DATABASE AS A SERVICE: SECURITY AND PRIVACY ISSUES, AND APPROPRIATE CONTROLS

Co-authored by Sarat Kehinde Akinade

Bobby Swar

Pavol Zavarsky

Project report

Submitted to the Faculty of Graduate Studies,

Concordia University of Edmonton

in Partial Fulfillment of the

Requirements for the

Final Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

April 2020

DATABASE AS A SERVICE: SECURITY AND PRIVACY ISSUES, AND APPROPRIATE CONTROLS

Sarat Kehinde Akinade

Approved:

Bobby Swar [Original Approval on File]

Bobby Swar Date: April 18, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: April 18, 2020

Dean, Faculty of Graduate Studies

Database as a Service: Security and Privacy Issues, and Appropriate Controls

Sarat Kehinde Akinade
Information Systems Security Management
Concordia University of Edmonton
Edmonton, Canada
sakinade@student.concordia.ab.ca

Bobby Swar
Information Systems Security Management
Concordia University of Edmonton
Edmonton, Canada
bobby.swar@concordia.ab.ca

Pavol Zavarsky
Information Systems Security Management
Concordia University of Edmonton
Edmonton, Canada
pavol.zavarsky@concordia.ab.ca

***Abstract*— Database as a Service (DBaaS) is one of the key cloud computing services that is well-known as a type of Application-as-a-Service which gives users access to a database without downloading and installing software or performance configuration but maintains the customers database. DBaaS assumes the responsibility of traditional database administration software in which data owners and clients can build, update, delete, and have access to database services without installing physical hardware and it is also economically feasible for users. Despite the advantages that DBaaS has, it suffers from many challenges, which need considerable security. For example, providers are liable to infringe consumer confidence with the risk that data security and privacy may be impeded. Additional overheads of remote network access, data security infrastructure, and user interface design for such a service are among the key issues that DBaaS faces. So, the migration of databases without impacting the consistency of the solutions is still in its infancy. This research paper identified security and privacy issues in DBaaS and offered adequate solutions to mitigate it. The identified security and privacy issues are discussed with their consequences and the security functions are taken into consideration to demonstrate the impacts on security purpose. With that, the provision of security controls by three vendors (Amazon, Microsoft Azure and Oracles) and together with related security controls and best practices from ISO 27001/2013, CSA/CCMv3.0.1 and NIST 800-53 R5 are mapped with the identified issues to aid the creation of security controls to mitigate the risks.**

Keywords- **Assurance, Database as a Service (DBaaS), DBaaS, Security and Privacy, Cloud client, DBaaS Service provider, security and privacy Controls.**

I. INTRODUCTION

Database as a Service (DBaaS) is one of the cloud computing models enjoying the high-scalability and availability of the cloud without downloading, maintaining, updating, backing or handling the database or underlying infrastructure [1]. Based on Software as a Service (SaaS), DBaaS transfers database management system (DBMS) to a third-party architecture from a conventional client-server model where the data owner is responsible for handling DBMS and responding to user requests and Where the data owner does not control the data security [2]. In that regard, DBaaS offers on-demand data management services for cloud clients and cloud computing support to big-data by providing high-performance virtual hardware, storage, processing of data, providing a fault-tolerant, available, reliable and scalable environment [6][2].

Cloud applications have made the DBaaS a popular way to provide versatile and secure data storage services [7]. In DBaaS**,** all the slow time-sensitive administrative database activities can be outsourced or automated**,** which means Database Administration System (DBAs) will not only be freed from database setup but will finally be able to focus on something more than backups, recovery, tuning, optimization, patching, and upgrading [19].

DBaaS is particularly suitable for Small to Medium-sized enterprises SMEs, which depend on databases but find their deployment and maintenance costs to be restrictive. They can access on request their database instances, using interfaces or programming tools [1] [2]. Based on the DBaaS model, there are two significant platforms that DBaaS is categorized as rational database SQL and non-rational NoSQL [1]. DBaaS realized that developers would call a database service and function without even considering the database [1]. For business organizations to keep track of their everyday transactions, there are several cloud repositories available [21].

According to the 451 Voice of the Enterprise Research (VotE): Cloud Computing survey conducted in the second quarter of 2015, 4.4% of respondents using SaaS with Platform as a Service (PaaS) as the primary implementation platform for operational and analytical database workloads, while 2.9% using network databases as a service. In comparison, 58.1% of operational and analytical database workloads are implemented in on-site, non-cloud settings, while 16.8% use on-site private cloud. More than 51% of social business applications are delivered as a service and 9.6% of analytics / business intelligence deployments are recently delivered as a service [11]. Rising cloud use for operational and analytical databases was indicted by the respondents as being 8.5% in the next two years. The database deployed on IaaS is expected to grow from 2.9% to 8.0%, the use of on-premises is expected to decline but remain with levels at 38.7% compared to the recent 58.1%. On-premises private cloud usage will grow from 16.8% to 22.5%, while hosted private cloud usage should almost double from 8.5% to 16.1%. Off-premises will decline from 9.3% to 6.2% [11].

Since the data is processed on the service provider servers, the server may be wary of leakage and abuse of the data. In this situation, database protection can be disrupted

dramatically when adequate protection is not implemented, then there is the risk of data breaches and unauthorized manipulation of the data [26].

Findings have shown that none of today's cloud service providers provide security assurances in their Service Level Agreements (SLAs) [23]. The SLAs of S3, Azure, and Amazon relational database service, for example, it just guarantees flexibility (percentage of monthly uptime). When the quality drops below 99.95%, consumers must refund a fixed amount of money [23].

Although, authentication, confidentiality, data integrity and non-repudiation of the cryptographic database are some of the important security features that are easy to obtain. Before this new computing paradigm is implemented, however, some issues about privacy and security need to be addressed. Firstly, the consumer does not have the kind of control over data processing that can result in data breaching by revealing sensitive data intentionally or unintentionally, or the performance of the applications necessary, or the ability to inspect or alter the processes and policies under which it must operate. Different parts of an application could be in different places in the cloud which could adversely affect the application's efficiency. Such issues emanate from the large size geographical distribution and structure of cloud computing.

Customers will be gained from the cloud infrastructure if the process for data security and privacy of the users is strengthened.

Therefore, this paper explores the use of international frameworks, guidelines and standards to establish appropriate security controls to mitigate DBaaS security and privacy concerns which will serve act as a key security guideline for its reliability.

II. Review of Related Work

In the following sections, DBaaS Security and privacy issues are discussed which were categorized into the security principle (C I A) Confidentiality, Integrity and Availability.

A. Security and Privacy Issues with DBaaS

The DBaaS model was introduced by Hacig umus and others which has attracted a significant attention to the research community [22]. Because of the various threats that obscure the use of cloud computing, the security of confidential business data is becoming a matter of concern. There has been a lot of data security and privacy breaches in the cloud, and especially in the cloud database domain [3].

Basically, data owners turn over their data authority to the DBaaS service providers which there can be security issues like data availability, integrity, confidentiality (access to critical business information). If service providers fail to satisfy these requirements, then their clients seek service from alternative companies. The confidentiality in the context of DBaaS concerns the secure implementation of queries produced by trusted clients [9]. This shows that only authorized persons can access data in an encrypted format. However, lack of privacy reduces the degree of confidence users are willing to place in the system is also one of the major barriers in cloud database deployment [24].

In addition, the integrity of the database is also a security issue in DBaaS management; referring to the right to test if the outsourced data is corrupted or compromised without requiring retrieval[24].Also, Query integrity refers to the ability to check the accuracy and completeness of the results of the query returned from Cloud Service Provider CSP; this means that the records returned still remain in the outsourced database and were not updated in any way [23]. Many current methods, such as probable data possession (PDP) and retrievability proofs (POR), are aimed at solving this problem [23]. The service provider can leak confidential data, change the data or return users with inaccurate data. Security in the outsourcing of databases mainly means data protection and data integrity [25].

Also, *data integrity*; This process entails the protection of information from fabrication, modification and deletion [7]. Therefore, it is the responsibility of DBaaS service providers to guarantee cloud clients with data consistency and accuracy. Data integrity, however, for example, when a disgruntled user accesses the data, unauthorized can by any form causes data manipulation and conflict in DBaaS [7]. However, some important aspects of security in cloud integrity include problems with middleware muddles, authentication and regulatory enforcement [21][7]. The middleware muddle deals with the technology that allows the incorporation of the components into a distributed network. As software, it enables application components to interoperate through network links despite the differences in underlying device architectures, communication protocols, and other application services. Middleware allows architectural patterns to be created which reflect innovative design methods for device-specific problems. Many managers in an enterprise have found and attested that unauthorized access to the database creates security holes [21].

Furthermore, *data availability* is an issue resulting from the assessment of DBaaS security. It describes the levels to which DBaaS resources remain intact and therefore serves as an essential security requirement. In particular, the unavailability effect occurs either temporarily or permanently [3]. During such a time, DBaaS unavailability may result from resource exhaustion, natural disasters, DOS attacks, internet downtime, poor auditing and equipment failures. On the other hand, external malicious attacks cause distrust between DBaaS service providers and cloud clients [8]. Such include phishing, denial-of-service, scamming, data intrusion, and fraud and software exploitation. Besides, the unavailability of database resources affects the output and any other related service [3]. In its licensing agreement, Amazon stated that service is often unavailable [3]. For example, Some cloud database service providers, Google Cloud SQL and Amazon's relational database service, provide clients with a network interface or application programming interface to access transaction logs in the database[23]. These logs are however, not cryptographic evidence, and can therefore easily be falsified or erased.

In the same way as other cloud services, DBaaS has challenges that leads to availability issues such as load balancing and the assignment of adequate logical resources [9]. Therefore, to support significant data functions, tenant networks must run independently. As a result, this multi-tenancy creates a management challenge in dynamic cloud environments where the number of tenants varies from time to time [9][3]. Hence, tenants can experience database unavailability, which affects the performance of their information system. The role of DBaaS security is always ensuring data transit while minimizing the risk from malicious parties [9][3].

These attacks cause harm and theft of information residing in DBaaS repositories following unauthorized access to such resources. Researchers argue that if end-users encrypt their data, then they would not suffer from privacy concerns that comes with this issue.

Similarly, access control issues breach DBaaS *confidentiality* when service providers are unable to effectively manage the access to and transfer of data [7]. In this case, outsourced data is challenging to manage, primarily if it is in restrictive categories. Therefore, the inability to manage big data results in the loss of cloud client trust. Illegal data recovery is a problem identified to cause breach of data confidentiality in DBaaS systems [7][3].

During DBaaS operations, service providers may alter or delete data from their storage devices. Besides, recovering data from hard drives introduces logical and physical risks. Also, confidentiality of DBaaS Problem is Failed supply chain. In such instances, DBaaS service providers outsource specialized database services to third parties [8][3]. As a result, the security of their systems relies on those of the third parties contracted. Therefore, such contracts must be transparent [8]. Confidentiality issues also arises when DBaaS service providers are unable to conduct data provenance [8]. In that regards, this concerns can be from errors, bugs and external attacks.

Similarly, insider threats emanating from privileged access to data and maintenance purposes is a concern [8]. This problem manifests in instances where DBaaS administrators misuse their privileges and fail to enforce strict security measures to protect data. In such cases, organizations link legal actions by specifying roles to mitigate espionage and intentional misconduct. In such instances, it becomes challenging to trace data movement to determine the source. Such details include the data creator and accuracy of information [8][3]. In addition, the scalability promised by DBaaS is also challenging for service providers to handle, particularly when scaling the cause of the increase in storage nodes [3].

Another pressing issue among DBaaS vendors is the lack of interoperability [3]. For DBaaS providers to be able to connect by Application Programming Interface API, there must also be a popular front-end which appears as a single homogeneous entity with semantic calls [3]. Databases are the most attractive targets for attackers because they store information with all the confidential data. Having access to databases is often useful with security layers, such as firewalls and intrusion detection systems [19]. However, recent attacks have leveraged channels that have authorized access to the database, such as users, administrators, developers, testers, partners, and outsourced services.

Furthermore, privacy is a concern in cloud databases associated with access to confidential user data. The issue could either result from accidental or deliberate actions of malicious parties, whose aim is to delete or change information [14]. Unfortunately, most of the cloud service providers share their clients' data with third parties, which introduces privacy concerns. Often, privacy issues emanate from the inability of data handlers to follow the regulations and policies of data protection [14]. Hence, cloud clients lose trust in their cloud database service providers. However, the researchers argue that if end-users encrypt their data, then they would not suffer from privacy concerns. Therefore, service providers have the responsibility of encrypting client data at different levels based on the query executions of the end-user [14].

DBaaS service providers deal with privacy issues where the contracts with their cloud clients require them to protect private information [9]. The issue of privacy increases the susceptibility to data breaches. In DBaaS, data locality remains unknown to clients, which raises privacy concerns. In some cases, it is unclear whether DBaaS service providers follow data privacy laws [9]. Hence, the issue of data locality arises when nobody seems to take responsibility for data disruption. Resultantly, the co-location of data becomes difficult for a service provider serving multiple cloud clients [8].

Similarly, jurisdiction differences make the enforcement of legal frameworks for data privacy a challenge for DBaaS companies [7][3]. For instance, some countries are reluctant in the enforcement of relevant laws. Cloud data, which stored in different locations, is vulnerable to jurisdiction differences. Therefore, it can be accessed by unauthorized parties, especially when their lack of strict policies on consumer data protection in cloud platforms such as DBaaS [7][3].

In the next section, the overview of the related security and privacy guidelines, frameworks and standards are discussed.

Besides, network breaches affect the DBaaS model, where communication becomes susceptible to eavesdropping and modification. Attackers use techniques such as network sniffing to identify database vulnerability and launch attacks such as man-in-the-middle and cross-site [3]. Such reports can not be attestations of either the property breach or the service provider's tampering with the service provided [23].

Similarly, DBaaS providers incorporate different security standards, such as identity and access management, data encryption, and that ensures physical security and data center monitoring. Providers such as Amazon, Google, Microsoft, IBM and Rackspace are all certified for their cloud services according to ISO/IEC 27001 [1].

B. *Overview of the Related Security and Privacy Guidelines, Frameworks and Standards.*

1) *NIST SP 800-53 Revision 5*

The National Institute of Standards and Technology, Security and Privacy Protection for Federal Information Systems and Organizations (NIST SP 800-53 Revision 5) has been developed to assist organizations in the selection of security controls for information systems by implementing baselines for security control [4]. Based on many assumptions, including specific environmental, organizational and functional criteria, the baselines discuss the protection needs of a broad and varied set of classes. However, the baselines often presume that rising information systems face traditional threats but not directly in the sense of a cloud or cloud storage [4].

2) *ISO/IEC 27001:2013*

ISO/IEC 27001 defines the requirements for establishing and maintaining an Information Security Management System (ISMS) [18]. This standard describes the process of creating a model of the entire business risks of a given organization and specific requirements for the implementation of security controls. The ISMS is established in the Plan phase, and the ISMS is implemented and operated in the Do phase. During the check phase, the ISMS is monitored and reviewed, and during the Act phase, the ISMS is maintained and improved. The scope and boundaries of ISMS, its stakeholders, the environment, assets and all the technology involved are defined in the Plan phase.. In this phase, also the ISMS *policies*, *risk assessments*, *evaluations*, and *controls* are defined. Risk is modified with the help of various controls in ISO 27001[18]. Where specific and detailed thresholds are not provided, most organizations usually use ISO 27001 in combination with ISO 27002. For instance, ISO 27002 offers fourteen requirements and guidance on how to implement the measures that are specified [15].

3) *CSA/CCM v3.0.1 Cloud Security Alliance*

CSA is a non-profit organization and over time, it has developed refined practices that define cloud computing based on a new model of operation. The organization also came up with a set of technologies useful in computer resources that are shared. To come up with their findings on vulnerabilities in cloud computing, the organization carried out a survey that assisted in coming up with findings. The group identified data loss and breaches and insecure APIs, CSA created a standard, cloud control matrix CCM to provide security controls that can be a guide for both customers and providers in the assessment of the risk associated with the providers [17]. CCM Matrix is designed as a control framework that is aligned with CSA guidance v3 of 13 domains and CSA guidance v4 of 14 domains [10]. Hence, some other related industry-accepted security standards, regulations, and controls frameworks such as ISACA COBIT, PCI, Jericho Forum and NERC CIP are also described in the CCM Matrix. CSA/CCMv3.0.1 Matrix is used as a related control framework to map the identified issues for DBaaS [17].

C. *Security and Privacy Protection Solutions from Three Related Vendors*

1) *Oracle cloud database security*

A multitenant version of a database cloud service comprises Oracle database cloud service that is independent and separated from all other cloud services offered by the company. This can be defined as follows, administrators can identify users for the services they manage, and users can be categorized either with the Cloud Identity Manager or within the Database Cloud Service-Multitenant Edition Development Platform Administration region itself [12]. There are three roles for each Database Cloud Service - Multitenant Edition, Service Administrator, who can create, modify and delete service users and their privileges. Both in the Cloud Identity Manager and the Administration area of the service development platform [12].

Another one is the Developers who can use the software framework for developing applications within a service but cannot build, change or uninstall users for that service. Finally, end-users who can run applications and when a feature is connected to a device Identity Domain, three individual roles which map to these levels are created within the Identity Domain [12]. Strict security procedures and practices that are based on experience acquired over a long period are used to incorporate the Oracle Multitenant Version cloud database. Safe access to data centers, regular security audits by third parties to ensure compliance with regulatory requirements and a full audit of the entire cloud stack every quarter [12].

To protect data that is stored in disks against direct access to the information that is unauthorized, transparent data encryption is used. The encryption and decryption of data are handled automatically by the Oracle Database. The data that is to be loaded is compressed automatically which reduces the time required to upload the data into the cloud. The main motive for developing Application Express was to be used in coming up with applications that were based on HTML and to develop an application that is safe for use in the Database Cloud service. This supports several authentication schemes, gives developers the ability to use authorization schemes, includes robust monitoring tools, protection against cross-site scripting attacks and the option to automatically protect navigational URLs from being maliciously modified, this is called “session state protection” [12].

Lastly, Application Express reports allow to see the security options in force for an application rapidly and to monitor the usage of applications and individual pages in applications [12]. RESTful Web Service is one of the security measures and access to RESTful calls uses HTTPS which secures communication between the client and the Database Cloud Service [12].

Therefore, various strategies used to enhance security include Oracle detective security controls, data encryption, user and multifactor access control, database activity monitoring and blocking, auditing and reporting that is consolidated, and data masking [19][12]. The Oracle Database Vault which is a unique security control was also developed to prevent the database accounts that are privileged from accessing sensitive information. However, these individuals can perform essential operations such as patching and backup [19]. With the help of sub-setting and data masking, it makes it possible for individuals to extract copies of application data either as a whole or in subsets. Another part of the data cloud service offered by Oracle is fine grain and unified auditing that is like encryption.

2) Microsoft Azure database security

Microsoft Azure provides confidentiality, integrity, and availability of customer data, while also enabling transparent accountability. As a public cloud service platform, Azure assists in the support of a wide selection of devices, database tools, programming languages, and operating systems among others [13]. One of the top priorities for the Azure SQL database is the issues relating to security. Firewall rules are used to restrict access to databases and other authentication procedures. The azure active directory SQL database for Azure to the warehouse for SQL data through the help of identities in Azure AD [13]. The figure that has been featured below outlines the basics that are used to secure the data tier of an application through the application or use of the Azure SQL Database. The strategy that is used to enhance security as described applies the layered defense-in-depth approach as shown in figure 1 below:

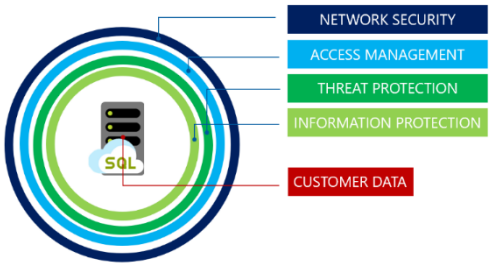

Fig. 1. Azure SQL database defense-in-depth approach [13].

Research [13], stated that with the help of Microsoft Azure SQL Database, enterprise applications and cloud are provided with a relational database service. To enhance security by safeguarding customer data, the outer layer, which is network security, prevents any access into a database from any network until access is granted based on Azure virtual network traffic origin or IP address. Also, in the second step, *access management* ensures that *authentication* comes in two types SQL and Azure *Active Directory Authentication* The user is also assigned permission within the Azure SQL database which determine what an individual can do. Customers can control access to rows through permission granted by *Role level security* [13]. Figure 6 below shows the role level security analysis in the Azure SQL database.

The third layer of protection as seen above is threat protection and it facilitate the detection of various threats that may arise which facilitated SQL auditing which occurs in Azure Even Hubs and monitors logs. [13]. The last layer is information protection and encryption that enhances security for the database through transport layer security (TLS) and Transparent Data Encryption (TDE) [13]. All these controls can be managed securely by vulnerability assessment, data discovery Classification, compliance, and feature restrictions [13].

See figure 2 below for the illustration of role level security in the Azure SQL database.

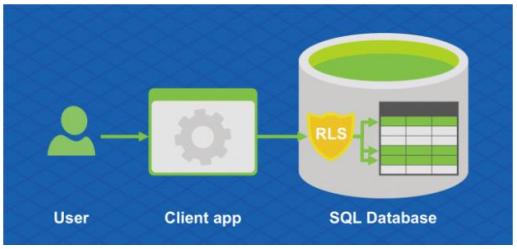

Fig. 2. Role Level security in Azure SQL database security [13].

3) Amazon AWS Security Database Service

Through Amazon Web Services, several database solutions are available to businesses and developers. They include managed relational, petabyte-scale data warehouse service, and NoSQL database services among others [20]. This part will give an elaborate discussion on Amazon Relational Database Security (RDS). Through RDS, individuals can create a relational database that enables them to have a storage capacity that meets the demand of an application [20].

The Amazon RDS usually works in managing databases for clients by performing various activities such as backing up data, dealing with failover, and handling the database software. Currently, this RDS is available for Microsoft SQL Server, MySQL, Oracle, Amazon Aurora, MariaDB database engines, and PostgreSQL [20]. To promote reliability and efficiency Amazon RDS for critical production applications has various features such as DB snapshots, multi-AZ deployments, SSL connections, and back-ups that are automated. Also, amazon RDS can support access control which is used to control access to DB instances [20].

Network isolation is a network access control that can be run in the DB Instances in an Amazon VPC [20]. It makes it possible for clients to select the IP range that they wish to use and then connect to their IT infrastructure that facilitates the isolation of DB instances. Another means that is used is encryption where a secure socket layer (SSL) is used to encrypt the connection between the DB Instance and the application [20]. The Transparent Data Encryption (TDE) is also supported by the Amazon RDS which allows data to be encrypted during storage. Also, this RDS facilitates DB instance Replication that makes it possible to

come up with data center facilities that are available with ease in various parts around the world. This provides reliable, in-expensive, network connectivity availability to zones in the same location [20].

Also, Amazon provides Redshift to offer an SQL database service that operates highly optimized AWS compute and storage resources [20].

The available security and special protections that are currently and presently used by the service provider mentioned in the white papers are summarized in Table 1 below. See Appendix 3 for the rest of the

TABLE I. LIST OF THE VENDORS PROVIDED SOLUTIONS FOR PRIVACY AND SECURITY ISSUES

			ORACLE CLOUD DB			MICROSOFT AZURE			AMAZON AWS		
	IDENTIFIED ISSUES	**VENDORS PROVIDED SOLUTIONS**	**C**	**I**	**A**	**C**	**I**	**A**	**C**	**I**	**A**
1	Resource Allocation for Multiple Tenants: Multi-Tenancy [3] [8] [10] [12]	• Oracle Database Vault. • Azure Key Vault and Dynamic data masking. • Azure Row level Security.	✓	✓		✓	✓				
2	Resource Exhaustion [3] [12]	• Amazon Redshift of a petabyte-scale. • Amazon RDS, DB Instance replication. • Oracle Data masking and sub-setting			✓			✓			✓

Furthermore, the identified issues collected from the different sources are listed in Table II alongside the consequences and specified with the security principles, Confidentiality, Integrity and Availability. More so, the STRIDE threat modelling mapped together with it, (Spoofing, Tampering, Repudiation. Information Security, Denial of Services and Elevation of Privilege).

Table II below shows the list and see the rest of the results in appendix 1. Also, in the next step, the identified issues are mapped with the guidelines, standards, frameworks to mitigate the security and privacy issues to serve as a core security guideline for the reliability of DBaaS. See Table III and Appendix 2 for the rest of the results.

Lastly, the state-of-the-art solutions from three key vendors such as Oracle (Cloud Database), Amazon (AWS), and Microsoft (Azure) are listed in a table. See Table I and Appendix 3 for the rest of the results.

For the next section, the results were discussed to describe each table.

IV. RESULTS AND DISCUSSION

There were fourteen identified issues collected from the related papers and they are listed in table II below with the issues explanation and consequences described in different columns and specified with the key security principles, Confidentiality, Integrity and Availability and STRIDE threat model.

III. METHODOLOGY

In order to identify the security and privacy-related issues in DBaaS, literature review of related papers on DBaaS security and privacy issues is conducted by using the most popularly and well-known research database engines name as IEEE Xplore, Google Scholar, ACM Digital Library and Science Direct, a semantic scholar with the use of the search keywords, “Overview Database as a Service (DBaaS)”, “Security and privacy issues in DBaaS”, “Database as a Service security and privacy issues, Controls and Solutions ” and a total of 110 papers are selected based on the keywords.

The identified issues described in table II second column are the types of vulnerabilities in the DBaaS that pose significant security and privacy risks to the data stored in the database which can be utilized by the attackers to gain unauthorized access into the asset. The consequences in the third column show the effect the identified issues could cause the stored data in DBaaS. Below is the brief description of the security principle. The Security requirement is specified with the identified issues to show the effect of each issues to the security purpose a system requires. The security requirement is the principle of security called CIA which acronyms are classified as Confidentiality Integrity and Availability identified the threats in DBaaS.

Confidentiality applies to data privacy where, on any occasion, data belonging to the User is not exposed to unauthorized parties. *Data integrity* refers to the trust that the data stored in the cloud is not manipulated by unauthorized parties, data in transit often relates to Integrity and on-site. The quality of data is simply that data should be *available* without pause or reject whenever the user wants data. The *privacy* of the database conceals the identity of the user when the data is collected or manipulated.

STRIDE is a type of system that intends to identify known threats by the form of exploits used. STRIDE is classified into six classes and the acronym derives from the first letter of each of the terms are as follows (Spoofing, Hacking, Repudiation, Information Security, Service

Denial and Privilege Elevation), this is used to resolve threats and create security specifications that mitigate the issues identified in this paper, also, enables security designers to reliably predict the capabilities of the attackers, and provide general security guidance. Table II shows the summary of the identified issues.

Besides, the identified issues were mapped with the related standard, framework and guideline such as ISO 27001:2013, NIST 800-53 r5 and CSA/CCM v3.0.1. Also, with the solutions provided by the three recognized vendors (Oracle cloud DB, Microsoft Azure and Amazon AWS) serve as a control guideline for DBaaS.

In Table III, the first column is the identified issues, the next three columns are the three related standards, frameworks and guideline where each control are listed to map the issues, the next column is the control description where the appropriate controls used are explained. The last column represents the vendor's solutions provided to mitigate DBaaS Security and Privacy.

TABLE II. LIST OF THE IDENTIFIED SECURITY AND PRIVACY ISSUES IN DBAAS

NO	ISSUES	ISSUES EXPLANATION	CONSEQUENCES	SECURITY CATEGORIES	THREAT TYPE(STRIDE)
1.	Resource Allocation for Multiple Tenants: Multi-Tenancy [3] [8] [10] [12]	Potential architecture software in which programs run on a single server and serves several tenants i.e. it allows each user to have their instance of a shared application. In that case, outsourced data is critical as several users will be sharing software in the same system and this required privacy, confidentiality and integrity.	• The issue faced is the allocation of physical resources to multiple users who access common data repository which increases the risk of data stored in the database. • Side-channel attacks could occur based on information gathered from bandwidth-monitoring and lack of authorization mechanisms for sharing physical resources. • Some Physical device configuration can be tricky. • Load balancing will be like a hybrid method across physical resources. .	• Confidentiality • Integrity	• Information Disclosure • Tampering
2.	Resource Exhaustion [3] [12]	• This is one of the memory use problems on the database server that can result from a lack of throttling over the number of resources allocated and some other likely scenarios.	• Denial of services caused by flooding of abnormal TCP packets without any collection of flags can affect performance. • Users can steal each other disk space and partition that is used which can cause a spoofing attack. • Memory Failure.	• Availability • Authorization	• Denial of Service • Spoofing
3.	Escalation of data resources [3] [10]	• The capability of Database to handle the demand of removing/adding of resources to improve availability and performance especially when changes are unpredictable but realizing such gains requires reconfiguration and downtime.	• The automated data scaling causes confidentiality and Availability problems.	• Confidentiality • Availability • Authentication	• Information Disclosure • Denial of Service. • Spoofing

TABLE III. DBAAS SECURITY AND PRIVACY ISSUES MAPPED TO RELEVANT CONTROLS AND VENDOR'S SOLUTIONS

IDENTIFIED ISSUES	NIST 800-53 R5	ISO 27001:2013	CSA/CCM V3.0.1	CONTROL DESCRIPTIONS	VENDORs SOLUTIONS
Resource Allocation for Multiple Tenants: Multitenancy [3][8][10][12].	AC-4 RA-2. CA-3 CA-9 SC-2 SC-7 SC-4	A.8.2.1 A.6.1.1 A.6.1.2 A.8.1.4 A.13.1.3 A.9.4.1	DSI-01- IVS-09 IAM-05	• The conflicting duty and areas of responsibility should be separated to minimize the risk of unwanted or accidental modification or misuse of the properties of the organization. • Separation of duty reduces the potential for misuse of permitted rights and helps reduce the possibility of non-collusion malicious activity. • Information should be classified against unauthorized disclosure or alteration in terms of legal criteria, interest, criticality and sensitivity. • Organization should Separate vital Internet networks from other, less responsive and the internal networks through firewall, virtual local network and separation techniques (Segregation of Network)	• Oracle Database Vault. • Azure Key Vault and Dynamic data masking. • Azure Row level Security.
Resource Exhaustion [3] [12]	CP-2,7,6,8,9, CP-10 RA-3 MP-4, MP-5, PE-3, SC-36, SI-13.	A 12.3.1 A.8.2.3 A.17.1.1 A.17.1.2	BCR11 BCR09	1. Fault-tolerant services should be required to prevent interruptions arising from a single failure point and to ensure the high availability and business continuity of mission critical applications or systems . 2. 2. Alternate storage sites are the basis for contingency planning, so organizations can maintain critical operations and business processes despite the interruption, disagreement or failure of the organizational structure. 3. Organization backup arrangement for specific systems and facilities should be reviewed regularly to ensure that they follow the business continuity plans criteria.	• Amazon Redshift of a petabyte-scale. • Amazon RDS, DB Instance replication. • Oracle Data masking and sub-setting.
Escalation of data resources e.g. (SQL Server) [3] [10]	AC-2,3,5,4 S1-2,3,4,6,7 SI-11,10 CM-6.	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	AIS-03	1. Organizations need to break up large operations into batches. 2. Organization should create error messages that provide the information required for corrective measures without disclosing information that could be exploited 3. Transactions must be kept shorter. 4. The lock footprint of expensive queries must be reduced by performance tuning and making them efficient.	• Oracle multitenant edition, service administrator.

V. CONCLUSION

The growth of cloud database platforms such as database as a service (DBaaS) supports the provision of big data services. DBaaS services provide cloud customers with the opportunity to outsource their database for more reliability, fault tolerance, scalability, availability, confidentiality and integrity. However, no detailed research has been done to carefully cover the security aspects of DBaaS. Despites, numerous approaches have been introduced to resolve this issue like distributed sharing algorithm, the security risk mitigation mechanisms should be improved, developed and tested to make DBaaS more comprehensive, mature, realistic and reliable. This paper has identified some security and privacy issues such as data confidentiality, availability, integrity and privacy which were deeply rooted from the existing related papers and presented with consequences and STRIDE model to create an appropriate solution. The key objective of this paper is to put standard measures in place to further reduce issues related to security and privacy by creating a guideline from best practices and security controls. The identified issues are mapped with security requirement principle to highlight its significance to a system's security. In addition, the related framework, standards and guidelines were mapped with the identified issues to serve as a core security guideline for the reliability of DBaaS cloud platform and to improve it wide-scale use.

REFERENCES

[1] Manar Abourezq, Abdellah Idrissi, "Database-as-a-Service for Big Data: An Overview," *International Journal of Advanced Computer Science and Applications*, vol. 7, pp. 1, 2016.

[2] Faria Mehak, Rahat Masood, Yumna Ghazi, Awais Shibli and Sharifullah Khan, "Security Aspects of Database as a Service in cloud computing," *Springer*, pp. 297-324,2015.

[3] Shweta Dinesh, Bijwe et al "Database in Cloud Computing-Database-as-a-Service (DBaaS)with its Challenges," *International Journal of Computer Science and Mobile Computing*, vol 4, issue. 2, pp. 73-79,2015.

[4] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," Natl. Inst. Stand. Technol. Spec. Publ. 800-53 Revision. 5, 2017.

[5] X. Zheng, "Database as a Service – Current Issues and It is Future," *arXiv preprint arXiv:1804.00465*, 2018. Available: 10.1145/1235 [Accessed 4 November 2019].

[6] Muntjir M and Haque M "Cloud Database Infrastructure: Database System Transference in Cloud Computing Management and Security," International *Journal of Computer Trends and Technology*, vol. 47, no. 1, pp. 16-28, 2017. Available: 10.14445/22312803/ijctt-v47p103.

[7] Reddy M, "Big Data and Current Cloud Computing Issues and Challenges," *International Journal of Engineering and Computer Science*, 2016. Available: 10.18535/ijecs/v5i4.30.

[8] Ahmed M and Litchfield A, "Taxonomy for Identification of Security Issues in Cloud Computing Environments," *Journal of Computer Information Systems*, vol. 58, no. 1, pp. 79-88, 2016. Available: 10.1080/08874417.2016.1192520.

[9] Kashif Munir and Lawan A. Mohammed, "Authentication Scheme for Database as a Service (DBaaS) Solutions," *International Journal on Cloud Computing: Services and Architecture*, vol. 8, no. 12345, pp. 11-22, 2018. Available: 10.5121/ijccsa.2018.8502.

[10] CSA, "The security guide V4.0 White Paper," *Cloud Security Alliance (CSA*), 2017. [Online]. Available: https://cloudsecurityalliance.org/download/security-guidance-v4/ [Accessed: 2019].

[11] Oracle, "Database as a Service (DBaaS): Use Cases and Adoption Patterns," *451 Research, 2016*, [Online]. Available: http://www.oracle.com/us/products/database/451-report-dbaas-3038788.pdf [Accessed: November 2019].

[12] Oracle, "Security and the Oracle Database Cloud Service," *An Oracle White Paper*, November 2016[online] Available: https://www.oracle.com/assets/oracle-inf-cloud-security-wp-3840537.pdf , [Access: October 2019].

[13] Microsoft Azure, "An overview of Azure SQL Database security capabilities," *Microsoft article document*, [Online] Available: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview, [Access: May 13, 2019].

[14] Waleed Al Shehri, "Cloud Database: Database as a Service," *International Journal of Database Management Systems*, Vol.5, No.2, April 2013.Available: 10.5121/ijdms.2013.5201[25] NIST SP 800-36, "Guideline for Media Sanitization," Guide *to Selecting Information Technology Security Products*, Vol.5, No.2, pp-66[Accessed October 2019].

[15] ISO/IEC, "Information technology – Security techniques –Information security management systems," – Requirements. ISO/IEC 27002 (2013)", *International Organization for Standardization International Electrotechnical Commission*, [online] Available: https://iso.org/download/, [Access: October 2019].

[16] CSA, "Cloud Computing Vulnerability Incidents: A Statistical Overview Report," *Cloud Security Alliance (CSA), 2013*. [Online]. Available: https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/. [Accessed: October 2019].

[17] CSA, "The Cloud Control Matrix V3.0.1 White Paper," Cloud Security Alliance (CSA), 22 August 2014 [Online], Available: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1. [Accessed: October 2019].

[18] International Organization for Standardization (ISO), "International Electrotechnical Commission (IEC): Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC 27001", Available

[19] Dinesh Rajase kharan, "Defense-in-Depth for Cloud Databases-Unifying Cloud and On-Premises Database Security," *Oracle White Paper*, March 2016 [Online], Available: https://www.oracle.com/technetwork/database/security/wp-security-dbsec-cloud-3225125.pdf [Accessed: November 2019].

[20] Amazon AWS, "Overview of AWS Security - Database Services," *Amazon White Paper*, June 2016 [online], Available: http://aws.amazon.com/security/, [Access: November 2019].

[21] Izang A. A, Adebayo A.O., Okoro O.J. & Taiwo O.O., "Security And Ethical Issues To Cloud Database," *The Journal Of Computer Science And Its Applications,* Vol. 24, No. 2, 2017.

[22] Mykletun E. and Tsudik, "Aggregation Queries in the Database-As-a-Service Model," pp. 89–103, 2006.

[23] Gwan-Hwan Hwang and Shih-Kai Fu, "Proof of Violation for Trust and Accountability of Cloud Database Systems," *IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing,* pp. 425-433, 2016.

[24] Junggab Son; Donghyun kim; MdZakirul Alam Bhuiyan; and Rahman Tashakkori; Jungtaek Seo and Dong Hoon Lee, "Privacy enhanced location sharing for mobile online social networks," *IEEE Transactions on Sustainable Computing*, pp 1-1, 01 June 2018.

[25] Jianfeng Wang Xiaofeng Chen, "Efficient and Secure Storage for Outsourced Data: A Survey," Data Science and Engineering, Available: https//www.springler.com/DOI 10.1007/s41019-016-0018-9, vol 1, no 3, pp 178-188, 2016.

[26] Ajeet Ram Pathak1, B. Padmavathi, "Analysis of Security Techniques Applied in Database Outsourcing*", International Journal of Computer Science and Information Technologies,* Vol. 5 (1), 665-670, 2014

APPENDIX

NO	ISSUES	ISSUES EXPLANATION	CONSEQUENCES	SECURITY CATEGORIES	THREAT TYPE(STRIDE)
4	Lack of Interoperability [2]	• The need to render and transform standards to have interoperability standards driven by native databases and when two or more systems or components to communicate are not functioning to extract and share data.	• Communication between multiple heterogeneous databases maybe be lost • There will be lock down of communication causing Unavailability of data.	• Confidentiality • Authorization	• Elevation of Privilege • Information Disclosure. • Repudiation
5	Query and Transactional Workloads [7][5][22][24]	• The number of potential users who simultaneously query a Cloud-based database is a variable in the query workload; therefore, estimating the time required for query workloads is a challenge.	• Lack of systems management because the number of users querying database is unknown • Time estimation in the workload query cannot be possible.	• Integrity, • Authentication	• Tampering • Spoofing
6	Vendor lock-in [2]	• DBaaS-used APIs are proprietary and are not subject to successful standardization; the application lock-in problems occur as a result. • The free transfer from one provider to another, to reuse their essential and redundant data across portable applications allowing components written for one DBaaS provider to operate on another DBaaS provider.	• The transferring of data between vendors is not considered • The data reusability is not guaranteed across portable applications. • Customers can't move data from one site to another. • Failure of one vendor's services will lead to total data loss. • Need a standard API to operate under the infrastructure of any provider	• Availability • Integrity	• Tampering • Denial of services
7	Middleware muddles [24][7]	• Middleware provides the possibility to create or incorporate client applications independently of the server applications in a client / server environment. • This allows elements of applications to interoperate across network links despite the differences in underlying system architectures, communications protocols and other application services. with this, developers required authentication, authorization and encryption to build in security.	• Secure implementation of queries leads to only allow unauthorized persons to access data in an encrypted format.	• Availability, Integrity and Authentication.	• Denial of services. • Spoofing

8	Data Provenance [2][9]	• This is referring to the method of identifying and documenting the origin of the data and its movement between the databases.	• Cloud-hosted databases are more resistant to performance attacks because of their inherent agility. • The provenance of sensitive data may expose some private information. • Intensive computations involved in getting the required history from the providence metadata. • An Adversary can forge data provenance from existing source data using fake data.	• Integrity • Confidentiality	• Tampering • Information Disclosure • Repudiation
9	Supply Chain Failure [2][7][5][9]	Database tasks or all of their supply chain management functions to third parties. Therefore, their level of security in such situations may depend upon the security of these third-party links. Lack of transparency in the contract can be the root cause of problems	• Failure to properly manage cloud access can lead to serious IT risks, Including providing users with excess privilege or worse still leave cloud storage repositories open and accessible to anyone.	• Confidentiality • Integrity	• Information Disclosure • Tampering
10	Escalation of data resources [3] [10]	• The capability of Database to handle the demand of removing/adding of resources to improve availability and performance especially when changes are unpredictable. but realizing such gains requires reconfiguration and downtime.	• Automatic scaling of data cause confidentiality and availability issues	• Confidentiality • Availability • Authentication	• Information Disclosure • Denial of Service. • Spoofing
11	Illegal Recovery of Data from Storage Devices [2]	• Threats on this replicated data, stored on multiple locations are possible since data sanitization has several techniques that can recover data that has not been properly discarded from the hard drives, might introduce physical and logical security risks.	• Degaussing, destruction and overwriting of data can be performed to cause data leakages. • Data could be recovered by malicious sources when it is not properly discarded. (media sanitization)	• Integrity, • Confidentiality	• Tampering • Information Disclosure

12	Synchronization of Replication [2][8]	• This method is to maximize the degree of concurrency in replication and reduce the possibility of transaction rollback but during the process, an error can occur which might lead to the total stop of the transaction and open it for the internal malicious.	• Replications between multiple servers' cause miss management as well as consistency issues	• Confidentiality • Authentication • Availability	• Information disclosure • Spoofing
13	Network Breaches [5][7][2]	• Communicating data over the network makes it prone certain threats such as data modification and eavesdropping and any weakness at the network level will allow malicious users such that they can exploit data.	• Data flowing over the network (internet) is prone to hazardous circumstances and network performance issues • Possible network failure reasons are misconfiguration. • lack of resource isolations, poor or untested • Business continuity, disaster recovery • plan, network traffic modification	• Confidentiality, Integrity and Availability, Authentication and Authorization.	• Tampering • Information disclosure • Denial of Service • Spoofing • Elevation of privileged • Repudiation
	Jurisdiction Differences [7][2]	• Outsourced data in the Cloud DBaaS are stored at various location and thus, high risk and restrictions are faced when customer data is subjected to multiple jurisdictions	• Risks and restrictions faced when the customer's data is subjected to multiple country's legal jurisdictions. • Data in this situation is accessible by multiple parties	• Integrity Privacy • Authorization	• Elevation of Privilege • Tampering
	Data Locality Raising Obligation Issues [2][9]	• DBaaS service providers deal with privacy issues where the contracts with their cloud clients require them to protect private information. Therefore, data locality remains unknown to clients.	• Compliance and data-security privacy laws prohibit the movement of sensitive data among countries. • Issues faced when no one takes the responsibility of data in location independent data storage.	• Privacy Integrity and Authentication • Non-repudiation	• Tampering • Spoofing • Repudiation

APPENDIX 1: LIST OF THE IDENTIFIED SECRUITY AND PRIVACY ISSUES IN DBAAS

IDENTIFIED ISSUES	NIST 800-53 R5	ISO 27001:2013	CSA/CCM V3.0.1	CONTROL DESCRIPTIONS	VENDORs SOLUTIONS
Lack of Interoperability [2]	MA-6 SC-29 SC-28 SC-27 SC-8 AC-18 AU-10	Clause 6.1.1 A.6.1.2	IPY-02 IPY-04 IPY-03	1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access. e.g. information security roles and responsibilities, segregation of duties. 2. The provider should use secure standardized network protocols for the import and export of data and manage the service and make available a document to consumers (tenants) detailing with the relevant interoperability and portability standards that are involved. 3. Provider should consider Digital signatures, Timestamps, Encryption and Protect secrets	• RESTful Web service Security (Oracle DB). • (Oracle DB) Session state protection.
Query and Transactional Workloads [7][5][22][24]	RA-5 AC-2, 6,10,14 PM-23 AU-8 AU-14 IA-1 MA-1, 2 SC-39 CM-7	A.9.2.6-4-5 A.9.4.1-2 A.9.1.1-2 A.9.2.2-1-4-5 A.12.1.2 A.11.2.5	IAM-12 IAM-02 DCS-08	1. Security perimeters should be defined and used to protect areas containing either sensitive or critical information and information processing facilities. i.e. Protect Secrets. 2. Access to systems and applications should be controlled by a secure log-on procedure. 3. A suitable authentication technique to prove a user's claimed identity should be adopted. 4. Provide and incorporate the ability to pick a user session to capture record, or view catch for registered users.	• Oracle Cloud Identity and access management. • Oracle multifactor access control. • Azure Access management database authentication. • Azure role level Security. • Amazon Rational database security access Control • Amazon Redshift.
Vendor lock-in [2]	PE-1,4,13 IR-3(2) ,9 MA-2 MA-3(1,2,3) MA-4 MA-6 MA-5	A.11.2.2 A.11.2.4 A.11.2.3	BCR-03 BCR-07	1. An organization should adopt the use of the latest and greatest technology to keep the company moving ahead and being able to iterate quickly to keeps them ahead of the pack. 2. The agile process is important to be focused to make use of the next technology to avoid vendor lock-in trap. i.e. to keep quality of service. 3. Equipment should be secured against power failures and other disturbances caused by service support failures	• Microsoft Azure RDS. • Amazon Rational database services
Data Provenance [2][9]	SC-31,8,7 SC-28,28(1) SC-26 SC-13 PE-19 IR-9 AC-1,2,3,5,6, AC-6 (10),18(1) SI- 2,3(1,2),4(2,3,5) SI-6,7, 8,10, 11.	A.11.1.4 A.11.2.1 A.10.9.2-3 A.12.2.1-2-3-4 A.12.6.1 A.15.2.1 A.13.1.1 A.14.1.3-2 A.18.1.3-4 A.8.3.3 A.10.1.1	AIS-03 BCR-05 BCR-06 IVS-01 EKm-03	1. Components within organizational systems should be included and specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks. 2. System should be protected from information leakage due to electromagnetic signals emanations. 3. Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. 4. Implementation of cryptographic mechanisms to avoid unauthorized knowledge disclosure and alteration when at rest must be adopted. 5. Both the query and its reply must be encrypted to ensure confidentiality on the communication channel.	• SSL (Secure Socket Layer) • Transparent Data Encryption (TDE) • Azure Key Vault and dynamic data masking. • Oracle DB Fine-grained and unified auditing

Middleware muddles [24][7]	SA-17 SA-21 AC-6 AC-3 AU-2 SA-25 SC-27 SI-10 CM-1-10	A.9.4.4 A.9.4.1-2 A.12.5.1 A.12.2.1 A.6.1.2 A.14.2.4	CCC-04	• The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. • Detection, prevention and recovery controls to protect against malware should be implemented and combined with appropriate user awareness. • Implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting). • The use of utility programmed that could bypass system and application controls should be restricted and strictly controlled.	• Oracle DB Application Express. • Threat Protection. (Oracle Defense in depth) • Amazon RDS instance • RESTful Web Service
Supply Chain Failure [2][7][5][9]	SA-12 SA-7 SA-10 PM-31 PM-9 CP-3,6,7,8 MP-5 CA-3 PS-7 Si-7 SC-7	A.6.1.1 A.15.1.2 A.13.1.2 A.10.6.2	STA-01-09	• Organizations must be ensured to Develop a plan for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; • Implement the supply chain risk management plan consistently across the organization. • Regular review and update of the supply chain risk management plan or as required to address organizational changes • Providers shall audit, account for and collaborate with their cloud supply chain partners to correct defects in data quality and related risks. • • Providers shall develop and enforce data protection risk reduction and controls through proper division of duties, role-based access and low-privilege access for all workers within their supply chain. • Customers should establish an alternate storage site including necessary agreements to permit the storage and retrieval of system backup information.	
Illegal Recovery of Data from Storage Devices [2]	MA-1 MA-2 PE-16,1 SC-39 MP-6,7 CP-10 AC-18,1 4 SC-28 SC-23 SC-13 SC-8 SC-7 IA-7 SI-8	A.11.2.5-7 A.13.1.1 A.8.3.3-2 A.13.2.3 A.14.1.3 A.10.1.1 A.18.1.3 A.18.1.4	DCS-08 EKM-03 DSI-07	• Customers should properly employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. • Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries. • employees and external party users who have authority to permit off-site removal of assets should be identified. • Provide for the recovery and reconstitution of the system to a known state after a disruption, compromise, or failure within.	• Amazon RDS. • Oracle Multitenant Edition.
Synchronization of Replication [2][8]	SA-18 AU-1 AU-7 (1) AU-8	A.12.4.1 A.12.4.4	IVS-03	• The synchronization process must contain timestamp information and modifier information to be used to determine whether information must be extracted from server database table. • Also, to indicate if the table has been updated since the last synchronization by a given client or not. • A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	

Network Breaches [5][7][2]	SC-7 SC-11 CM-7,3,4 CA-9,8 AC-4 CA-3 SC-3 SI-1 RA-5 SA-11	A.13.1.1 A.13.1.2 A.14.1.2 A.12.4.1 A.12.1.4 A.12.6.1. A.9.1.2 A.13.1.3 A.18.1.4 A.14.2.2.3	IVS-06 IVS-07 IVS-11 IVS-12 TVM-02	• Monitor and control communications at the external boundary of the system and at key internal boundaries within the system. • Implement subnetworks for publicly accessible system components that are separated from internal organizational networks. • Provide a isolated trusted communications path for communications between the user and the trusted components of the system. • Configure the system to provide only essential capabilities; and prohibit or restrict the use of the following functions, ports, protocols, and/or services • Security mechanisms, service levels and management requirements of all network services should be • identified and included in network services agreements, whether these services are provided in-house or outsource	• Azure Virtual network traffic origin and network, firewalls. • Amazon network access control. • Amazon encrypted IPsec VPN. • SSL (Secure Socket Layer) • Transparent Data Encryption (TDE
Jurisdiction Differences [7][2]	AC-4 AC-1 SC-1 SC-8 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 SA-4	A13.2.1,2 A.9.1.1 A.9.4.1 A10.1.1 A.18.1.4 A.8.2.1 A.18.1.1-3 Clause 4.2-4 5.2-2 6.1.2-3 7.5.3 8.1-3 9.2-3 10.2	AAC-03 AIS-06 IVA-04	• Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable • Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	
Data Locality Raising Obligation Issues [2][9]	SA-4,5,8,9 SA-10,18 CM-5 CM-7,8,9,10 SI-1 SI-3,4,7 MP-7 PE--16	A18.2.1 A.15.1.2 A.12.1.4 A.14.2.9 A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 A.12.6.1 A.16.13 A.18.2.2 A.18.2.3	CCO-02 CCO-04 DCS-01 DCS-07 IVS-04	• Organization should implement malicious code security mechanisms for the identification and eradication of malicious code at device entry and exit points; • An organization policy on programmed and information integrity should address intent, scope, functions, responsibilities, management commitment, collaboration between organizations and compliance; • Organization policy should comply with relevant laws, executive orders, instructions, regulations, rules, standards and guidelines associated with each providers locality.	

APPENDIX 2: DBAAS SECURITY AN D PRIVACY ISSUES MAPPED TO RELEVANT CONTROLS AND VENDOR'S SOLUTIONS

			ORACLE CLOUD DB			MICROSOFT AZURE			AMAZON AWS		
	IDENTIFIED ISSUES	**VENDORS PROVIDED SOLUTIONS**	**C**	**I**	**A**	**C**	**I**	**A**	**C**	**I**	**A**
1	Resource Allocation for Multiple Tenants: Multi-Tenancy [3] [8] [10] [12]	• Oracle Database Vault. • Azure Key Vault and Dynamic data masking. • Azure Row level Security.	✓	✓		✓	✓				
2	Resource Exhaustion [3] [12]	• Amazon Redshift of a petabyte-scale. • Amazon RDS, DB Instance replication. • Oracle Data masking and sub-setting			✓			✓			✓
3	Escalation of data resources e.g. (SQL Server) [3] [10]	• Amazon Redshift of a petabyte-scale. • Amazon RDS, DB Instance replication. • Oracle Data masking and sub-setting	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	Lack of Interoperability [2]	• RESTful Web service Security (Oracle DB). • (Oracle DB) Session state protection	✓								
5	Query and Transactional Workloads [7][5][22][24]	• Oracle Cloud Identity and access management. • Oracle multifactor access control. • Azure Access management database authentication. • Azure role level Security. • Amazon Rational database security access Control • Amazon Redshift		✓			✓			✓	
6	Vendor lock-in [2]	• Microsoft Azure RDS. • Amazon Rational database services					✓	✓		✓	✓
7	Middleware muddles [24][7]	• Oracle DB Application Express. • Threat Protection. (Oracle Defense in depth) • Amazon RDS instance • RESTful Web Service		✓	✓		✓	✓		✓	✓

8	Data Provenance [2][9]	• SSL (Secure Socket Layer) • Transparent Data Encryption (TDE) • Azure Key Vault and dynamic data masking. • Oracle DB Fine-grained and unified auditing	✓	✓		✓	✓		✓	✓	
9	Supply Chain Failure [2][7][5][9]										
10	Illegal Recovery of Data from Storage Devices [2]	• Amazon RDS. • Oracle Multitenant Edition.	✓	✓		✓	✓				
11	Synchronization of Replication [2][8]										
12	Network Breaches [5][7][2]	• Azure Virtual network traffic origin and network, firewalls. • Amazon network access control. • Amazon encrypted IPsec VPN				✓	✓	✓	✓	✓	✓
13	Jurisdiction Differences [7][2]										
14	Data Locality Raising Obligation Issues [2][9]										

APPENDIX 3: SUMMARY OF THE VENDORS PROVIDED SOLUTIONS PRIVACY AND SECUIRT