**CIA Traid**

For you to be able to do these things, several controls must be in place to ensure that you have the proper authorization to perform them (confidentiality), that the numbers are accurate (integrity), and that the system is up and running so they can service your request (availability). For this assignment, use the CIA triad to answer the following questions:

1. Name some ways the bank ensures that your information remains confidential (Example: PIN code).

* measures for multi-factor authentication. The usage of two or three different authentication factors is required for multi-factor authentication, which can take many various forms. The bank login page, for instance, should ask you for a second authentication when you input a password or PIN to log in, typically in the form of a text message, phone call, or email notification.
* Credential confidentiality. Banks never reveal usernames or passwords to third parties.
* using biometric identification. The mobile banking apps of several banks now include fingerprint authentication. The verification of eye prints, as well as facial and voice recognition, are further biometric security measures.
* Password. A strong password often consists of a combination of letters, numbers, and characters. A password is a string that is only known by the users.

2. What principle in the CIA triad is applicable in the example of a bank ensuring that the customer information is accurate and reliable? What technical controls can be implemented to enforce this principle? (Example: Hashing)

* Encryption. Online transactions and personal data are protected by banks employing encryption software, which turns the data into a code that only your bank can decipher.
* Firewalls. Computer network firewalls filter data entering and leaving the network, preventing unwanted access and halting traffic from dubious internet sources.
* SSL, or Secure Sockets Layer, encryption. When logging in, completing an application, etc., the browser and computer are connected securely thanks to SSL encryption. Data integrity will be maintained throughout the transport thanks to SSL encryption.
* Automatic Logout. To help stop anyone from accessing or using their online accounts, banks also automatically log out clients from your secure connection after a certain amount of inactivity.

3. Name some ways the bank ensures that you can get to your information and/or execute transactions whenever you want (Example: load balancing/fault tolerance).

* Redundancy: Having redundant data, or, in other words, having numerous sources of the data available, may be the greatest strategy to increase data availability. In this way, the availability of your data won't be affected if one of the disks, servers, or databases hosting it fails.
* Automate failover: With automated failover, your data will be automatically replaced in the event of a disaster or infrastructure failure.
* Prevent single points of failure: By ensuring that not all company data is routed through a single point (server, router), you can rest assured that even if the single point fails, the infrastructure and application components will continue to operate correctly.

4. How do these three principles work together? Can you think of any situations where one of these could be considered more important than the other two?

* The three principles combine to provide a system of guiding principles that may be used by any company. Well, there isn't a circumstance that comes to me where one of the principles would be more important than the other. Every one of the three elements confidentiality, integrity, and availability is provided by an efficient and secure system. A lack of any one of the CIA triad's three components makes an information security system weak.