, hacker attacks, troubles in the process of information transmission, security management of information system access control, and design defects in the identity authentication system. The management of EIS should adhere to the idea of taking data information as the centre. Data security management applies security technology and constructs data organization, system processes, technical tools, and personnel ability (Lechner & Gatzert, 2018). The maturity model of IS management capability is a set of methodologies obtained by combining management and general practice, which has vital theoretical and practical guiding significance for the construction of internal data security in enterprises. Its theoretical basis has been generally applied in various enterprises, and more and more companies take it as a reference point in the construction process of IS management ability (de Araújo Lima et al., 2020). The specific model structure is denoted in Figure 2.

The established EIS management maturity model is three-dimensional, including capability maturity level, data lifecycle security, and security capability dimension. The capability maturity level is divided into five classes: informal execution, plan tracking, fully defined, quantitative control, and continuous optimization. Data lifecycle security includes acquisition, storage, transmission, processing, exchange, and destruction. The security capability dimension is divided into four dimensions: organization construction, system process, technical tools, and personnel capability.

Effectively conducting quantitative management analysis in the collected data to ensure the information system's safe, scientific, and stable operation is almost impossible to achieve by using the traditional analysis method based on a relational database (Baryannis et al., 2019). Therefore, BDT is employed to collect data on the operational behavior of enterprise user terminals. The analysis of terminal usage, terminal application usage, and terminal behavior characteristics provides tools for the company to conduct safe operation analysis and quantitative management of enterprise information systems. The results are presented in Ustundag et al., 2018.

The database information system in the big data era faces a variety of security risks, such as Trojan viruses and hacker attacks, and it is characterized by diversified security attack forms and channels, the rapid growth of this system's vulnerabilities, intelligent security threats, etc. (Radanliev et al., 2018; Feng & Chen, 2022).

Figure 2. The maturity model of EIS management



Firstly, the rapid development and progress of cloud computing, distributed computing, mobile computing, and other technologies have brought potential attacks. Additionally, people use big data resources to diversify attack forms and channels. Security attacks can use application software access, mail transmission, data collection, and other ports to attack the data information system. In addition to Trojans, viruses, and hackers, attacks also take the form of denial of service and network disconnection.

Secondly, the rapid growth of database information system vulnerabilities has led to the information system facing a variety of access modes, such as offline, online, breakpoint continuation, etc. These access modes make the vulnerability of database information systems rise continuously in the application and bring potential threats to the protection of information systems.

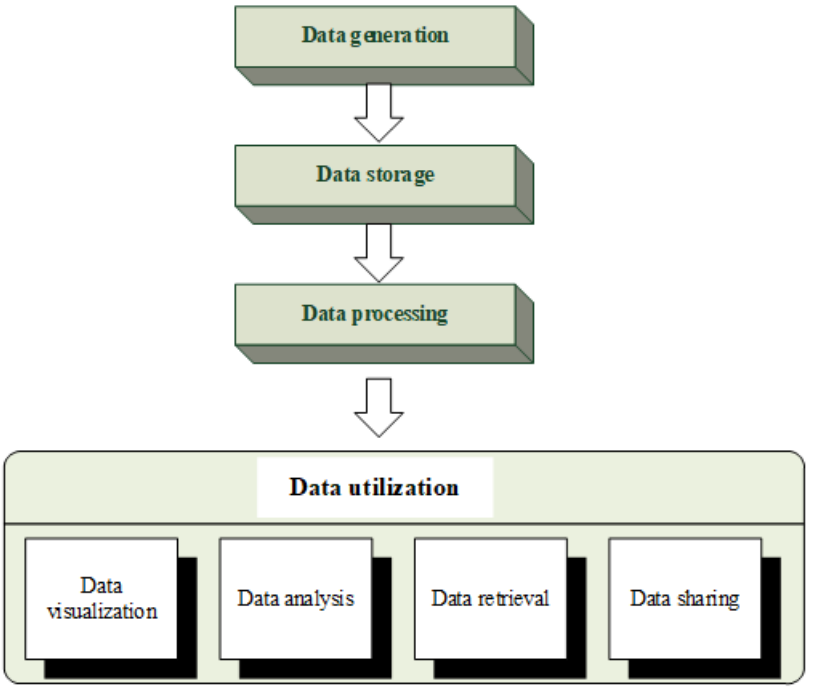
Finally, the security threat intelligence of the database information system also rapidly improves the Trojan Horse, virus, and hacker attacks spread in the network. These viruses show the characteristics of intelligence. They have a longer latent time, a faster transmission speed, a more comprehensive range of infections, and are more difficult to scan by RA and security defence technology. Once these attacks break out, they will seriously impact the database information system.

Evaluation of Information Risk in BDT

Big data means information data of an enormous scale, which cannot be acquired, processed, and stored by traditional methods, nor can it be directly sorted into usable information for production applications (Zhang et al., 2021; Miao, 2023).

Big data has a broad and narrow sense, and big data in a broad sense includes BDT, big data applications, big data engineering, and big data science. In a narrow sense, big data only indicates the large-scale and complex data collection and technical systems for analyzing, storing, and managing big data based on the characteristics of volume, variety, velocity, and veracity (4V) (Oussous et al., 2018; Cheng & Yang, 2022). The process of data information is presented in Figure 3.

Figure 3. Information processing under the background of big data

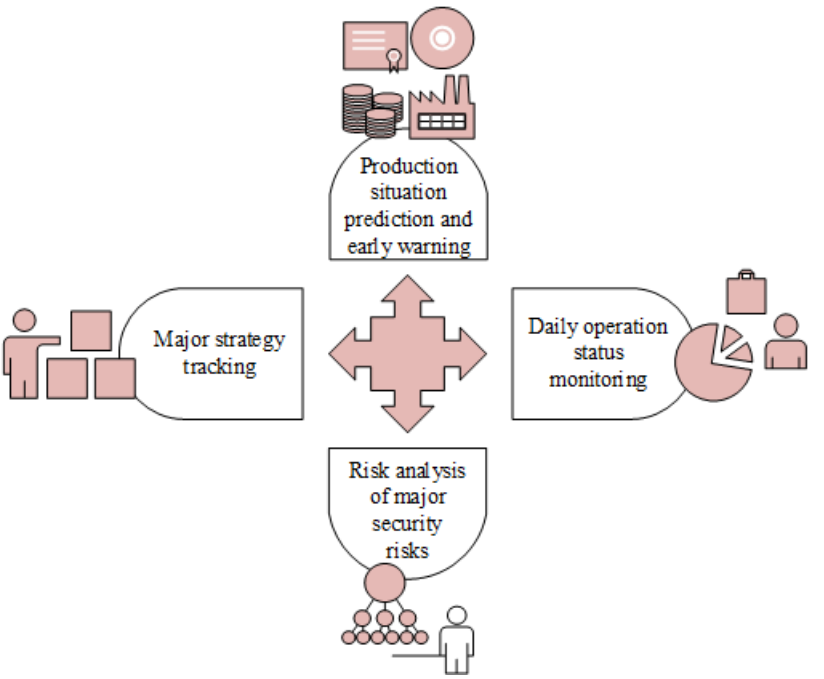


Big data research is a systematic study that roughly includes data generation, storage, processing, and utilization (Yu et al., 2021). The data generation part needs to be cleaned to ensure the quality and credibility of the data. After the data is collected, it is stored and pre-processed, including de-duplication, exception handling, and normalization. Then, the data is stored in a large distributed database or storage cluster. The data can be used after processing, including sharing, retrieval, analysis, and visualization. Data statistical analysis requires tools like Statistical Product and Service Solutions (SPSS). Some structural algorithm models are used for classification and summary to meet the analysis requirements of various data. Finally, the data is analyzed visually. Visual analysis can intuitively present the characteristics of big data. Additionally, this analysis method is straightforward enough to be accepted by users, making complex data simple after analysis.

The application mode of big data itself is an emerging product of information technology (IT) development. It has mass data storage and can accurately process massive information through data operation (Urbinati et al., 2019; Lei et al., 2022). The big data analysis core is realized through ”data warehouse + data platform”, in which the data warehouse integrates the data of various business lines to eliminate data islands. Data platforms have different characteristics and positioning (Wu et al., 2020). When establishing the big data risk prevention and control enterprise management platform, to achieve real-time and precise risk control and protection, the platform should have the functions shown in Figure 4.

First, risk identification should be carried out truly and reliably. Data association analysis and rule mining should be performed through automatic, systematic, and intelligent processing to make up for the shortcomings of traditional risk identification methods. Second, it is necessary to be able to conduct RA based on big data, integrate and mine the database, carry out model analysis, and realize the RA grading of data. Next, it needs to implement the risk warning, prediction, and control of big data, organically combine the safety science theory and big data theory, and predict the trend of accidents that may be formed in the future, thereby eliminating or controlling the safety risks in

Figure 4. Basic requirements of big data risk control management



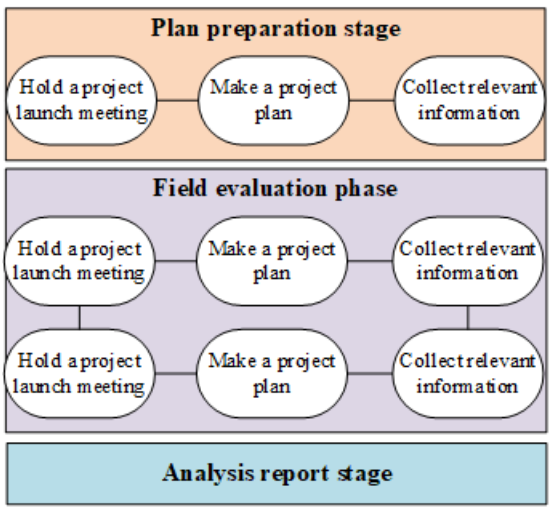
a targeted way and giving scientific data support for risk management decision (Aryal et al., 2020; Tchuente, 2022).

An enterprise information system's security RA process can be roughly divided into three stages: plan preparation, field evaluation, and analysis report. The work contents and steps of the three stages are shown in Figure 5.

In the preparation stage of the plan, three tasks need to be carried out. (1) Preparation of project plan. The evaluation objectives, scope, and objects need to be determined. The organization of evaluators, including the project leading group, the leader, the project technical advisory group, the RA group, the project coordinator of the evaluated unit, and the project cooperation personnel, should be informed. The project schedule is formulated. The project communication and cooperation system has been clarified. (2) The project kick-off meeting is held to mobilize the project before the evaluation. (3) Collection of relevant information. All asset information of the appraisal object is collected. The collected information includes security management, technical facilities, application system, and computer room environment.

The field evaluation stage includes document review, questionnaire survey, vulnerability scanning, local audit, penetration test, on-site observation, and personnel interview. (1) Document review. Based on the document review, the experiment is used to understand the basic information of the evaluation object, the problems found, and the implemented security measures. The information learned through the interview and the clarified questions are determined to minimize the time of personnel interview and communication and reduce the impact of the evaluation on normal business. (2) Questionnaire. A group of related closed or open questions is used to obtain the security status of the information system at all levels during the evaluation process, including security strategy, organizational system, implementation, etc. (3) Vulnerability scanning. Technical means are used to identify information system components and collect information on possible technical vulnerabilities of each element for detailed analysis at the analysis stage. (4) Local audit. Local audit and vulnerability scanning can complement each other. Information on possible technical vulnerabilities of various information system components is collected for detailed analysis at the analysis stage. (5) Penetration test. Hacker attack methods are used to simulate and discover the exploitable weaknesses of networks and systems. The simulation aims to detect the system's security configuration and find potential configuration problems. (6) On-site observation. On-site inspection and observation methods are used to observe the management system related to the application system and the computer room environment, the

Figure 5. Steps of security RA of enterprise information system



mechanism related to safe operation and maintenance, and the system configuration status. The on-site observation can understand the actual implementation of the system, retain the inspection evidence, and fill in the results.

The main work of the analysis report stage is to sort out the data obtained from the on-site evaluation, conduct a comprehensive analysis, and generate the final assessment. The collected information is comprehensively analyzed and the system/asset vulnerability is sorted out. Vulnerability is subject to threat analysis, including analysis of the possibility and consequences of threat occurrence, determination of risk level, and formulation of the risk treatment plan. Comprehensive analysis requires a higher ability of analysts. The personnel who lead the comprehensive analysis and report generation must have participated in all stages of information system RA and master the methods, means, processes, calculation methods, and fundamental RA theories. Additionally, they should also have strong writing and expression skills (Wang & Dai, 2022).

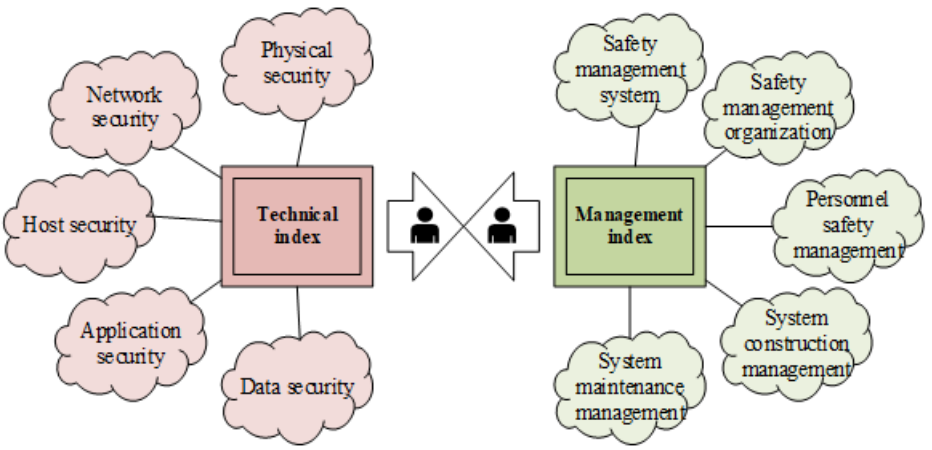
Establishment of the RA System

The RA system includes data collection, pretreatment, identification, and IS RA classification. According to the decision algorithm modelling and the established data model, the IS risk of the new instance is evaluated and a conclusion is drawn. The first two parts have been introduced above. Next, this study will present the DT algorithm modelling.

Before system design and development, it is necessary to investigate the background and relevant theoretical knowledge of IS's RA. Because of EIS-related background and risk item characteristics in the rapidly developing internet environment, an appropriate DA model can be selected to design relevant system architecture according to specific functional requirements (Dai et al., 2020; Dai, 2022). According to the four related concepts of asset, threat, vulnerability, and security control measures proposed in the RA standard of IS and the relevant standards of national-level protection, this study summarizes the elements of RA of IS, as portrayed in Figure 6.

This study introduces the DT algorithm into the RA study of EIS in the big data environment. The complex problem of relevant indicators is simplified relatively intelligently in RA of EIS in this environment. The DT-based evaluation algorithm can be applied well to irregular data. It can use limited information to analyze and deal with incomplete and uncertain phenomena. In addition, it can also focus analysis points on indicators with a higher proportion of risk factors, which has the characteristics of paying more attention to evaluation results (Liao & Liu, 2022).

Figure 6. Elements of RA for IS



The data source is pre-processed using the DT algorithm, and each attribute's information gain (IG) and IG ratio are calculated. IG ratio will be used as an example of selecting variable attributes. The entropy of training samples should be calculated first, and the expression is shown in Equation 1:

$$info\left(T\right) = -\sum_{J=1}^{K} \frac{freq\left(C_j \cdot s\right)}{\left|s\right|} \cdot log_2 \left(\frac{freq\left(C_j \cdot s\right)}{\left|s\right|} \right) \tag{1}$$

In Equation 1, freq(C_j, s) represents the sample size of class *Ci* in the set *s*, which belongs to one of the *k* classes, and $\left|s\right|$ stands for the sum of the sample sizes in *s*.

Then, according to the non-category attribute X, the data set is divided into sets of subsets, and the entropy of these subsets is weighted according to the formulated RA system of IS. The calculation is illustrated in Equation 2:

$$infox\left(T\right) = -\sum_{j=1}^{j} \frac{\left|T_j\right|}{\left|T\right|} \cdot info\left(T_j\right) \tag{2}$$

info(T_j) refers to the entropy value of the training sample. The difference is calculated according to Equation 1 and Equation 2 to get IG: Gain(X). Since IG prefers to select attributes with more values when selecting attributes, it is necessary to calculate the IG ratio, which divides the objects to be evaluated individually. Considering the size of the subset after each division and the number of each subset, there is no longer a need to consider the amount of information contained in the subset after classification, as indicated in Equation 3:

$$Split\_Infox\left(X\right) = -\sum_{j=1}^{j} \left(\left(\left|T_j\right| / \left|T\right| \right) \cdot log\left(\left|T_j\right| / \left|T\right| \right) \right) \tag{3}$$

IG ratio is expressed as shown in Equation 4:

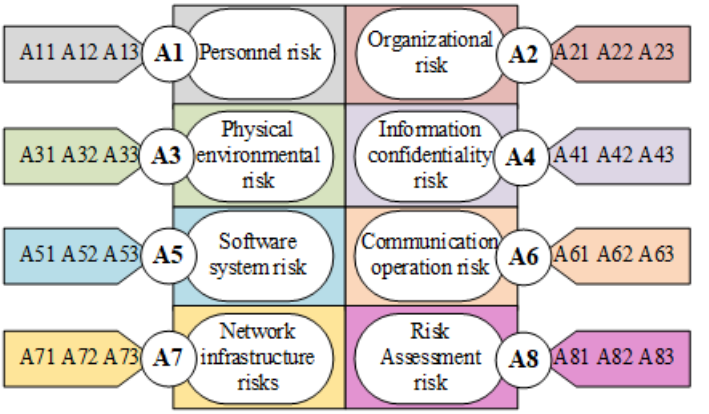
$$Gain\,ratio\left(X\right) = Gain\left(X\right) / Split\_Infox\left(X\right) \tag{4}$$

The structure of DT is adopted to design the decision rules of data in the decision-making process so that the new data sets can be classified (Xu & Duan, 2019).

RA of IS in a big data environment is a complex assessment process which requires continuity and dynamic adjustment (Zhu et al., & Li, 2022). The most important factors include the system's business strategy and security requirements, assets and value, vulnerability, threats and risks, measures to reduce risks, and residual risks. The implementation of RA must have an accurate understanding of its indicators. Therefore, it is necessary to select evaluation indexes that fit the actual situation and can make dynamic changes in real-time. According to the above requirements, essential risk reference elements conforming to the big data environment are selected from massive RA indexes of IS, including 8 first-level and 24 second-level indexes (Yang et al., 2022), as represented in Figure 7.

In Figure 7, the secondary indexes of personnel risk (A1) include personnel management system (A11), personnel post-safety responsibility (A12), and personnel technical ability (A13). The secondary indexes under organizational risk (A2) involve IS organization structure (A21), organizational culture awareness (A22), and human and financial security (A23). The secondary indicators of physical

Figure 7. Indicator system of RA



environment risk (A3) cover physical access control policy (A31), power supply security (A32), and standby working site (A33). Confidentiality policy (A41), user access identity authentication (A42), and data backup (A43) are the secondary indexes of information confidentiality risk (A4). The secondary indexes of software system risk (A5) are composed of operating system access control (A51), database system access control (A52), and application system access control (A53). The secondary indexes of communication operation risk (A6) include network isolation and access control (A61), firewall access control and audit (A62), and intrusion detection access control audit (A63). The secondary indexes of network infrastructure risk (A7) consist of line security (A71), computer security (A72), and network equipment security (A73). The secondary indexes of RA risk (A8) contain the RA system (A81), the rationality of assessment technology (A82), and irregular RA (A83).

RESULTS

According to the design scheme of the system, the main functional modules of the system are tested. Its contents include: (1) The system process can be normal flow. (2) The system data can be stored typically, and the correct evaluation results can be calculated. (3) Whether system security and system logs are recorded typically. The conventional methods' risk grading results are compared with the big data-based risk grading results, where 1, 2, and 3 signify low, medium, and high risk. The grading results are plotted in Figure 8.

The results display that in the conventional method. However, the influence degree of network attack threat is high, considering the possibility of success of network attack is low, the risk is determined to be medium. However, the corresponding assets of network attacks are service and data, which are the main assets in the core business of enterprises, and will cause severe damage once a security accident occurs. Considering assets, threats, and vulnerabilities, the risk level should be considered high. The risk level identified by BDT is generally higher than that of the conventional system, indicating certain identification flaws in the conventional risk rating, and that more serious risks are not identified (Wu & Zhang, 2022).

Finally, BDT evaluation investigates high, medium, and low-risk evaluation indexes. According to the standard index table, an enterprise is evaluated on the spot, and each index is assessed and investigated to obtain relevant evaluation results. Specific data are exhibited in Table 1.

The system is evaluated by DA, and the final overall RA conclusion is reasonable. Additionally, given the substandard items in the evaluation process, the corresponding treatment opinions and

Figure 8. Comparison of risk rating differences

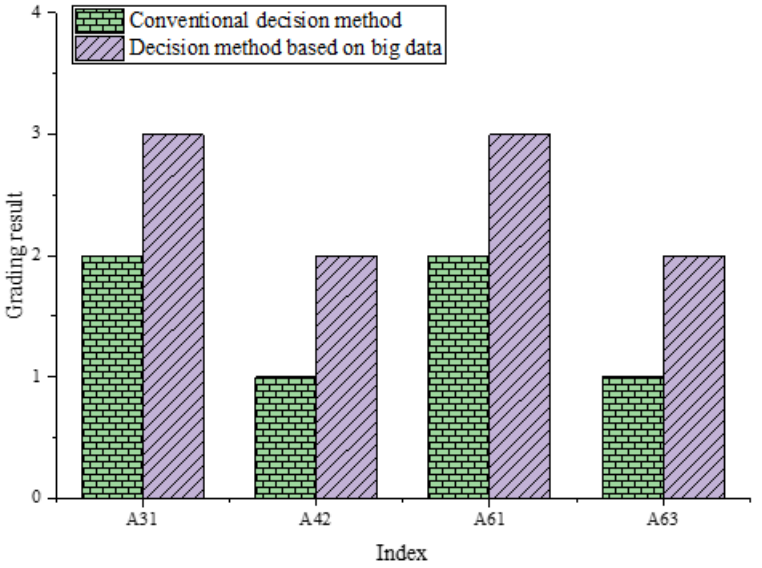


Table 1. RA of enterprise information systems

Index risk rating	First-level indexes	Second-level indexes	Compliant	Partially compliant	Non-compliant
High risk	Personnel risk (A1)	A11	/	/	√
		A12	/	√	/
		A13	/	/	√
Medium risk	Physical environment risk (A3)	A31	√	/	/
		A32	/	√	/
		A33	/	√	/
Low risk	Organizational risk (A2)	A21	√	/	/
		A22	/	√	/
		A23	√	/	/

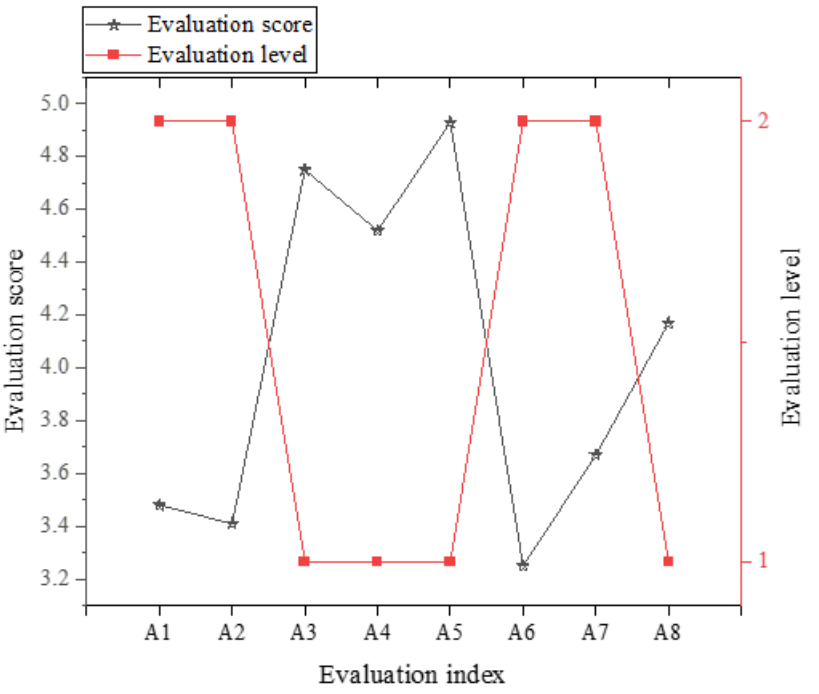
rectification plans are given. Thus, risks can be effectively avoided, and emergency rectification measures can be implemented to ensure timely control of the IS management of the system.

The established model tests the safety levels of the first-level indicators. The score and evaluation grade results are shown in Figure 9.

In Figure 9, evaluation level 1 means the first level of safety; level 2 indicates secondary protection. The EIS risk level is at the secondary security level. The risks of the physical environment, information confidentiality, software system, and RA are at the first level. Personnel, organization, communication operation, network infrastructure, and other risks are at the second level. In this enterprise, personnel, organization, and communication network are the main hidden dangers of IS risks.

This test is aimed at a specific instance, and the instance data is inputted and evaluated in the assessment system. Meanwhile, a comparative analysis is made between the result of the example data

Figure 9. Grade I index score and grade evaluation



running in the system and the evaluation report given by the authoritative evaluation organization. The example evaluated by the assessment system is similar to the evaluation result assigned by the authoritative organization, confirming that the RA application system has a specific evaluation reference value. The evaluation results are significant when the enterprise carries on the risk judgment and the safety construction.

DISCUSSION

Guo and Wang (2020) analyzed the application scenarios of big data in the internet finance (ITFIN) industry and explored the data security risks and challenges ITFIN enterprises face by combining them with actual cases. Given these risks and challenges of IS, relevant protection strategies are formulated and implemented to provide relevant reference ideas for ITFIN enterprises in the IS governance construction under the background of big data and to continuously improve and enhance the overall protection level of IS of these enterprises. Huang et al. (2019) explained the basic concept and main advantages of BDT and discussed the basic demands for establishing a big data risk prevention and control management platform. Additionally, the challenges brought by BDT to traditional safety management and the solution ideas were analyzed, which was conducive to the introduction of BDT by enterprises in combination with the actual management and promoting the construction of safety management informatization and realizing early warning and precise prevention and control of security risks. Some achievements have been made in the existing research, but a relatively mature technical route has not been proposed to support more research in the future. Based on existing theories, the DT algorithm is introduced into the study of RA of EIS in the big data environment. A relatively intelligent way is tried to simplify the complex issues related to evaluation indicators in the RA of IS in the relevant domain. The results manifest that the emergence of BDT has effectively contributed to

the IS and solved the risk problems, such as virus invasion, to the greatest extent through its technical means, thereby providing a guarantee for EIS management.

CONCLUSION

Based on the RA management platform of EIS established by BDT, through collecting, summarizing, and collating massive information and data generated by enterprise production activities, this study timely and accurately analyzes and predicts risks, accurately prevents hidden risks of safety accidents, and realizes instant feedback and directional warning of hidden risks. Furthermore, corresponding prevention and response measures have been proposed, which is an important management means to break the "information island" and prevent and control enterprise security risks scientifically and accurately. This study analyzes the current situation of enterprise internal information management and summarizes the deficiencies and security risks faced by the system. The application and characteristics of big data technology in EIS management and the security control measures for risks are explored and summarized to strengthen the innovation and application of information management. Finally, the DT algorithm is used to establish a RA system, develop a system with platform universality, and realize the system RA of IS. The main functional modules of the system are tested according to the design scheme of the system. The results show that the RA system based on big data technology has specific risk identification and early warning capabilities and can be used in EIS management for a long time to come.

Although this study has obtained some achievements, there are still some deficiencies in the method. The study has not been able to integrate data from different sources into a cloud computing analysis platform. The small amount of data leads to inaccurate risk factors. The test results are not targeted to some extent. This problem will be solved as soon as possible in the follow-up exploration.

FUNDINGS

This work was supported by the National Natural Science Foundation of China (Project No. 70673080,71073125) and Research project on major theoretical and practical issues in philosophy and social sciences of Shanxi Province (Project No. 2019XYZ007,2022ZD0717).

REFERENCES

Aryal, A., Liao, Y., Nattuthurai, P., & Li, B. (2020). The emerging big data analytics and IoT in supply chain management: A systematic review. *Supply Chain Management*, *25*(2), 141–156. doi:10.1108/SCM-03-2018-0149

Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. *International Journal of Production Research*, *57*(7), 2179–2202. doi:10.1080/00207543.2018.1530476

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360–376. doi:10.1108/MAJ-02-2018-1804

Cheng, L., & Yang, Y. (2022). The effect of online reviews on movie box office sales: An integration of aspect-based sentiment analysis and economic modeling. [JGIM]. *Journal of Global Information Management*, *30*(1), 1–16. doi:10.4018/JGIM.298652

Choi, T. M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. *Production and Operations Management*, *27*(10), 1868–1883. doi:10.1111/poms.12838

Dai, H. N., Wang, H., Xu, G., Wan, J., & Imran, M. (2020). Big data analytics for manufacturing internet of things: Opportunities, challenges and enabling technologies. *Enterprise Information Systems*, *14*(9-10), 1279–1303. do i:10.1080/17517575.2019.1633689

Dai, W. (2022). Application of improved convolution neural network in financial forecasting. [JOEUC]. *Journal of Organizational and End User Computing*, *34*(3), 1–16. doi:10.4018/JOEUC.289222

De Araújo Lima, P. F., Crema, M., & Verbano, C. (2020). Risk management in SMEs: A systematic literature review and future directions. *European Management Journal*, *38*(1), 78–94. doi:10.1016/j.emj.2019.06.005

El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469–482. doi:10.1016/j.compeleceng.2018.01.015

Feng, Z., & Chen, M. (2022). Platformance-based cross-border import retail e-eommerce service quality evaluation using an artificial neural network analysis. *Journal of Global Information Management*, *30*(11), 1–17. doi:10.4018/JGIM.306271

Guo, J., & Wang, L. (2020). Learning to upgrade internet information security and protection strategy in big data era. *Computer Communications*, *160*, 150–157. doi:10.1016/j.comcom.2020.05.043

Huang, L., Wu, C., & Wang, B. (2019). Challenges, opportunities and paradigm of applying big data to production safety management: From a theoretical perspective. *Journal of Cleaner Production*, *231*, 592–599. doi:10.1016/j.jclepro.2019.05.245

Kong, W., Lei, Y., & Ma, J. (2018). Data security and privacy information challenges in cloud computing. *International Journal on Computer Science and Engineering*, *16*(3), 215–218.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Basel, Switzerland)*, *8*(6), 898. doi:10.3390/app8060898

Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: Empirical evidence from Germany. *European Journal of Finance*, *24*(10), 867–887. doi:10.1080/1351847X.2017.1347100

Lei, Z., Gong, G., Wang, T., & Li, W. (2022). Accounting information quality, financing constraints, and company innovation investment efficiency by big data analysis. [JOEUC]. *Journal of Organizational and End User Computing*, *34*(3), 1–21. doi:10.4018/JOEUC.292525

Liao, S., & Liu, Z. (2022). Enterprise financial influencing factors and early warning based on decision tree model. *Scientific Programming*, *2022*, 1–8. doi:10.1155/2022/6260809

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2019). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling*, *18*(3), 2285–2312. doi:10.1007/s10270-018-0661-x

Meng, T., Li, Q., Dong, Z., & Zhao, F. (2022). Research on the risk of social stability of enterprise credit supervision mechanism based on big data. [JOEUC]. *Journal of Organizational and End User Computing*, *34*(3), 1–16. doi:10.4018/JOEUC.289223

Miao, R. (2023). Emotion analysis and opinion monitoring of social network users under deep convolutional neural network. [JGIM]. *Journal of Global Information Management*, *31*(1), 1–12. doi:10.4018/JGIM.319309

Oussous, A., Benjelloun, F. Z., Lahcen, A. A., & Belfkih, S. (2018). Big Data technologies: A survey. *Journal of King Saud University-Computer and Information Sciences*, *30*(4), 431–448. doi:10.1016/j.jksuci.2017.06.001

Paté-Cornell, M. E., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226–241. doi:10.1111/risa.12844 PMID:28679022

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, *102*, 14–22. doi:10.1016/j.compind.2018.08.002

Raguseo, E. (2018). Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. *International Journal of Information Management*, *38*(1), 187–195. doi:10.1016/j.ijinfomgt.2017.07.008

Saggi, M. K., & Jain, S. (2018). A survey towards an integration of big data analytics to big insights for value-creation. *Information Processing & Management*, *54*(5), 758–790. doi:10.1016/j.ipm.2018.01.010

Syafrudin, M., Alfian, G., Fitriyani, N. L., & Rhee, J. (2018). Performance analysis of IoT-based sensor, big data processing, and machine learning model for real-time monitoring system in automotive manufacturing. *Sensors (Basel)*, *18*(9), 2946. doi:10.3390/s18092946 PMID:30181525

Tchuente, D. (2022). User modeling and profiling in information systems: A bibliometric study and future research directions. [JGIM]. *Journal of Global Information Management*, *30*(1), 1–25. doi:10.4018/JGIM.307116

Urbinati, A., Bogers, M., Chiesa, V., & Frattini, F. (2019). Creating and capturing value from Big Data: A multiple-case study analysis of provider companies. *Technovation*, *84*, 21–36. doi:10.1016/j.technovation.2018.07.004

Ustundag, A., Cevikcan, E., Ervural, B. C., & Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. *Industry 4.0: Managing the Digital Transformation* (267-284).

Vassakis, K., Petrakis, E., & Kopanakis, I. (2018). Big data analytics: Applications, prospects and challenges. *Mobile Big Data: A Roadmap From Models to Technologies* (3-20).

Wang, J., & Dai, Y. (2022). The agglomeration mechanism of network emerging e-commerce industry based on social science. [JOEUC]. *Journal of Organizational and End User Computing*, *34*(3), 1–16. doi:10.4018/JOEUC.291561

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *International Journal of Information Security*, *17*(6), 681–699. doi:10.1007/s10207-017-0382-0

Wu, J., Wang, J., Nicholas, S., Maitland, E., & Fan, Q. (2020). Application of big data technology for COVID-19 prevention and control in China: Lessons and recommendations. *Journal of Medical Internet Research*, *22*(10), e21980. doi:10.2196/21980 PMID:33001836

Wu, J., & Zhang, K. (2022). Machine learning algorithms for big data applications with policy implementation. *Journal of Organizational and End User Computing*.

Xu, L. D., & Duan, L. (2019). Big data for cyber physical systems in industry 4.0: A survey. *Enterprise Information Systems*, *13*(2), 148–169. doi:10.1080/17517575.2018.1442934

Yang, J., Zhao, Y., Han, C., Liu, Y., & Yang, M. (2022). Big data, big challenges: Risk management of financial market in the digital economy. *Journal of Enterprise Information Management*, *35*(4/5), 1288–1304. doi:10.1108/JEIM-01-2021-0057

Yu, W., Wong, C. Y., Chavez, R., & Jacobs, M. A. (2021). Integrating big data analytics into supply chain finance: The roles of information processing and data-driven culture. *International Journal of Production Economics*, *236*, 108–135. doi:10.1016/j.ijpe.2021.108135

Zhang, X., Yu, Y., & Zhang, N. (2021). Sustainable supply chain management under big data: A bibliometric analysis. *Journal of Enterprise Information Management*, *34*(1), 427–445. doi:10.1108/JEIM-12-2019-0381

Zhu, W., Zhang, T., Wu, Y., Li, S., & Li, Z. (2022). Research on optimization of an enterprise financial risk early warning method based on the DS-RF model. *International Review of Financial Analysis*, *81*, 102–140. doi:10.1016/j.irfa.2022.102140

Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety*, *177*, 176–190. doi:10.1016/j.ress.2018.04.020