Indonesia Chapter #111

Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 7, Issue 2 (July-December) 2022

*Asia Pacific Fraud Journal now has been accredited "**SINTA 3**" by Ministry of Research and Technology of The Republic of Indonesia (No SK. 85/M/KPT/2020).*

Available online at: http://apfjournal.or.id/index.php/apf

Data Analytics of Procurement Fraud Risks in Indonesia

✉Mustofa Kamal
Pusdiklatwas BPKP, Bogor, Indonesia

ARTICLE INFORMATION
Article History:
Received September 23, 2021
Revised October 20, 2021
Accepted December 02, 2022

DOI:
10.21532/apfjournal.v7i2.264

ABTRACT

The era of digital transformation requires management and auditors to apply data analytics. This era also increases the risk of procurement fraud. This study aims to determine the application of data analytics in handling the risk of procurement fraud in the 4.0 era. Quantitative methods are applied with data analytics techniques to 2018 provincial tender data. The results show that descriptive statistical techniques can reveal the profile of collusion risk attributes. The average provincial construction tender in 2018 indicates a risk of collusion above 50% for the high price attribute. The visualization technique produces a tender collusion risk dashboard. There are 3 provincial LPSEs detected to meet the combined risk indications of collusion. The level of likelihood of collusion risk in the 3 provinces also shows "almost certain to occur" or with a value of 5. The results of this study have implications for data analytics which are very important to be immediately applied in government procurement to manage the risk of procurement fraud.

Keyword: Risk, Fraud, Data Analytics, Collusion, Procurement.

1. INTRODUCTION

The use of information and communication technology (ICT) has become part of the priority of government services in the areas of government administration, social, education, health, agriculture, urban ICT, and information dissemination. (Oktorialdi, 2019). The use of information systems must be adapted to the development of business scale and data complexity in the 4.0 era. This has consequences for the urgency of using methods or techniques in digital transformation (Bagas, 2018).

There are 2 (two) requirements for successful digital transformation: mastery of digital technology and competence in big data analytics. Data analytics competence is an important requirement to be able to play a role in the digital era (Oktorialdi, 2019). Data analytics is the process of inspecting, cleaning, transforming and modeling data sets with the aim of revealing information to support decision making (Telkom University, 2020). Data analytics also means the process of collecting and analyzing data. The use of big data

How to Cite:
Kamal, M. (2022). Data Analytics of Procurement Fraud Risks in Indonesia. *Asia Pacific Fraud Journal, 7*(2), 185-199. http://doi.org/10.21532/apfjournal.v7i2.264.

✉Corresponding author :
Email: kamalopek.bpkp@gmail.com

analytics can support better decision making and increase organizational value (Anderson et al., 2017; Mirarab et al., 2019). In the field of auditing, the use of data analytics by auditors in Malaysia is part of the revolution in audit work patterns in the internet of things era (Mohamed et al., 2019). In Indonesia, the role of internal auditors is required to transform according to the 4.0 revolution era in providing assurance to management (Asad et al., 2019). The value of internal audit will be better by optimizing data analytics from big data that can be obtained from management (Anderson et al., 2017).

There are four types of data analytics: descriptive, diagnostic, predictive and prescriptive analysis (principa.co, 2017). The auditing profession in the public sector allows the adoption of three data analytic cycles consisting of the use of more descriptive analysis, predictive analysis with lots of data, and prescriptive analysis with big data (Appelbaum et al., 2017). Data analytics can be applied in compliance audits, performance audits, and financial statement audits (CAGI, 2017; IIA, 2017). In fact, data analytics can be used for fraud analytics (Baesens et al., 2015) and fraud risk management (Horsey, 2017). Data analytics can be used to detect indications of fraud through analysis of several anomalies from the data (Banarescu, 2015; Gee, 2015; IIA, 2017), to uncover corruption schemes through association analysis of several transaction data (Gee, 2015), to uncover the risk of collusion in road construction tenders in Poland (Anysz et al., 2019), and to score the risk of collusion in tenders in Korea by determining its attributes based on law enforcement experience (Capobianco et al., 2017).

In Indonesia, previous data analytics research at https://garudaristekbrin.go.id shows that there are 35 (thirty five) articles with the keyword "data analytics" within a period of 5 years or in the time span from 2016 to 2020. Of all these articles, 34 (thirty four) articles can be mapped according to their fields, such as information and computer technology (ICT), supply chain management (SCM), research, health, astronomy, tax, agriculture, and education (appendix 1). There has been no research on data analytics in the field of procurement fraud or risk management or audits on the site within the period mentioned above.

There are several mandates related to data analytics and/or risk. These mandates include the implementation of an electronic-based government system in accordance with Presidential Regulation Number 95 of 2018, policies for the use of information technology in procurement in accordance with Presidential Regulation Number 12 of 2021, risk assessment and control according to the results of risk assessment based on Government Regulation Number 60 of 2008. Meanwhile, the use of information technology opens the door to Information Technology Risks (IT risks) (Anderson et al., 2017; Panuntun, 2020). In the digital era of procurement, procurement management and auditors encounter seven risks of procurement fraud that require data analytics to manage them (Kamal, 2020).

Based on all the descriptions above, it is revealed that there is an urgency in implementing data analytics in the digital transformation of the procurement sector to handle the risk of procurement fraud in the digital era. Therefore, there is one research question that needs to be answered; How is the application of data analytics in handling the risks of fraud in government procurement era 4.0?. The purpose of this research is to reveal the application of data analytics in handling the risk of fraud in government procurement era 4.0.

2. LITERATURE REVIEW AND HYPOTHESIS

In the context of knowledge management, data analytics can be used to increase value hierarchically; from data to information, from information to knowledge, and from knowledge to wisdom. There are 3 (three) phases of data analytics in the context of knowledge management. The first phase is knowledge disclosure or increased use of explicit knowledge. The second phase is knowledge creation or increased use of experiential knowledge. And the third phase is knowledge application or increased use of collective knowledge (Wang, 2018). Data analytics can be used to support fraud risk management and fraud prevention and detection systems (Horsey, 2017).

In the context of auditing, data analytics has become an opportunity for internal auditors in line with the challenges in the digital era. The value of internal audit will be better by optimizing data analytics from big data that can be obtained from management. Data analytics enable internal auditors to focus their resources on high-risk transactions and provide management with a higher level of operational assurance (Anderson et al., 2017).

The results of data analytics in the audit can be in the form of audit insight and/or audit evidence. Auditors gain audit insight through the application of various statistical and visualization methods. There is no generic set of steps that can be applied to all conditions in the acquisition of audit insights. Auditors can use tracing techniques or repeating steps through iterations. Audit insights can be used to identify areas for follow-up audits. Meanwhile, the results of data analytics can be audit evidence with the auditor's professional considerations. The results of data analytics need to be validated with other audit evidence collected through substantive examinations and in accordance with the fulfillment of the requirements specified in the Auditing Standards (CAGI, 2017).

There are two data analytics techniques that can be used; statistical techniques and visualization techniques (CAGI, 2017) which can be applied to descriptive, diagnostic, predictive, and prescriptive analysis (principa.co, 2017). The application of data analytics techniques should be adapted to the purpose and type of analytics (Rajesh, 2016). Some of these analytical techniques are described in table 1.

Table 1. **Some Analytical Techniques According to the Purpose and Type of Data Analtics**

No.	Purpose of Analytics	Type of Analytics	Analytic technique
1	Data quality	Preparation for analytics	Data quality rules, data quality scores, statistical process control
2	What happened	Descriptive analytics	Basic profiling, data mining, descriptive statistic
3	Why and when it happened	Diagnostic analytics	correlation analysis, Control charts, analysis of variance, hypothesis tests, etc
4	How it happened	Cause analysis	Cause n effect analysis, failure mode effect analysis, etc
5	What will happen	Predictive analytics	Artificial neural network, regression analysis, etc
6	What/how can be developed	Prescriptive analytics	Design of experiments, simulations, scenario planning, etc.
7	How trust can be achieved	Reality based analytics	Failure analysis, confidence intervals, signal to noise ratios, etc.

Source : Processed Data (Rajesh, 2016)

The table reveals the techniques that need to be applied according to the purpose and type of analytics. For example, to find out "what happened, the type of analytics used is descriptive analytics with descriptive statistical technique. Meanwhile, to find out "what will happen", the type of analytics used is predictive analytics and several analytical techniques that can be used such as Artificial Neural Network (ANN), regression analysis, and others. In the context of procurement fraud risk, ANN can be used to predict the level of collusion in tenders. The results can be grouped into three categories: no collusion, there is an indication of collusion, and there is a strong indication of collusion (Anysz et al., 2019).

3. METHODS

This study uses a quantitative approach to secondary data through literature studies and exploration with data analytics techniques. Two data analytic techniques used are statistical techniques and visualization techniques (CAGI, 2017). The application of the two data analytics techniques can be done independently (statistical techniques or visualization techniques) or a combination of the two techniques. The research process is carried out using a data analytics process approach (figure 1) and analytical techniques that are in accordance with the type of data analytics (table 1).

The first is the formulation of questions or insights that will be sought through the application of data analytics, as described in the introduction. At this stage, a literature study is conducted to obtain data on the risk of procurement fraud in the 4.0 era and the risk attributes of tender conspiracy based on the KPPU's decision which will be used to handle this risk. The second is the acquisition of secondary data in the form of construction tender data at the provincial level in 2018 (LKPP, 2019). The third is cleaning and normalizing the data according to some specified attributes. This process uses Power Query MS Excel. The fourth is data analysis using Power Query MS excel and Query Power Business Intelligence or powerBI. The type of data analytics used is descriptive analytics with descriptive statistics and basic profiling techniques (Rajesh, 2016). The fifth is the communication of data analytics results which will be carried out through visualization in the form of a dashboard that displays insights obtained using powerBI.

Dashboards can be used to analyze project information needed in real-time, anytime, and anywhere (Utomo et al., 2015). Dashboards can also be used to support executive information systems (Ismubandono et al., 2019).

4. RESULTS AND DISCUSSION

Define Question and Obtain Data

There are seven risks of procurement fraud in the 4.0 era as described in table 2 (Kamal, 2020). Based on the research questions in the introductory section, the application of data analytics in handling procurement fraud risk is carried out on the highest level of procurement fraud risk. The risk is in the form of conspiracy with a score of 9.06.

If the fraud risk level is less than or equal to 4 (Kamal, 2020), the risk of conspiracy needs to be addressed through prevention to reduce the likelihood and detection to reduce the impact of the

Figure 1. **Process of Data Analytics**

Source: Anderson et al., 2017

risk. This means that data analytics also needs to be developed to detect the risk of conspiracy in provincial tender data. Data acquisition shows that the 2018 provincial tender data is 3,496 lines (figure 2).

Meanwhile, the results of the literature study show that there are at least 10 (ten) attributes that can be used to develop an indication of the risk of conspiracy in tenders, as follows:

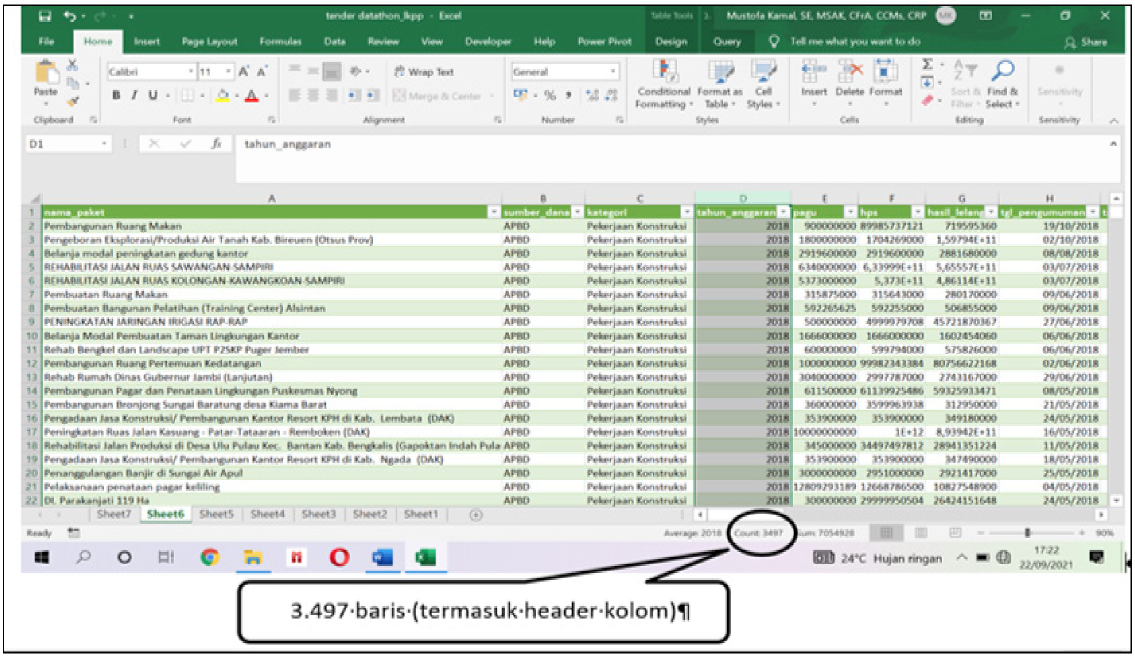
a. The last bidder to enter is declared the winner (OLAF, 2017)
b. Bid price is too high (Capobianco et al., 2017; Ferwerda et al., 2017) or the bid is approximately 98.50% of the self-estimated price (HPS) (Rachmania, 2020) or too low (OLAF, 2017).
c. Bid rotation between tender winners in several tenders (OLAF, 2017) or there is an association between several partners in several tenders (Anysz et al., 2019)
d. The percentage of partner success is very high (Capobianco et al., 2017) or repetition of winning tenders (Anysz et al., 2019) or the percentage of partners who win and lose (Vadász et al., 2016).

Figure 2. **Seven Risks of Procurement Fraud in the 4.0 Era**

No.	Description of Risk	Risk Level		
		Likelihood	*Impact*	Score
1	Conspiracy between providers in e-tendering/e-selection	2,76	3,29	9,06
2	Insider trading or conflict of interest in the form of working group/PPK/KPA/PA has a personal interest in one or several prospective providers of e-tendering/e-selection participants	2,69	3,36	9,04
3	Theft or leak of HPS details data for the benefit of prospective e-tendering/e-selection providers/participants	2,71	3,09	8,35
4	Misuse of ID user in e-tendering/e-selection	2,45	2,98	7,30
5	Manipulation of data or e-tendering/e-selection winners	2,37	3,06	7,27
6	Information accessed by unauthorized parties in e-tendering/e-selection	2,29	2,92	6,68
7	Cybercrime, piracy, hackers or vandalism in e-tendering/e-selection	1,97	2,74	5,41

Source: Kamal, 2020

Figure 3. **Screenshot of Tender Data 2018**



Source: Data Processed

e. There is a large gab or range between partners who win and lose (Capobianco et al., 2017) or the range of values between partners is 5% or less (Anysz et al., 2019) or the ratio of the bid value between the winner and the reserve (Vadász et al., 2016)
f. Single winner or partners who bid are few (Capobianco et al., 2017; Vadász et al., 2016) or the number of bidders is only 4 or less (Anysz et al., 2019).
g. Provider cluster distribution (Vadász et al., 2016)
h. Deviation of supply values from sector and regional averages (Vadász et al., 2016)
i. Distance between the partner's location and the project site (Anysz et al., 2019; Vadász et al., 2016)
j. Winner resigns (Vadász et al., 2016)

Clean and Normalize Data

Provincial tender data for 2018 is cleaned and normalized according to needs and searches for indications of tender conspiracy. If the tender data for 2018 is reviewed with the attribute of conspiracy risk, it is revealed that there are 8 (eight) attributes that cannot be used for data analysis, because:

a. The data only reveals the winner of the tender. This has the consequence that 6 (six) conspiracy risk attributes cannot be disclosed, such as;
    a. The last bidder to enter is declared the winner
    b. Rotation and/or association between partners in several tenders
    c. Percentage of partner's success in winning the tender
    d. The Range of partners' bidding values or the ratio of winning bidders to reserves
    e. Provider cluster
    f. Winner resigns
b. There is no sectoral and/or regional data. This has the consequence that the attribute in the form of deviation of the winning partner from the sectoral and/or regional average cannot be disclosed.
c. The partner's address is incomplete so it cannot calculate the distance between the partner's location and the project site

There are two attributes that can be used: a high bid price and a small number of partners who make bids. Data on past law enforcement experience can be used to develop these two attributes (Capobianco et al., 2017). The author develops the attributes of a high price and a small number of bidders from the decision of the Business Competition Supervisory Commission (KPPU) trial (KPPU, 2018) regarding the crime of conspiracy in tenders (Appendix 1).

The table reveals two attributes of the conspiracy: the price is equal to or above 96.30% of the self-estimated price (HPS) and the number of partners is equal to or below five. These results can be further developed as an indication of the risk of conspiracy (Table 2) which will be applied for the purposes of cleaning and normalizing data in the analysis of tender data 2018.

Cleaning and normalization of data according to the risk attributes result in 12 columns and 2,678 rows of data which are continued in data analysis (Table 3).

Table 2. **Two Attributes of Conspiracy Risk**

Conspiracy Risk	Indication of Conspiracy Risk
Bid price is too high (Capobianco et al., 2017; Ferwerda et al., 2017; Rachmania, 2020)	Bid price ≥ 96.3% HPS and HPS ≥ 96.3% Budget Ceiling
The small number of partners who bid (Capobianco et al., 2017; Vadász et al., 2016)	Number of bidders ≤ 5 partners

Source: Data Processed

Table 3. **Cleaning and Normalization of Data According to Conspiracy Attributes**

Step Description	Column	Row
Tender data 2018	20	3,496
Cleaning of columns and rows that cannot be continued in analysis	(8)	(818)
Analyzed tender data 2018	12	2,678

Source: Data Processed

Table 4. **Descriptive Statistics of the Two Conspiracy Attributes Using MS Excel**

Description	Number of Participants	HPS	Offer/HPS
Mean	44,70463032	0,988502962	0,932473201
Standard Error	0,657204117	0,00109023	0,001394896
Median	33	1,0000	0,9625
Mode	127	1,0000	0,9500
Standard Deviation	34,00991617	0,056418756	0,072185013
Sample Variance	1156,674398	0,003183076	0,005210676
Kurtosis	-0,12538864	66,12918616	7,582858501
Skewness	0,957172541	-7,67898417	-1,917912845
Range	125	0,668002278	0,900126765
Minimum	2	0,331997722	0,099873235
Maximum	127	1,0000	1,0000
Sum	119719	2647,210932	2497,163232
Count	2678	2678	2678
Largest(1)	127	1,0000	1,0000
Smallest(1)	2	0,331997722	0,099873235
Confidence Level (95,0%)	1,288679051	0,002137779	0,002735182

Source: Data Processed

Analyzing the Data and Understanding the Results

Data analysis begins with descriptive analytics on 2,678 provincial tender data in 2018 using descriptive statistics with Microsoft Excel 2019 (Table 4). This table shows a description of the conspiracy attributes. The number of participants indicates that the average bidder is 44.7 or 45 (rounded off) or more than 5 partners. This means that the average or mean tender does not reflect the presence of an indication of the risk of conspiracy in the aspect of the number of bidders. However, if the data shows the minimum number, namely 2 participants, it means that there is an indication of the risk of conspiracy among the 2,768 tender data. This condition requires further analysis.

There are two indications of the high price attribute: a high self-estimate price (HPS) and a high bid. Table 4 shows an average self-estimate price (HPS) of 0.989 or exceeding 0.963, which means that the average tender indicates a high HPS. In fact, the median shows the number 1 which means that the "mean value of 2,678 data tenders" is more than 50% with high HPS.

The bid attribute shows an average bid of 0.932 or close to 0.963 which means that it is close to an indication of a high bid price. In fact, if viewed from the median value of 0.963, this shows that there is an "indication of high bid prices in 2,678 tender data" or close to 50%. This condition needs to be studied in more detail.

The next data analysis is carried out by applying the indications of the risk of conspiracy (Table 4) in 2,678 tender data 2018. The analysis is carried out using a powerBI query through the "add conditional column" menu (Appendix 2).

The results of this analysis are used to fill in the dashboard menu of the risk of tender conspiracy.

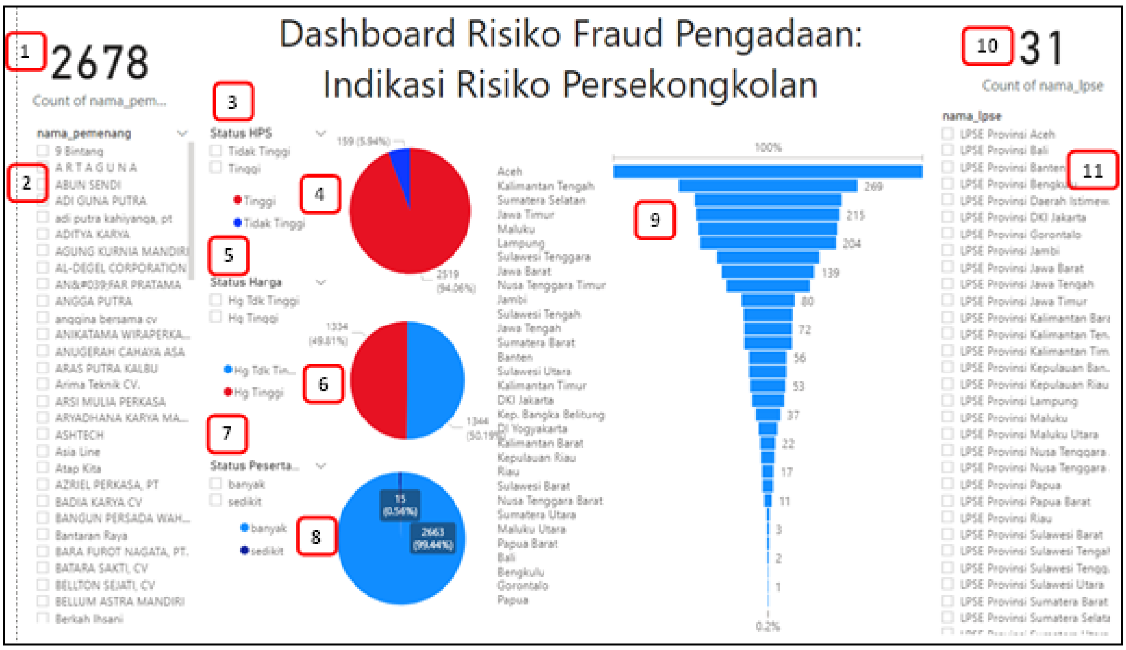
Communicate the Results

Insights can be communicated through the interactive display of the procurement fraud risk dashboard (Figure 4). The results show that the procurement fraud risk dashboard can display an indication of the risk of conspiracy. Search for information or insight can be done interactively through the use of several slicer menus according to the need for detection of indications of conspiracy risk.

Some information can be revealed on the dashboard through the use of several menus. The explanation of the menu is as follows:

1. The "card" menu for the number of data displays the number of data, as many as 2,678 rows, which is a reflection of the number of tenders
2. The "slicer" menu for the winner's name displays the names of partners and becomes a filtering tool according to the name of the partner whose insight will be sought.
3. The "slicer" menu for the HPS status displays "high" or "not high" HPS and can be used as filtering tools
4. The "pie chart" menu for HPS displays data on the number and percentage of high and not high HPS. This menu will follow the interactions performed on the selected or clicked slicer.
5. The "slicer" menu for the price status displays the high or not high bid price and can be used as filtering tools.
6. The "pie chart" menu for prices displays data on the number and percentage of high and not high bid prices. This menu will follow the interactions performed on the selected or clicked slicer.
7. The "slicer" menu for the status of the number of bidders displays the number of partners participating in the tender and can be used as a filtering tool to gain insight into the number of participants (few or many).
8. The "piechart" menu for the number of tender participants displays data on the number and percentage of tender participants (few or many). This menu

Figure 4. **Procurement Fraud Risk Dashboard Using Power BI**



Source: Data Processed

will follow the interactions performed on the selected or clicked slicer.

9. The "funnel" menu for the number of winners in each province
10. The "card" menu for the provincial LPSE displays the provincial LPSE as a result of data cleansing, consisting of 31 provincial LPSEs.
11. The "slicer" menu for the name of the provincial LPSE displays the names of the provincial LPSE and becomes a filtering tool according to the province whose insight will be sought.

An example of using the menu is as follows: if the high HPS slicer is selected, the dashboard shows the insight that there are 2,519 tenders (or 94.06% of the total tenders) in 31 LPSEs (or 100%) which indicate the risk of conspiracy (Table 5). Search and other insights communication can be developed as needed.

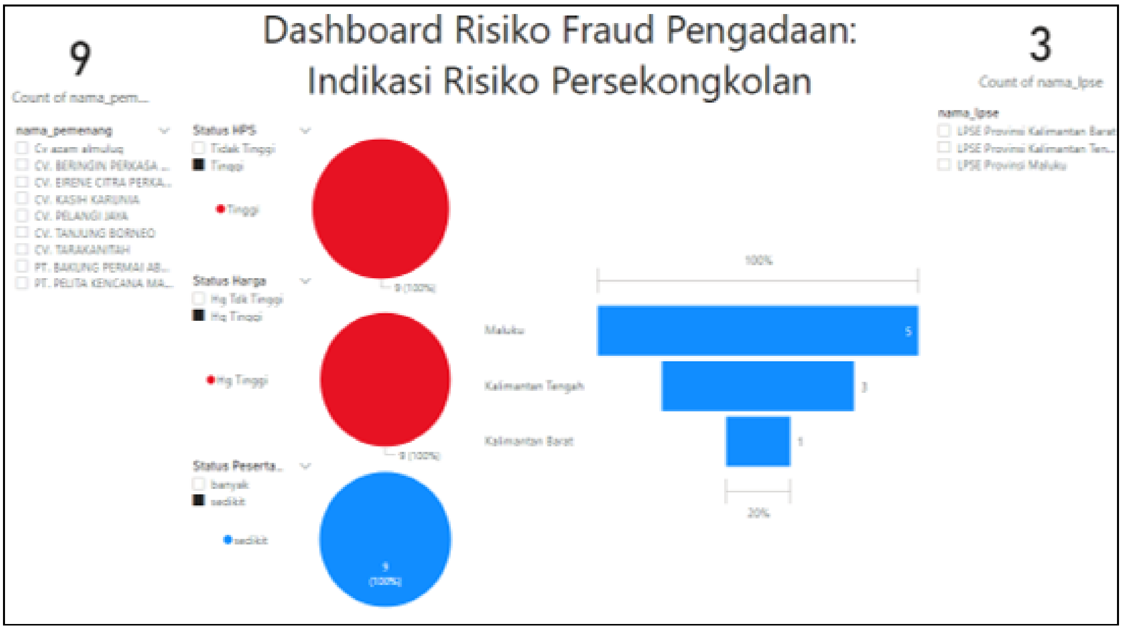
If the selected slicer is a combination of high HPS, high price, and few participants, then the dashboard displays 9 tenders in 3 provinces indicating the risk of tender conspiracy (Figure 5). The three provinces are Maluku, Central Kalimantan and West Kalimantan. This conspiracy risk insight can be used for more detailed research or audits.

Table 5. **Indication of Conspiracy Risk through the Use of Dashboard**

Indikasi Risiko Persekongkolan	Tender		LPSE Provinsi	
	Jumlah	%	Jumlah	%
Data tender provinsi tahun 2018	2.678		31	
Penggunaan menu slicer di dashboard:				
HPS tinggi	2.519	94,06	31	100,0
Harga penawaran tinggi	1.334	49,81	28	90,32
Gabungan HPS dan harga penawaran tinggi	1.257	46,94	27	87,10
Peserta Tender Sedikit	15	0,56	5	16,13
Gabungan HPS dan harga penawaran tinggi serta peserta tender sedikit	9	0,34	3	9,68

Source: Data Processed

Figure 5. **Analysis of the Combined Indications of Conspiracy Risk**



Source: Data Processed

The visualization technique through the dashboard of the three provinces can reveal some insights into the indications of the risk of conspiracy. The highest indication of conspiracy risk based on a combination of price indications is in LPSE Central Kalimantan Province, 75.84% (table 6). Meanwhile, for a combination of price indications and the number of tender participants, the highest indication of conspiracy risk is in West Kalimantan LPSE, 4.55%. This condition provides insight that indications of the risk of conspiracy in the form of high prices need more attention from management and or auditors because they are high risk.

Based on previous research, the likelihood level of conspiracy risk is 2.98 or sometimes occurs (Kamal, 2020), so that the likelihood level of the risk of conspiracy with an indication of "high prices" in the three provinces changes to 5 or almost certain to occur. The probability of the occurrence of the risk exceeding 50% in 1 period, with details as follows:

a. Central Kalimantan Province by 75.84%
b. West Kalimantan Province by 68.18%
c. Maluku Province by 51.20%.

Table 8. **Analysis of Conspiracy Risk in 3 Provinces**

Indication of Conspiracy Risk	Tender		Provincial LPSE
	Number	%	
Provincial tender data for 2018	209		Maluku
Using the slicer menu on the dashboard:			
High Self-Estimate Pirce (HPS)	157	75,12	
High bidding price	154	73,68	
Combined HPS and high bidding price	107	51,20	
Few Tender Participants	7	3,35	
Combined HPS, high bidding price, and few tender participants	5	2,39	
Provincial tender data for 2018	269		Central Kalimantan
Using the slicer menu on the dashboard:			
High Self-Estimate Pirce (HPS)	266	98,88	
High bidding price	206	76,58	
Combined HPS and high bidding pricei	204	75,84	
Few Tender Participantst	4	1,49	
Combined HPS, high bidding price, and few tender participantsit	3	1,12	
Provincial tender data for 2018	22		West Kalimantan
Using the slicer menu on the dashboard:			
High Self-Estimate Pirce (HPS)	22	100,00	
High bidding price	15	68,18	
Combined HPS and high bidding price	15	68,18	
Few Tender Participants	2	9,09	
Combined HPS, high bidding price, and few tender participants	1	4,55	

Source: Data Processed

5. CONCLUSION

Management and auditors need to transform digitally in handling the risk of procurement fraud in the 4.0 era. Data analytics can be applied in detecting the risk of conspiracy in tenders. The data analytics process can be designed by determining the insight to be sought, compiling attributes of the risk of conspiracy, analyzing data using statistical techniques in the form of descriptive statistics, visualization and communication techniques through the procurement fraud risk dashboard.

The results show that descriptive statistical techniques reveal the mean and median values of the conspiracy risk attribute above 50%. Meanwhile, visualization techniques can show insight through the use of interactive menus on the conspiracy risk dashboard. The dashboard shows that there are 3 provinces that meet the indications of conspiracy risk. The analysis of the three provinces shows that the likelihood level of conspiracy risk can be revised from 2.98 (sometimes occurs) to 5 (almost certain to occur). This shows that data analytics can be used to detect the risk of conspiracy in tenders and to update the likelihood level of conspiracy risk..

This research implies that management and auditors need to develop a data analytics framework in the performance of procurement fraud risk detection. Management and auditors need to improve performance evidence by instilling "let's data talks".

There are several limitations in this study, among others, the attributes of the risk of conspiracy are not fully applied and the research object data used also does not reveal all bidders, both winners and losers.

REFERENCES

Anderson, U. L., Head, M. J., Ramamoorti, S., Riddle, C., Salamasick, M., & Sobel, P. J. (2017). *Internal Auditing: Assurance & Advisory Services* (Fourth Edi). The Internal Audit Foundation, 1035 Greenwood Blvd., Suite 401.

Anysz, H., Foremny, A., & Kulejewski, J. (2019). Comparison of ANN Classifier to the Neuro-Fuzzy System for Collusion Detection in the Tender Procedures of Road Construction Sector. *IOP Conference Series: Materials Science and Engineering*, *471*(11). https://doi.org/10.1088/1757-899X/471/11/112064

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and Analytics in the Modern Audit Engagement: Research Needs. *Auditing*, *36*(4), 1–27. https://doi.org/10.2308/ajpt-51684

Asad, A. F., Tarjo, & Musyarofah, S. (2019). Reorientasi Audit Internal Untuk Melawan Korupsi Pengadaan. *Jurnal Akuntansi Multiparadigma*, *10*(3), 583–601.

Baesens, B., Vlasselaer, V. Van, & Verbeke, W. (2015). *Fraud Analytics using descriptive, predictive, social network techniques; A Guide to Data Science for Fraud Detection*. John Wiley & Sons, Inc.

Bagas, S. A. (2018). *Implementasi Data Analytics Dalam Audit Laporan Keuangan sebagai Dampak dari Perkembangan Teknologi* [Universitas Brawijaya]. repository.ub.ac.id

Banarescu, A. (2015). Detecting and Preventing Fraud with Data Analytics. *Procedia Economics and Finance*, *32*, 1827 – 1836.

CAGI. (2017). *Guidelines on Data Analytics* (First Edit). Office of the Comptroller and Auditor General of India.

Capobianco, A., Gonzaga, P., & Nyeső, A. (2017). *Algorithms and Collusion - Background Note by the Secretariat*. the OECD Competition Division. http://www.oecd.org/daf/competition/algorithms-and-collusion.html.

Ferwerda, J., Deleanu, I., & Unger, B. (2017). Corruption in Public Procurement: Finding the Right Indicators. *European Journal on Criminal Policy and Research*, *23*(2). https://doi.org/10.1007/s10610-016-9312-3

Gee, S. (2015). *Fraud and Fraud Detection_A Data Analytics Approach*. John Wiley & Sons, Inc.

Horsey, L. L. (2017). Data Analytics for Fraud Prevention and Detection in State Government. *ProQuest*.

IIA. (2017). *Data Analytics; Is it time to take the first step?*

Ismubandono, R. A. F., Putra, N. W. H., & Pramono, D. (2019). Analisis dan Perancangan Sistem Informasi Eksekutif Dashboard Data E-Government berbasis Service pada Pemerintah Kabupaten Sidoarjo. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(11), 10788–10796. http://j-ptiik.ub.ac.id

Kamal, M. (2020). *Peran Aparat Pengawasan Intern Pemerintah (APIP) dalam Manajemen Risiko Fraud Pengadaan era 4.0* (Makalah Lomba Karya Tulis Ilmiah HUT BPKP 2020). Tidak Dipublikasikan

KPPU. (2018). *P U T U S A N Perkara Nomor 21/KPPU-I/2018*.

LKPP. (2019). *Datathon LKPP* (Kulik Data Tender). Tidak Dipublikasikan

Mirarab, A., Mirtaheri, S. L., & Asghari, S. A. (2019). Value Creation with Big Data Analytics for Enterprises: a survey. *TELKOMNIKA*, *17*(6), 2790~2802.

Mohamed, I. S., Muhayyidin, N. H. M., & Rozzani, N. (2019). Auditing and Data Analytics Via Computer Assisted Audit Techniques (CAATS): Determinants of Adoption Intention Among Auditors in Malaysia. *Proceedings of the 3rd International Conference on Big Data and Internet of Things (BDIOT 2019). Association for Computing Machinery, New York, NY, USA,* 35–40. https://doi.org/10.1145/3361758.33617732019.

Oktorialdi. (2019). Arah Kebijakan Strategi National Transformasi Digital. *Seminar Standarization in a Living Concept Society 5.0*.

OLAF. (2017). *Fraud in Public Procurement A collection of Red Flags and Best Practices*.

Panuntun, D. J. S. (2020). Auditor Internal Pemerintah Di Era Digital. *Jurnal Pengawasan*, *2*(1), 1-7.

principa.co. (2017). *The 4 types of data analytics*. www.Principa.Co.Za. https://insights.principa.co.za/4-types-of-data-analytics-descriptive-diagnostic-predictive-prescriptive

Rachmania, S. N. (2020). Kesalahan Penyusunan Harga Perkiraan Sendiri (HPS) dalam Pengadaan Barang/Jasa Pemerintah Yang Berimplikasi Tindak Pidana. *Jurist-Diction, 3*(3), 1123–1152. https://doi.org/10.20473/jd.v3i3.18641.

Rajesh, J. (2016). Importance of Data Quality for Analytics. *Springer International Publishing Switzerland*. DOI 10.1007/978-3-319-21332-3_2

Telkom University. (2020). *Bahan Ajar Sertifikasi Big Data Analitik*.

Utomo, P., Setiawan, & Prayitno, W. F. (2015). Perancangan Dashboard Sistem Informasi Untuk Agile Manajemen Proyek d engan Menggunakan JIRA Studi Kasus d i P T . F LASH i Z Indonesia. *JURNAL SISFOTEK GLOBAL*, *5*(2), 17-24.

Vadász, P., Benczúr, A., Füzesi, G., & Munk, S. (2016). Identifying Illegal Cartel Activities from Open Sources. In B. Akhgar, P. S. Bayerl, & F. Sampson (Eds.), *Open Source Intelligence Investigation; From Strategy to Implementation* (pp. 251–274). Springer International Publishing AG 2016.

Wang, C. (2018). Integrating Data Analytics & Knowledge Management: A Conceptual Model. *Issues in Information Systems*, *19*(2), 208–216.

Appendix 1. **Pengembangan Indikasi Atribut Risiko Persekongkolan Tender Berdasarkan Putusan Nomor Perkara Nomor 21/ KPPU-I/2018)**

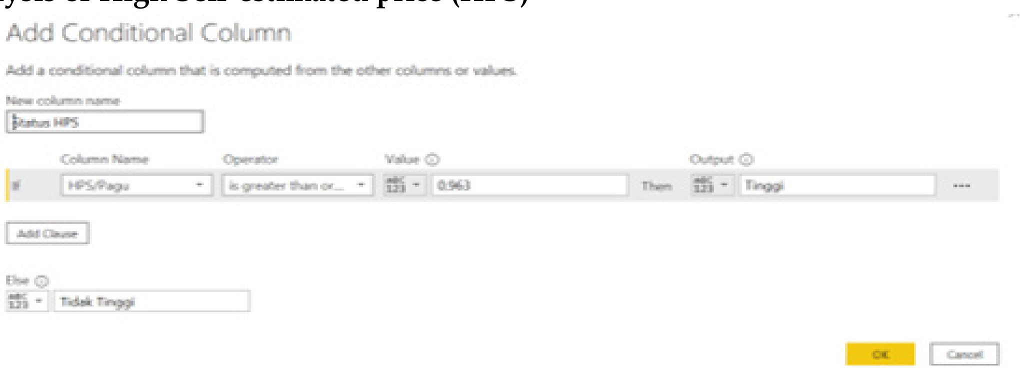
Perusahaan yang bersekongkol	Sumber dana	Tahun	Nama Pekerjaan	kode lelang	HPS	Penawaran	Penawaran/ HPS	Range peserta dengan pemenang	status
PT Jatisono Multi Kontruksi	APBD	2016	Peningkatan Jalan	583207	93.898.715.000	79.763.952.000	0,849	-0,144	peserta tender
PT Anugerah Karya Agra Sentosa	APBD	2016	Peningkatan Jalan	583207	93.898.715.000	88.712.454.000	0,945	-0,048	peserta tender
PT Kediri Putra & PT Triple S Indosedulur, KSO	APBD	2016	Peningkatan Jalan	583207	93.898.715.000	93.250.511.000	0,993	0,000	pemenang tender
PT Ratna	APBD	2016	Peningkatan Jalan	583207	93.898.715.000	93.603.266.000	0,997	0,004	peserta tender
PT Ayem Mulya Indah	APBD	2016	Peningkatan Jalan	583207	93.898.715.000	93.671.117.000	0,998	0,004	peserta tender
atribut persekongkolan berdasarkan fakta putusan					rata-rata		0,956	-0,037	
PT Jatisono Multi Kontruksi	APBD	2016	Pembangunan Jalan	584207	93.740.277.000	79.645.934.000	0,850	-0,143	peserta tender
PT Anugerah Karya Agra Sentosa	APBD	2016	Pembangunan Jalan	584207	93.740.277.000	95.093.768.000	1,014	0,021	peserta tender
PT Kediri Putra & PT Triple S Indosedulur, KSO	APBD	2016	Pembangunan Jalan	584207	93.740.277.000	92.999.148.000	0,992	-0,001	pemenang tender
PT Ratna	APBD	2016	Pembangunan Jalan	584207	93.740.277.000	93.442.383.000	0,997	0,004	peserta tender
PT Ayem Mulya Indah	APBD	2016	Pembangunan Jalan	584207	93.740.277.000	93.442.383.000	0,997	0,004	peserta tender
atribut persekongkolan berdasarkan fakta putusan					rata-rata		0,970	-0,023	
rata-rata atribut persekongkolan tender berupa harga tinggi berdasarkan pengalaman putusan KPPU							0,963	-0,030	
Jumlah rekanan yang bersekongkol= 5 rekanan									

Source: Data Processed

Appendix 2. **Analysis of Conspiracy Risk Indications Using Power BI**

Analysis of Few Tender Participants

Analysis of High Self-estimated price (HPS)



Analysis of High Bid Price