

## The Impact of Cyber Security Governance on the Efficiency of Big Data Implementation in Jordanian Commercial Banks, A Field Study

Jamal Hassan Al-Afeef

Faculty of Economics & Administrative Sciences

Jerash University

Jerash, Jordan.

### Abstract

*The study aimed to demonstrate the impact of cybersecurity governance on the efficiency of big data implementation in Jordanian commercial banks. The study population consisted of the 13 commercial banks operating in Jordan. (89) questionnaires were distributed to the commercial bank branches of the study sample, from which the researcher retrieved ( 70) Questionnaire, After reviewing the retrieved questionnaires, it was found that there are (3) questionnaires that are not valid for statistical analysis, so the number of valid questionnaires for analysis reached (67) questionnaires. The study relied on the (VIF) test to ensure that there is no problem of multiple linear relationships (multiple correlation), because it is considered One of the problems facing the statistical estimation of regression coefficients. The study reached many results, the most important of which was that there is an impact of cybersecurity governance on the efficiency of big data implementation in Jordanian commercial banks, represented by (cybersecurity governance requirements ,cybersecurity program, cybersecurity policy, cyber information security management, assessment and management of cyber risks) on big data implementation in commercial banks in Jordan. "As for the most important recommendations of the study, it crystallizes in the need of the Jordanian commercial banks' departments for paying attention to restructuring their organizational structure in a way that supports the flow of data between the different departments through ways of creating solid cyber governance that has its own inputs which is related to big data technologies.*

**Key words:** Cyber Security Governance: Big Data: Jordanian Commercial Banks

### 1. Introduction:

Information plays great importance in developed societies worldwide in all its different fields of use, and because of its role in achieving human and technological progress as well, based on the above; Information systems have been invented for their superior ability to provide accurate, structured and valuable information that meets the needs in the best possible way, and it also facilitates the process of updating and changing data. Despite the importance of big data in many aspects of accounting and auditing work; However, bank management has little awareness of the importance of analyzing big data, which may affect the administration's assistance to achieve its goals. Analyzing big data is also one of the most important aspects that banks need in order to develop their role in serving the administration due to the challenges that banks face in the contemporary business environment, where banks need to identify best practices and provide a base for them that clarifies the opportunities, challenges and changes that big data can cause in accounting when starting the implementation process.

Here comes the role of the existence of correct governance applied in these banks, which is represented here by cyber security governance, which has an impact on improving accounting performance with its direct impact on the efficiency of implementation of "Big Data" technology in commercial banks.

Hence, this study worked on knowing the impact of cybersecurity governance on the efficiency of big data implementation in Jordanian commercial banks

### 2. Objectives of the study:

- 1- Recognizing the intellectual concept of cybersecurity governance and its importance for Jordanian commercial banks
- 2- Recognizing the intellectual concept of big data and its real components
- 3- identifying the real impact of cybersecurity governance on the efficiency of big data implementation in Jordanian commercial banks.

### 3. Problem of the study:

The main and subsidiary study problem is as follows:

The main problem:

Is there an impact of cybersecurity governance on the efficiency of big data implementation in Jordanian commercial banks, the following sub-problems are branched out of it:

The first sub problem:

Is there an impact of cybersecurity governance represented by cybersecurity governance requirements on the efficiency of big data implementation in Jordanian commercial banks?

The second sub-problem:

Is there an impact of cybersecurity governance represented by the cybersecurity program on the efficiency of big data implementation in Jordanian commercial banks?

The third sub-problem:

Is there an impact of cybersecurity governance represented by the cybersecurity policy on the efficiency of implementing big data in Jordanian commercial banks?

The fourth sub-problem:

Is there an impact of cybersecurity governance represented by cyber information security management on the efficiency of big data implementation in Jordanian commercial banks?

The fifth sub-problem:

Is there an impact of cybersecurity governance represented in assessment and management of cyber risks on the efficiency of big data implementation in Jordanian commercial banks

### 4. Study hypotheses:

Based on the questions of the main and sub problem, the hypotheses of the study revolve around the following:  
The main hypothesis:

There is no impact of cybersecurity governance on the efficiency of big data implementation in Jordanian commercial banks, the following sub-hypotheses are branched out of it:

The first sub-hypothesis:

There is no impact of cybersecurity governance represented by cybersecurity governance requirements on the efficiency of big data implementation in Jordanian commercial banks

The second sub- hypothesis:

There is no impact of cybersecurity governance represented by the cybersecurity program on the efficiency of big data implementation in Jordanian commercial banks

The third sub- hypothesis:

There is no impact of cybersecurity governance represented by the cybersecurity policy on the efficiency of implementing big data in Jordanian commercial banks

The fourth sub- hypothesis:

There is no impact of cybersecurity governance represented by cyber information security management on the efficiency of big data implementation in Jordanian commercial banks

The fifth sub- hypothesis:

There is no impact of cybersecurity governance represented in assessment and management of cyber risks on the efficiency of big data implementation in Jordanian commercial banks.

### 5. The Theoretical side of the study:

The concept of cyber security governance.

Some researchers believe that the concept of cyber-governance revolves around the data of electronic governance in companies and banks, so we find that (Saleh and Al-Salehi, 2018) defined it as a set of mechanisms that include drawing the strategic direction of the organization, to control the variables of its internal environment, meet its requirements and prepare to face the variables of its external environment and adapt to it.

But (Al-Harmzi, 2019) defined it as the exercise of economic, political and administrative power to manage state affairs at all levels through the use of information and communication technology to increase access to government services and spread them across the network in order to benefit individuals, private business owners, and workers

Finally, we find (Al-Saeed, 2019) believes that what is meant by governance in the context of cybersecurity is that it is the principles, administrative rules and methods used in an entity to control decision-making powers and identify those with responsibility and accountability in carrying out the tasks and duties related to protecting the entity from cyber attacks or misuse of information assets, with ensuring the continuity of operations in the event of accidents or disasters. Accordingly, the cybersecurity governance aims to direct, monitor, guide and improve the decisions and actions of individuals to raise efficiency and facilitate coordination of efforts between the relevant authorities, in line with the direction and aspirations of the stakeholders in the entity (internal factors), and in a manner that does not contradict the agreements and laws to which the entity is a party in (external factors).

Factors for the success of cybersecurity governance in banks:

In order to control the governance of cybersecurity and enhance responsibilities within banks, the information technology function must be separated from the cybersecurity function, and this separation is not for administrative luxury, but rather is a general trend to enhance governance, transparency and accountability practices within banks. The goal of separating the two functions is the regulatory framework for cybersecurity issued by the Monetary Agency, where it demanded that the Cybersecurity Department follow an administrative path that differs from the Department of Information Technology and that it be one of the tasks of the control function in the entity. The second condition is what distinguishes the regulatory framework of the Monetary Agency compared to the controls of the Cybersecurity Authority, for its implicit statement that cybersecurity is a comprehensive program for the entity's work, affecting and influencing various initiatives and projects even if they are not related to information technology, and equating it with the responsibilities of other disciplinary functions such as management Risks or legal management in the entity. If we assume that the cybersecurity management follows one of the planning functions or the administrative functions (Directing Function), then - in theory - the cybersecurity requirements can be integrated into one or several different stages of the entity's work without a control point that verifies the requirements in the required form before launching or ending projects. Practically, this gap can be bridged through the official and explicit assignment of the controlling responsibility to the requirements of cybersecurity (as a responsibility and not a full function) for one of these non-controlling functions, and for the success of this method, substantial support must be provided from the decision-makers in the entity with a periodic review and evaluation of the efficiency and effectiveness of this assignment. (Al-Saeed 2019)

The importance of cybersecurity governance for banks:

One of the most important reasons for the necessity of having a cybersecurity governance concept and calling for creating legislative and regulatory frameworks that commensurate with the challenges faced by society or organizations and banks

It can be summarized as follows: (Abd Al-Reda and Al-Mamouri, 2020)

1- The need to be linked to communication systems and the Internet, and the inability to isolate devices from the local and wide-area networks they need

2- The reliance of various institutions and banks on the effectiveness of information, which increases with the increase in technological developments and with the increase in the requirements of these institutions and banks.

3- The difficulty of challenging and controlling dangers or following criminals and punishing them, due to the lack of geographical borders when using the Internet and electronic communications because they provide an opportunity to penetrate spatial borders.

4- The steady growth in electronic uses and applications, and the emergence of electronic commerce, network shopping, e-government and electronic management, which need a safe information environment.

5- The relationship between security and technology has become a direct one with the possibility of exposing strategic interests of a cyber nature to electronic dangers and rethinking the concept of national security, which means protecting the basic values of society, and then it is a new tributary to national security.

6- Cybersecurity is concerned with the process of developing standards and procedures to prevent non-peaceful uses of cybersecurity and the threats it poses to global security and the information infrastructure. Therefore, state security has become part of collective security.

7- The issue of cybersecurity has become an international issue that requires flexible strategies that adapt to continuous changes, whether in security mechanisms or tactics, in exchange for the continuous development of threats.

8- The interest in cybersecurity was not limited to the technical dimension only, but went beyond to other dimensions that have become relevant in explaining the issue, such as the cultural, social, economic and military dimensions.

9 - The role of non-state actors in international relations has increased, which in turn affected the sovereignty of the state, especially with the emergence of technology companies crossing borders.

## **5.1 The concept of big data**

The definition of big data is broad and varies by industry and user. In addition, continuous technological development is affecting big data visualization (Gupta and Gunasekaran, 2020). Big data can be defined as the collection, storage and analysis of huge amounts of data, and it is fast data; Collected, transported, and processed immediately (ACCA & IMA, 2013).

The term "Big Data" is considered relatively recent, as it has caught the attention of the world, international organizations, companies and researchers due to its social and economic importance. Researchers have endeavored to define a concept of big data, as it was defined before (Fan & Bifet, 2013) as a group of large-sized data that cannot be analyzed with traditional instruments due to its large size and complexity.

While the International Organization for Standardization (ISO, 2017) defined it as a set of data that cannot be efficiently processed using traditional technology to achieve benefit from it, and it has several characteristics, including size, speed, diversity, variance and reliability.

(Gamage, 2016) shows that it is possible to exploit big data and its analyzes in the accounting profession through the use of predictive models and other sources to improve budget, control and risk management, and to improve internal audit activities and its quality by analyzing an integrated set of data with artificial intelligence instruments.

Looking at the previous definitions, the researcher can conclude that big data is generated quickly and in a large volume, and that the increase in this data has created challenges for companies because of the inability of traditional instruments to work with them. Thus, it can be defined as data of large size that comes from different sources, and it cannot be managed by traditional instruments, and it needs to be dealt with through advanced technologies and instruments to create new horizons for companies.

### Sources of Big Data

#### The importance of big data analysis

The importance of big data analysis is as follows (Gartner, 2014) (Marijn, et.al, 2017).

- ❖ Analyzing big data helps in increasing the quantity, quality and speed of information, thus improving the decision-making process and making the most appropriate decision.
- ❖ Helps companies detect fraud and theft through fraudulent purchases.
- ❖ It helps in reducing costs, increasing productivity and increasing profits, thus improving financial performance and accelerating growth.
- ❖ Analyzing big data helps to understand customer behavior better, and work to improve and develop services provided to customers.
- ❖ Analyzing social media data gives you the ability to know what people are talking about concerning the organization and thus discover untapped opportunities and potential weaknesses, based on the results of data analysis.
- ❖ It provides a high competitive advantage for companies, by anticipating the future in a better way, as managers can exploit this data by identifying new opportunities and expanding their own course of work (Tesfaye, 2017).

## **5.2 Characteristics of Big Data**

Big data has different characteristics from traditional data, and (Daniel, 2018) pointed out that there are a set of characteristics that big data possess, which are as follows:

- 1- Variety: The collection of large samples in big data is usually from multiple sources at different points in time using different techniques. Confirm that the data is more than the traditional digital accounting data, this would help researchers and analysts choose the appropriate data for their field
- 2- Value: It is one of the most important characteristics as it indicates the extent to which this data contributes to generating insights and benefits of economic value and contributes to making the right decision in a timely manner, and better the understanding the requirements of its customers or the market.
- 3- Veracity: This characteristic indicates the extent to which big data can be relied upon in terms of reliability, and the quality of data that comes from various sources in order to aid in decision-making (Singh et..al. 2015

- 4- Velocity: It means the speed of production and generation of new data that is faster than the speed of traditional data production.
- 5- Volume: it refers to the large volume of data that consumes large storage capacity or consists of many records that exceed the ability of traditional systems to store them, which also produce a large amount of information after its analysis. (Bin Al-Tayeb, Al-Raiyi, 2019).

### **5.3 The intellectual relationship between cyber governance and big data:**

The prevailing culture of cybersecurity in the vestibules of the entity is affected by the style of governance followed by its higher management, whether this is documented in its systems, policies and regulations or practiced without documentation. This requires that the method of cybersecurity governance and management is consistent with the direction and culture of the entity, And the level of administrative and technical maturity. When designing a cybersecurity governance program, three main levels must be considered: First, the responsibility for defining the security vision and priorities, and this task is often assigned to the Cybersecurity Supervisory Committee. Second, the responsibility for defining the programs and implementation mechanisms is assigned to the director of cybersecurity in the entity and his work team. Third, the responsibility for implementing and following up the initiatives and programs is assigned to the various departments and divisions in the entity each according to his job duties and role in achieving the general vision of cybersecurity (Al-Saeed, 2019).

Banks may particularly rely on modern technologies to accomplish their banking business, and among these technologies is the big data that needs advanced cyber governance to deal with it because big data plays a role in improving the accounting performance in the bank. It is one of the most important future technological fields, and it receives more attention from the world, especially banks, due to its huge potential to provide added value to the bank, and it also provides information to decision-makers, preparing reports and monitoring banks' performance (Raguseo.2018Boomer.2018; Gamage.2016;).

This data is characterized by characteristics of huge quantities and speeds and types with different structures, which distinguish it from data derived from traditional sources. Big data comes from various sources such as the Internet, social media, sensors and smart phones, and it needs modern analytical techniques when processing it, Where traditional analytical instruments cannot handle it (Qantqji, 2014). This drives the existence of high-class cybersecurity governance to control the mechanism of action for big data.

## **6. The practical side of the study:**

### **6.1 Study Population and Sample:**

The study population consisted of the 13 commercial banks operating in Jordan. (89) questionnaires were distributed to the commercial bank branches of the study sample, from which the researcher retrieved ( 70) Questionnaire, After reviewing the retrieved questionnaires, it was found that there are (3) questionnaires that are not valid for statistical analysis, so the number of valid questionnaires for analysis reached (67) questionnaires.

### **6.2 Characteristics of the study sample:**

Table No. (1) shows the demographic characteristics of the individuals responding to the questionnaire questions, which are made up of scientific qualification, scientific specialization, professional certificates and years of practical experience, i.e. the distribution of the study sample according to its variables, as follows:

Table No. (1)  
Distribution of the sample members according to demographic characteristics

<b>Variable</b>	<b>level</b>	<b>repeats</b>	<b>percentage</b>
<b>scientific qualification</b>	<b>Intermediate diploma</b>	<b>46</b>	<b>68.7</b>
	<b>BSc</b>	<b>12</b>	<b>17.9</b>
	<b>MSc</b>	<b>5</b>	<b>7.5</b>
	<b>PhD</b>	<b>2</b>	<b>3.0</b>
	<b>Missing values</b>	<b>2</b>	<b>3.0</b>
	<b>Total</b>	<b>67</b>	<b>100.0</b>
<b>scientific specialization</b>	<b>Accounting</b>	<b>35</b>	<b>52.2</b>
	<b>Business Administration</b>	<b>10</b>	<b>14.9</b>
	<b>Banking and Financial Sciences</b>	<b>14</b>	<b>20.9</b>

<b>Variable</b>	<b>level</b>	<b>repeats</b>	<b>percentage</b>
<b>professional certificates</b>	<b>IT</b>	<b>4</b>	<b>6.0</b>
	<b>Economy</b>	<b>2</b>	<b>3.0</b>
	<b>Missing values</b>	<b>2</b>	<b>3.0</b>
	<b>Total</b>	<b>67</b>	<b>100.0</b>
	<b>JCPA</b>	<b>6</b>	<b>9.0</b>
	<b>CPA</b>	<b>4</b>	<b>6.0</b>
	<b>CIA</b>	<b>19</b>	<b>28.4</b>
<b>years of practical experience</b>	<b>CMA</b>	<b>3</b>	<b>4.5</b>
	<b>None</b>	<b>34</b>	<b>50.7</b>
	<b>Missing value</b>	<b>1</b>	<b>1.5</b>
	<b>Total</b>	<b>67</b>	<b>100.0</b>
	<b>From 5 years or less</b>	<b>8</b>	<b>11.9</b>
	<b>From 5 to less than 10 years</b>	<b>17</b>	<b>25.4</b>
	<b>From 10 years - less than 20 years</b>	<b>33</b>	<b>49.3</b>
	<b>More than 20 years</b>	<b>8</b>	<b>11.9</b>
	<b>Missing values</b>	<b>1</b>	<b>1.5</b>
	<b>Total</b>	<b>67</b>	<b>100.0</b>

It appears from Table No. (1) that the study sample is qualified to answer the items of the questionnaire and thus can be relied upon in their answers, which in turn enhances and strengthens the results of this study.

### 6.3 Test of validity and reliability of the study instrument:

The validity of the content of the instrument used in the study was confirmed by presenting it to a group of (8) experienced faculty members and departments in banks, to express their opinion in each field of study and the drafting of paragraphs and the extent to which each paragraph relates to its field. As some of the questions were modified, others were deleted, and new questions were added to conform to the proposals and observations of the arbitrators. Thus, the study instrument (the questionnaire) became in its final form consisting of (38) paragraphs distributed into (5) fields.

While the stability of the study instrument means the stability, reliability and predictability of the results; That is, the extent of agreement or consistency in the results of the questionnaire, as it was applied more than once in similar circumstances. To calculate the stability of the study instrument, the study instrument was divided into six field to measure the reliability of each one of them and for the instrument as a whole.

The Cronbach Alpha internal consistency test was used for the answers of the study sample obtained, and alpha can be interpreted as the internal stability factor between the answers. The increase in its value indicates the degree of high stability, and the statistically acceptable value for this scale is (60%) or more (Sekaran & Bougie, 2017), and in other studies the statistically acceptable value is (70%) or more, and it is clear from the results of the data analysis in Table No. (1) The result of the stability of the study paragraph is high.

**Table No. (2)**

The internal stability coefficients (Cronbach alpha) for each field of the study instrument and for the instrument as a whole

<b>Field</b>	<b>Number of Paragraphs</b>	<b>(Cronbach alpha)</b>
<b>Independent variable: cybersecurity governance</b>		
<b>Cybersecurity governance requirements</b>	<b>5</b>	<b>0.885</b>
<b>Cybersecurity program</b>	<b>5</b>	<b>0.928</b>
<b>Cyber Security Policy</b>	<b>5</b>	<b>0.917</b>
<b>Cyber information security management</b>	<b>5</b>	<b>0.905</b>
<b>Assessment and management of cyber risks</b>	<b>5</b>	<b>0.961</b>
<b>The dependent variable: big data</b>	<b>13</b>	<b>0.874</b>
<b>instrument as a whole</b>	<b>38</b>	<b>0.949</b>

Table No. (2) shows that all the values of the Cronbach alpha coefficients were high and that the stability of the study Paragraphs as a whole was high, reaching (94.9), which indicates that the study instrument has high

reliability (stability).

#### 6.4 Normal distribution:

Table No. (3) shows the result of the normal distribution test for the data, where the (Skewness& Kurtosis) test was used, and the results were as follows:

**Table No. (3)**

Field	Skewness	Kurtosis
<b>Cybersecurity governance requirements</b>	<b>- .960</b>	<b>.783</b>
<b>Cybersecurity program</b>	<b>-1.230</b>	<b>1.483</b>
<b>Cyber Security Policy</b>	<b>- .772</b>	<b>.810</b>
<b>Cyber information security management</b>	<b>- .787</b>	<b>.130</b>
<b>Assessment and management of cyber risks</b>	<b>- .717</b>	<b>-.199</b>
<b>Big data</b>	<b>- .236</b>	<b>1.341</b>

It appears from Table (3) that the test value for Skewness is between (1.96) and the value of the Kurtosis test lies between ( $\pm 2.85$ ), so the distribution of the data is subject to a normal distribution (Hair, Black, Babin& Anderson, 2010).

#### 6.5 Test for interference (correlation) between independent variables

Table No. (4) shows the value of VIF and Tolerance

The (VIF) test was relied upon to ensure that there is no problem of multiple linear relationships (multiple correlation), because it is considered a problem as one of the problems facing the statistical estimation of the regression coefficients, and Table No. (4) shows the results of the test for VIF:

Field	VIF	Tolerance
<b>Cybersecurity governance requirements</b>	<b>1.669</b>	<b>.599</b>
<b>Cybersecurity program</b>	<b>1.406</b>	<b>.711</b>
<b>Cyber Security Policy</b>	<b>1.289</b>	<b>.776</b>
<b>Cyber information security management</b>	<b>1.386</b>	<b>.722</b>
<b>Assessment and management of cyber risks</b>	<b>1.284</b>	<b>.779</b>

The above table shows that there is no multiple correlation problem between the independent variables being less than 5, thus accepting the level of variance in each of the independent variables.

## 7. Results:

Discussion of the results of the study:

Main hypothesis:

There is no impact of cybersecurity governance on the efficiency of big data implementation in Jordanian commercial banks. To test this hypothesis, multiple regression analysis was used to identify the relationship between cybersecurity governance and the efficiency of big data application in Jordanian commercial banks, represented by (cybersecurity governance requirements, cybersecurity program, cybersecurity policy, cyber information security management, assessment and management of cyber risks) in the implementation of big data in Jordanian commercial banks.

Table No. (5) shows that the value of Adj.R2 reached 0.779, which means that the independent variables explain 77.9% of the variance in the dependent variable. Also, the value of F = 47.520 and in statistical significance at the level of (0.00) confirms a strong and statistically significant relationship between cybersecurity governance and the efficiency of big data application in Jordanian commercial banks, represented by (cybersecurity governance requirements, cybersecurity program, cybersecurity policy, cyber information security management, assessment and management of cyber risks) in the implementation of big data in Jordanian commercial banks.

Thus, we reject the main null hypothesis, and accept the alternative hypothesis, which states: There is an impact of cybersecurity governance on the efficiency of big data implementation in Jordanian commercial banks. To test this hypothesis, multiple regression analysis was used to identify the relationship between cybersecurity governance and the efficiency of big data application in Jordanian commercial banks, represented by (cybersecurity governance requirements, cybersecurity program, cybersecurity policy, cyber information security management, assessment and management of cyber risks) in the implementation of big

data in Jordanian commercial banks.

Independent variable	$\beta$ value	T value	Statistical significance
<b>Constant</b>	<b>1.753</b>	<b>10.871</b>	<b>.000</b>
<b>Cybersecurity governance requirements</b>	<b>.134</b>	<b>3.187</b>	<b>.002</b>
<b>Cybersecurity program</b>	<b>.102</b>	<b>3.224</b>	<b>.002</b>
<b>Cybersecurity policy</b>	<b>.116</b>	<b>3.673</b>	<b>.001</b>
<b>cyber information security management</b>	<b>.145</b>	<b>4.563</b>	<b>.000</b>
<b>assessment and management of cyber risks</b>	<b>.103</b>	<b>4.048</b>	<b>.000</b>
<hr/>			
<b>F value</b>	<b>47.520</b>	<b>Statistical significance of F</b>	<b>.000</b>
<b>Adj. R<sup>2</sup></b>	<b>.779</b>	<b>R<sup>2</sup></b>	<b>.796</b>
<b>Durbin-Watson</b>	<b>2.258</b>	<b>Number of watches</b>	<b>67</b>

Results related to the first sub-hypothesis:

There is no impact of cybersecurity governance represented by the cybersecurity governance requirements on the efficiency of big data implementation in Jordanian commercial banks.

The result of the multiple regression showed a positive relationship between the cybersecurity governance requirements in cybersecurity governance and is statistically significant with the efficiency of implementing big data in Jordanian commercial banks, as the result indicates that increasing the independent variable by 1% leads to an increase of the dependent variable (big data) by (0.134) unit, and thus we reject the null hypothesis and accept the alternative hypothesis which states : "There is an impact of cybersecurity governance represented by the cybersecurity governance requirements on the efficiency of big data implementation in Jordanian commercial banks.

Results related to the second sub-hypothesis:

There is no impact of cybersecurity governance represented by the cybersecurity program on the efficiency of big data implementation in Jordanian commercial banks

The result of the multiple regression showed a positive relationship between cybersecurity program in cybersecurity governance and is statistically significant with the efficiency of implementing big data in Jordanian commercial banks, as the result indicates that increasing the independent variable by 1% leads to an increase of the dependent variable (big data) by(0.102)unit, and thus we reject the null hypothesis and accept the alternative hypothesis which states : "There is an impact of cybersecurity governance represented by the cybersecurity program on the efficiency of big data implementation in Jordanian commercial banks.

Results related to the third sub-hypothesis:

There is no impact of cybersecurity governance represented by the cybersecurity policy on the efficiency of implementing big data in Jordanian commercial banks

The result of the multiple regression showed a positive relationship between the cybersecurity policy in cybersecurity governance and is statistically significant with the efficiency of implementing big data in Jordanian commercial banks, as the result indicates that increasing the independent variable by 1% leads to an increase of the dependent variable (big data) by (0.116)

Unit, and thus we reject the null hypothesis and accept the alternative hypothesis which states : "There is an impact of cybersecurity governance represented by the cybersecurity policy on the efficiency of implementing big data in Jordanian commercial banks

Results related to the fourth sub-hypothesis:

There is no impact of cybersecurity governance represented by cyber information security management on the efficiency of big data implementation in Jordanian commercial banks

The result of the multiple regression showed a positive relationship between the cyber information security management in cybersecurity governance and is statistically significant with the efficiency of implementing big data in Jordanian commercial banks, as the result indicates that increasing the independent variable by 1% leads to an increase of the dependent variable (big data) by (0.145) unit, and thus we reject the null hypothesis and accept the alternative hypothesis which states : "There is an impact of cybersecurity governance represented by cyber information security management on the efficiency of big data implementation in Jordanian commercial banks.

Results related to the fifth sub-hypothesis:

There is no impact of cybersecurity governance represented in assessment and management of cyber risks on the efficiency of big data implementation in Jordanian commercial banks.

The result of the multiple regression showed a positive relationship between the assessment and management of cyber risks in cybersecurity governance and is statistically significant with the efficiency of implementing big data in Jordanian commercial banks, as the result indicates that increasing the independent variable by 1% leads to an increase of the dependent variable (big data) by (0.103) unit, and thus we reject the null hypothesis and accept the alternative hypothesis which states : "There is an impact of cybersecurity governance represented in assessment and management of cyber risks on the efficiency of big data implementation in Jordanian commercial banks

## **8. Recommendations:**

- 1) The necessity of realizing the reality of dealing with big data and increasing the interest of the administrations of Jordanian commercial banks by providing robust and supportive cyber governance.
- 2) The necessity for Jordanian commercial banks to exploit large amounts of data to predict future expectations for many important financial decisions.
- 3) That Jordanian commercial banks should rely on a variety of sources commensurate with the nature of the required tasks, with an increase in interest in classifying data through systems that help in retrieving and using them in the future and in a manner consistent with the cyber governance tools that they have.
- 4) That the administrations of Jordanian commercial banks should pay attention to restructuring their own organizational structure to support the flow of data between different departments, by means of creating robust cyber governance that has its own inputs related to big data technologies.

## **Resources and references:**

- Abdullah Khalid; Al Henini, Abdullah. (2018). Big data in Sultan Qaboos University libraries: its reality and the impact of the role of managers as a mediating variable to be used in improving services. Iraqi Journal of Information Technology, 9 (1).
- Abdul Ridha Asaad Tarish; Al-Maamouri, Ali Ibrahim. International Studies (2020) Cybersecurity and its role in the spread of the phenomenon of terrorism in Iraq after the year 2003, University of Baghdad, Center for International Studies. Issue 80, p. 149-190,
- ACCA &IMA ,(2013) Big Data: Its Power And Perils, [Https://Www.Accaglobal.Com/Bigdata](https://Www.Accaglobal.Com/Bigdata)
- Al-Hormzi, SaifNasrat 2019 Describing Approaches to Digital Actor Perspectives and Strategic Exposure in the Light of Cybersecurity, Al-Farahidi Literature Journal, Issue 37, University of Tikrit
- Al-Saeed, Fadi, (2019), Letters on Cybersecurity Governance, <https://www.linkedin.com/>
- Al-Saeed, Ibrahim. (2019). Governance and asymmetry of accounting information, Cairo: El-Baheith Foundation for Research Consulting - AskZad.
- Boomer,J,(2018).The Value Of Big Data In An Accounting Firm.Available From [Www.Cpacpracticeadvisor.Com](http://Www.Cpacpracticeadvisor.Com)
- Bin Al-Tayeb, Zainab, Al-Rubaihi, Suleiman Bin Ibrahim. (2019). New Information Specialist Roles for Engaging with Big Data, Journal of Information Studies & Technology. Issue (2).
- Daniel,L.,(2018). Big Data Analytics And Business Analytics, Journal Of Management
- Fan, W, Bifet, A.(2013). Mining Big Data: Current Status, And Forecast To The Future, AcmSigkdd Explorations Newsletter, (14) 2.
- Gamage,P.(2016). Big Data: Are Accounting Educators Ready?, Accounting And Management Information Systems, (15) 3.
- Gartner, Anne L.(2014). Government Information Policy In The Era Of Big Data, *Review Of Policy Research*. Jul2014, Vol. 31 Issue 4, P319-325.
- Gupta,S, Modgil,S, And Gunasekaran,A.(2020). Big Data In Lean Six Sigma: A Review And Further Research

- Directions, Journal International Journal Of Production Research, (58) 3.
- Hair, Black, Babin&Anderson, (2010). Multivariate Data Analysis, 7<sup>th</sup> ed. Upper saddle River, new Jersey, Person Education International.ISO,2017,big data <https://www.iso.org/home.html>
- Marijn,W.(2017). Opportunities And Challenges Faced By Management Accounting In The Era Of “Internet Plus”And Big Accounting.Advances In Social Science, Education And HumanitiesResearch, (172).
- Raguseo, E. (2018). Big Data Technologies: An Empirical Investigation On Their Adoption, Benefits And Risks For Companies, International Journal Of Information Management, (38) 1.
- Roger J. Bougie,Uma Sekaran, 2017 .Research Methods for Business ,John Wiley & Sons, 7,Limited, 2017
- Saleh, Ahmad Ali and Al-Salehi, Nazal Amin, (2018), University Governance Models and their Impact on Building Strategic Orientation - An Applied Study in Private Jordanian Universities in Amman, Journal of the Association of Arab Universities for Research in Higher Education, 28 (2).
- Singh, S, Firdaus, T, And Sharma, A.K .(2015). Survey On Big Data Using Data Mining, International Journal Of Engineering Development And Research, (3) 135.
- Tesfaye,B.(2017).What Is The Influence Of Big Data And Analytics On Management Control Systems?,Accounting And Control Master Thesis.
- The Central Bank of Jordan, (2018), Instructions for Adaptation to Cyber Risks
- Qantqji, Samer. (2014). The Big Data Market and New Concepts, The International Journal of Islamic Economics, Issue (23).