Information Security and Risk Assessment

Project: IBM Cloud

TA: Alaa Prince

Team Members:

Makarious Magdy Azmy: 20231700340

Kerolos Ayman Ebrahim: 20231700329

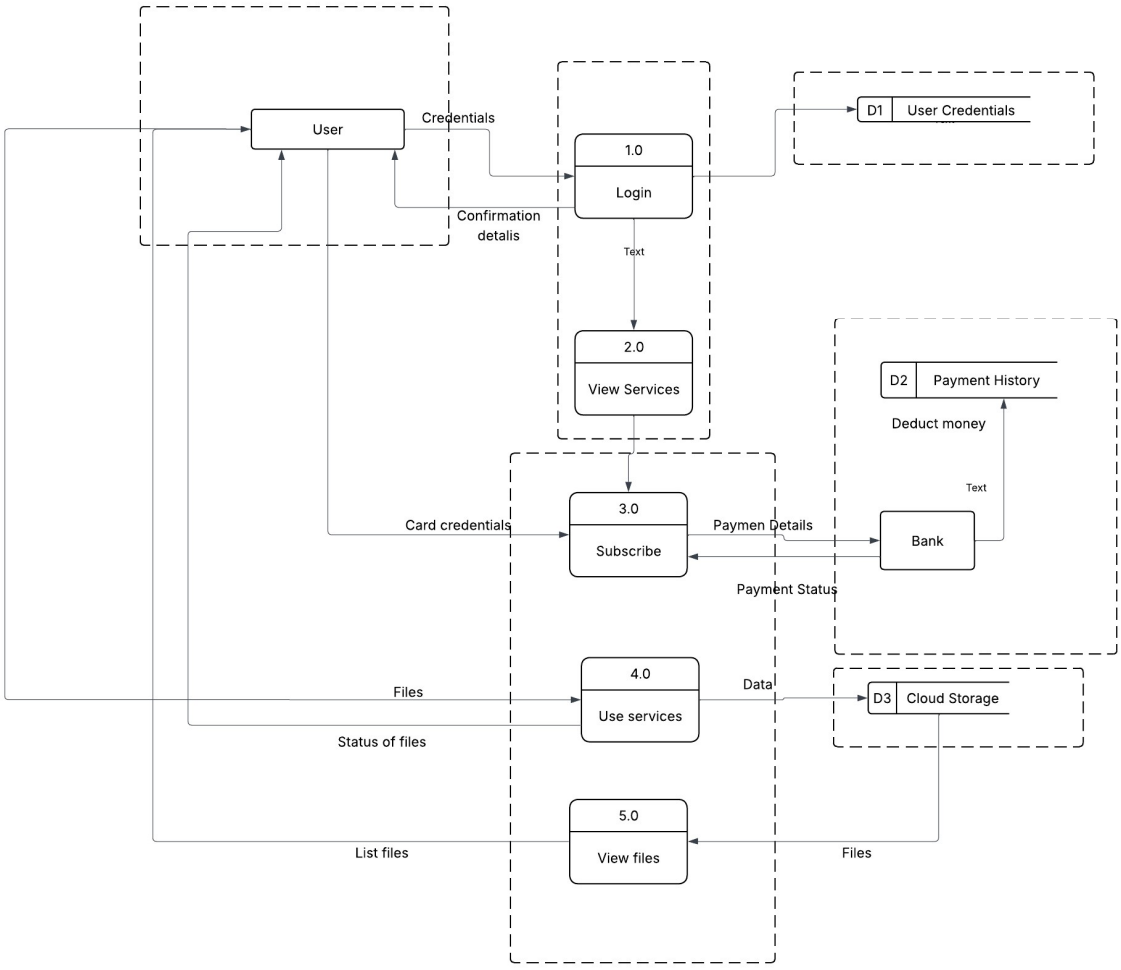
Yara Tamer Kamel: 20231700343

Joy Ashaf Drehem: 20231700217

Rinad Osama Mahmoud: 20231700222

Executive Risk Brief:

IBM Cloud is a cloud platform that helps organizations run and manage their applications and data over the internet. It provides services such as computing, storage, networking, and integration tools that allow systems to work together. IBM Cloud is often used for enterprise and business applications because it focuses on security, reliability, and support for hybrid cloud environments.



Data Flow Diagram (DFD) Description

The Data Flow Diagram illustrates the main interactions between the user, IBM Cloud services, external systems, and internal data stores.

- Initially, the user registers or logs into the system by providing credentials, which are processed by the login function and securely stored in the **User Credentials data store (D1)**. At this stage, the user operates with **lower privileges**, allowing them to view available IBM Cloud services without accessing restricted features.
- When the user chooses to subscribe to a service, they provide payment details that are sent to an external **Bank system**. The bank processes the payment and returns the payment status to the system. Both the bank and its payment data store (**Payment History – D2**) are considered **outside the scope of IBM Cloud**, as payment processing is handled by a third-party entity.
- Once the payment is successfully approved, the user is granted **higher privileges**, enabling access to subscribed services. The user can then use cloud services such as uploading, managing, and viewing files.

- All user data and service-related files are stored in **Cloud Storage (D3)**. Authorized users can retrieve, edit, and manage their stored files through the system, depending on their access level.

Real Life assts and what they do

- **User / Browser**
  Allows users to access IBM Cloud services, view available options, and interact with the system.
- **IBM DataPower Gateway**
  Acts as a gateway that securely connects users and external systems to IBM Cloud services.
- **Web Server & WebSphere Application Server**
  Hosts and runs the main applications that provide IBM Cloud services to users.
- **IBM Cloud Pak for Integration**
  Connects different services and systems together and manages the flow of data between them.
- **Payment Gateway / Payment API**
  Handles payment requests and communicates with the bank to approve or reject transactions.
- **Bank (External System)**
  Processes payments and manages financial transactions outside of IBM Cloud.
- **Cloud Logging and Monitoring**
  Records system activities and helps track usage and system behavior.
- **Object Storage (Cloud Storage)**
  Stores user files and service data so they can be accessed when needed.
- **Virtual Private Cloud (VPC)**
  Provides a private cloud environment where services run in an isolated and controlled space.
- **IBM PureApplication**
  Hosts and manages enterprise applications in a controlled and reliable environment
- **IAM Database**
  Centralized data store that maintains user identities, credentials, roles, permissions, tokens, and policy relationships used to make authentication and authorization decisions across systems.

Risks based on the assets

1."Connector" IBM Cloud Pak: THE DIGITAL NERVOUS SYSTEM

The Business Role

- Ensure that when a customer places an order, the warehouse knows how to ship it, and finance knows how to bill it. It connects to all applications.

The Risk

- Vulnerabilities allow attackers to "cross the wires," stealing sessions or injecting scripts.

BOTTOM LINE: Operational Paralysis. Business units stop communicating; orders fail

2."Engine"WebSphere App Server: The Powerplant

The Business Role

- The heavy-duty engine runs our main websites and mission-critical services.

The Risk

- Java flaws act like "leaving keys in the ignition," allowing full remote-control hijack.

BOTTOM LINE: Total Takeover. Attackers can crash into storefronts or delete essential files.

3."Library" Infosphere: The Source of Truth

The Business Role

- Central Archive for trusted business data, organized for decision-making.

The Risk

- SQL Injection can "poison the well," altering financial figures or deleting databases.

BOTTOM LINE: Data Poisoning. Strategic errors based on false data and GDPR/PCI fines.

4. The "Safe Deposit Box"Cloud VPC: The Secure Vault

The Business Role

- Store critical files, backups, and private workloads.

The Risk

- "Broken locks" allow bypass via skeleton keys. Attackers can break walls, separating data.

BOTTOM LINE: Ransomware. Attackers can encrypt backups, forcing payment.

5. The "Alarm System “Tivoli & Monitoring: The Security Cameras

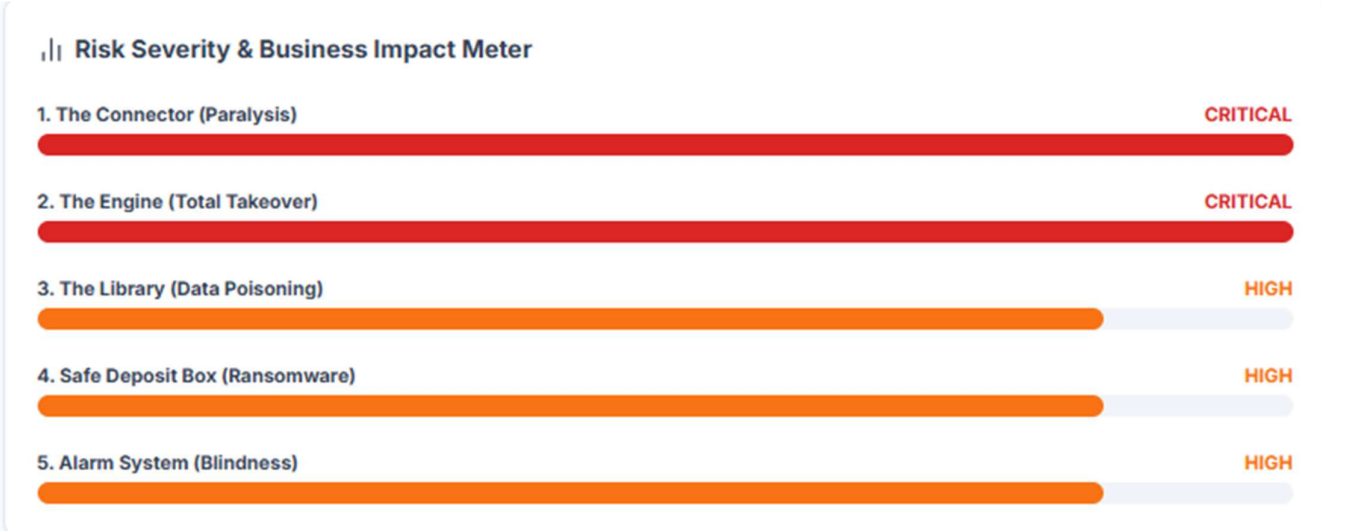
The Business Role

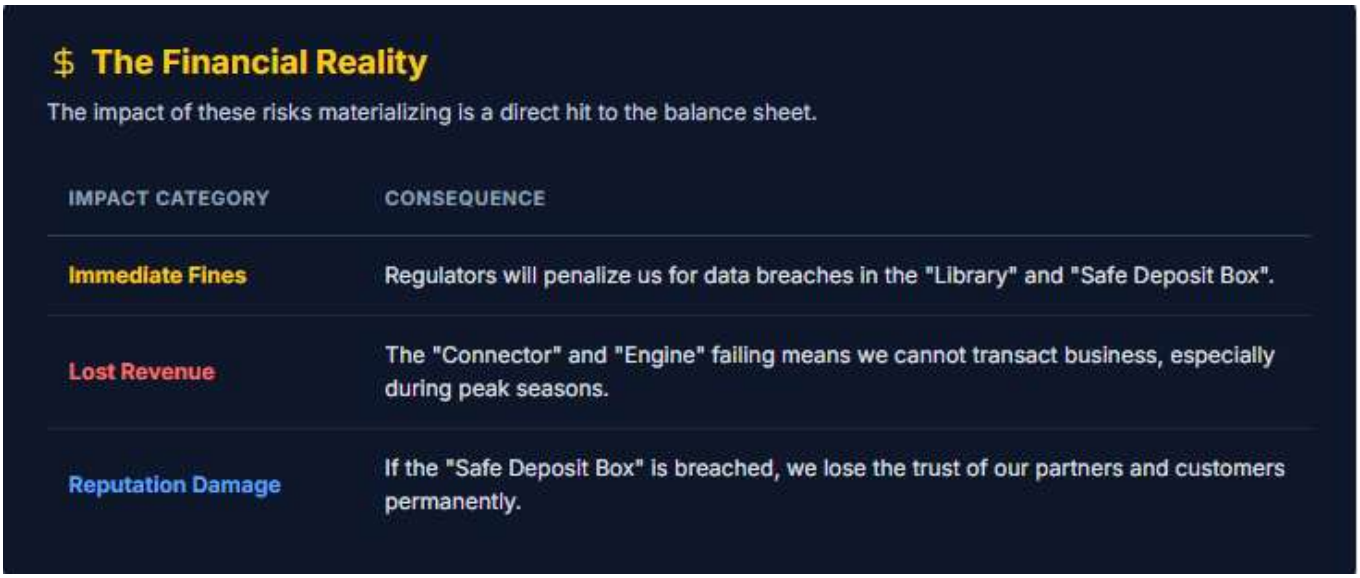
- Watches network 24/7 to detect hackers and provide forensic evidence.

The Risk

- Attackers can turn off alarms or delete logs to hide their tracks.

BOTTOM LINE: Flying Blind. Active attacks (money/data theft) occur without detection.





Financial Impact on IBM During Seasonal Peaks

During the holiday season, IBM Cloud Pak for Integration handles a higher volume of data exchanges and transactions because many business processes and customer activities increase. As a result, any attack or outage would affect more transactions, more connected applications, and more users in a shorter period. This amplifies the business impact of disruptions or data exposure, since failures during peak usage can lead to delayed operations, lost revenue, and cascading issues across dependent systems.

Regulatory and Business Risk Context for IBM Cloud Assets

IBM Cloud operates in a highly regulated environment and must comply with global data protection laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These regulations apply whenever personal or sensitive business data is accessed, processed, or stored within IBM Cloud services. Violations can result in severe financial penalties, including fines of up to 4% of annual global revenue under GDPR and up to $7,500 per violation under CCPA, in addition to reputational damage and loss of customer trust.

Based On OSINT Findings

OSINT analysis indicates that IBM Cloud's internet-facing infrastructure is generally well secured, with limited direct exposure. However, credential leakage remains a key risk, as email addresses and passwords may appear in public breach of data or underground sources, particularly through third-party compromises.

Additionally, supply chain and legacy infrastructure risks exist. Historical exposure of SoftLayer-related IP ranges highlights the need for continuous monitoring of acquired or partner environments.

Finally, default credentials represent a critical weakness and must be eliminated through enforced secure configuration baselines and strong identity controls.