Unit-4
Computer-Based Controls

The different forms of countermeasure to threats on computer systems range from physical controls to managerial procedures. In spite of the range of computer-based controls that are preexisting, it is worth noting that, usually, the security of a DBMS is merely as good as that of the operating system, due to the close association among them.

Most of the computer-based database security are listed below:

- Access authorization.
- Access controls.
- Views.
- Backup and recovery of data.
- Data integrity.
- Encryption of data.
- RAID technology.

What is Access Controls?

The usual way of supplying access controls to a database system is dependent on the granting and revoking of privileges within the database. A privilege allows a user to create or access some database object or to run some specific DBMS utilities. Privileges are granted users to achieve the tasks required for those jobs.

The database provides various types of access controls:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Backup and Recovery

Every Database Management System should offer backup facilities to help with the recovery of a database after a failure. It is always suitable to make backup copies of the database and log files at the regular period and for ensuring that the copies are in a secure location. In the event of a failure that renders the database unusable, the backup copy and the details captured in the log file are used to restore the database to the latest possible consistent state.

Integrity Controls

Integrity controls are designed to manage the *integrity* of data, which is a fundamental component of information security. In its broadest use, “data *integrity*” refers to the accuracy and consistency of data stored in a database, data warehouse, data mart, or other construct.

Integrity controls are an integral part of applications, helping to enforce an organization’s data integrity goals. They can be used to prevent semantic user errors, to protect against unauthorized changes in software code, to help prevent vulnerabilities, and to stop malicious code from entering a system.

Integrity controls apply rules that verify the database and database operations, ensuring that data is not corrupted by applying integrity control features that are informed by business processes, computer edits, and other types of security infrastructure.

What is Data Integrity?

Data integrity refers to the reliability and trustworthiness of data throughout its lifecycle. It can describe the state of your data—e.g., valid or invalid—or the process of ensuring and preserving the validity and accuracy of data. Error checking and validation, for example, are common methods for ensuring data integrity as part of a process.

What is the Difference Between Data Integrity and Data Security?

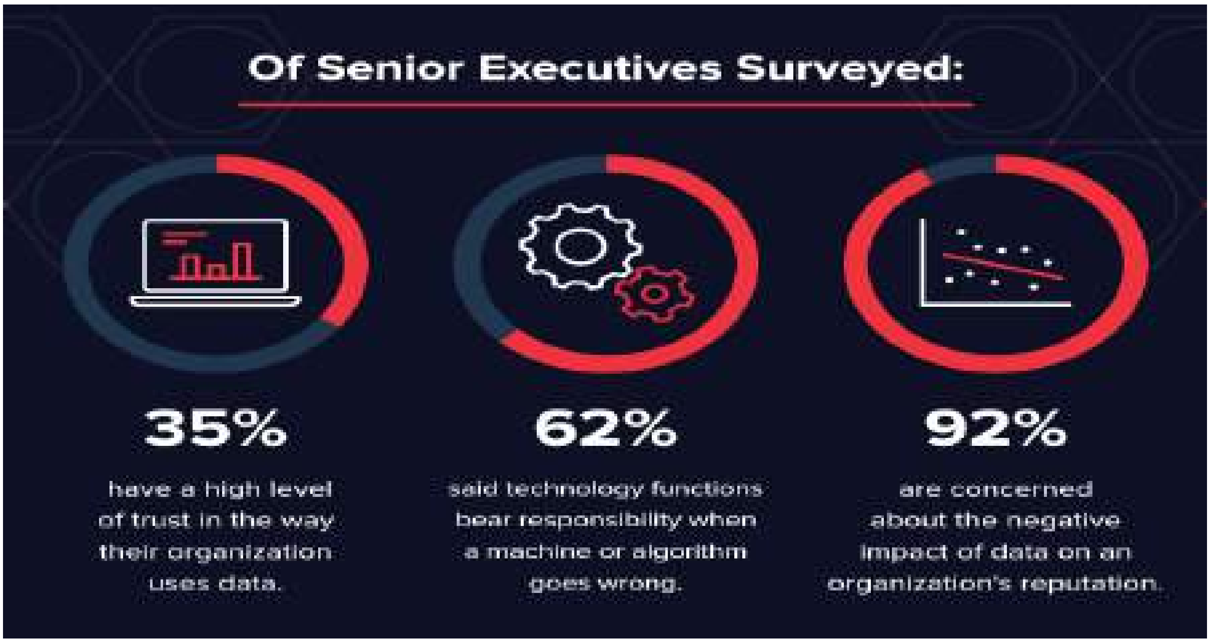
Data integrity is not to be confused with data security. Data security refers to the protection of data, while data integrity refers to the trustworthiness of data.

Data security focuses on how to minimize the risk of leaking intellectual property, business documents, healthcare data, emails, trade secrets, and more. Some data security tactics include permissions management, data classification, identity and access management, threat detection, and security analytics.

Why is it Important to Maintain Data Integrity?

Imagine making an extremely important business decision hinging on data that is entirely, or even partially, inaccurate. Organizations routinely make data-driven business decisions, and data without integrity, those decisions can have a dramatic effect on the company’s bottom line goals.

A new report from KPMG International reveals that a large majority of senior executives don’t have a high level of trust in the way their organization uses data, analytics, or AI.



Only 35% say they have a high level of trust in the way their organization uses data and analytics. 92% are concerned about the negative impact of data and analytics on an organization’s reputation. What’s more, 62% of senior executives said technology functions, not the C-level and functional areas, bear responsibility when a machine or an algorithm goes wrong.

Organizations need to go through the motions of preserving data integrity in order for C-level executives to make proper business decisions.

Data Integrity Threats

Data integrity can be compromised through human error or, worse yet, through malicious acts. Data that’s accidentally altered during the transfer from one device to another, for example, can be compromised, or even destroyed by hackers. Common threats that can alter the state of data integrity include:

- Human error
- Unintended transfer errors
- Misconfigurations and security errors
- Malware, insider threats, and cyberattacks
- Compromised hardware

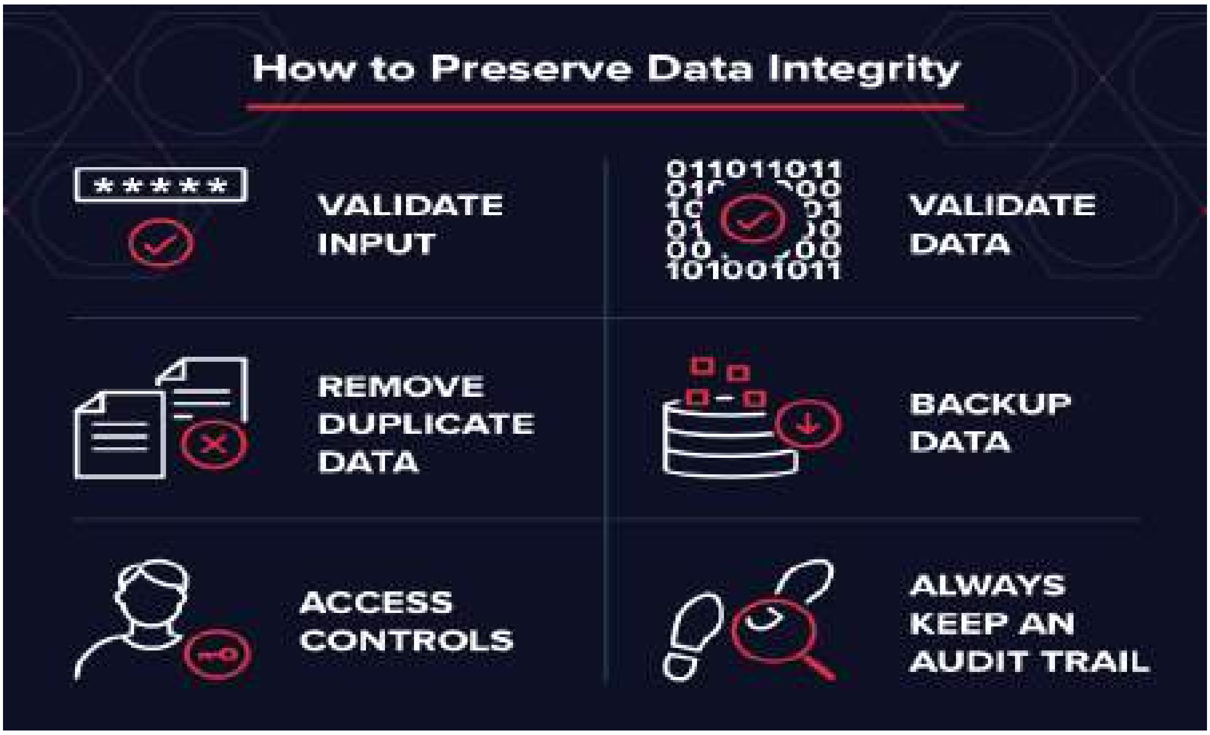
So how do you know when your data has integrity? You have to look at the following features:

Retrievability and accessibility – It’s important to have accurate data in the proper locations at the right time when anyone is working on projections, a deal, or presentation. Without proper and easy access and retrieval, it can be detrimental to the business, yielding the way for your competition to win.

Traceability –Today, you can trace every touchpoint you make with a prospect or customer. How? With a data point. The data can inform decision makers, highlight red flags, deficiencies, or limitations. Make sure these touchpoints are accurate.

Reliability – Having reliable, consistent business metrics against company goals and the competition is what will take an organization to the top.

How to Preserve Data Integrity [Checklist]



The data integrity threats listed above also highlight an aspect of data security that can help preserve data integrity. Use the following checklist to preserve data integrity and minimize risk for your organization:

1. **Validate Input:** When your data set is supplied by a known or unknown source (an end-user, another application, a malicious user, or any number of other sources) you should require input validation. That data should be verified and validated to ensure that the input is accurate.
2. **Validate Data:** It's critical to certify that your data processes haven't been corrupted. Identify specifications and key attributes that are important to your organization before you validate the data.
3. **Remove Duplicate Data:** Sensitive data from a secure database can easily find a home on a document, spreadsheet, email, or in shared folders where employees without proper access can see it. It's prudent to clean up stray data and remove duplicates.

Smaller companies without a dedicated staff will find that these tools can assist them clean up duplicate files on a hard drive or cloud.

- Clone Files Checker
- Duplicate Images Finder
- Easy Duplicate Finder
- Duplicate Cleaner
- CCleaner

- DoubleKiller
- WinMerge

For Windows Servers: Use the Data Deduplication feature to clean up cloned files. Also try the File Server Resource Manager to remove stray files.

4. **Back up Data:** In addition to removing duplicates to ensure data security, data backups are a critical part of the process. Backing up is necessary and goes a long way to prevent permanent data loss. How often should you be backing up? As often as possible. Keep in mind that backups are critical when organizations get hit with ransomware attacks. Just make sure that your backups aren't also encrypted!
5. **Access Controls:** We've made the case above for input validation, data validation, removing duplications, and backups – all necessary to preserve data integrity. Let's not rule a few popular data security best practices that can also lend a hand or two: access controls and an audit trail! Individuals within an organization without proper access and with malicious intent can do grave harm to the data. What's worse, an outsider impersonating an insider can also be detrimental. Implementing a least privilege model – where only users who need access to data get access – is a very successful form of access control. What's often overlooked is physical access to the server. The most sensitive servers should be isolated and bolted to the floor or wall. Only individuals who access should have an access key – ensuring that the keys to the kingdom are kept secure.
6. **Always Keep an Audit Trail:** Whenever there is a breach, it's critical to data integrity to be able to track down the source. Often referred to as an audit trail, this provides an organization the breadcrumbs to accurately pin point the source of the problem.

Typically, an audit trail has the following:

- Audit trails need to be automatically generated
- Users should not have access to or the ability to tamper with the audit trail
- Every event – create, delete, read, modified – is tracked and recorded
- Every event is also aligned to the user, so you know who accessed the data
- Every event is time stamped so that you know when the event took place

Data Integrity Empowers Decision Makers

Not too long ago, it was difficult to collect data. However, today it's no longer an issue. In fact, we're able to collect so much data, the responsible thing to do is to preserve data integrity. That way, management can confidently make data-driven decisions that steer their company in the right direction.

Interested in more information on data integrity? Take a listen to our podcast with Ann Cavoukian on GDPR and Access Control or browse through our article on The Difference Between IAM's User Provisioning and Data Access Management.

Database SecurityDatabase security has many different layers, but the key aspects are:

Authentication

User authentication is to make sure that the person accessing the database is who he claims to be. Authentication can be done at the operating system level or even the database level itself. Many authentication systems such as retina scanners or bio-metrics are used to make sure unauthorized people cannot access the database.

Authorization

Authorization is a privilege provided by the Database Administer. Users of the database can only view the contents they are authorized to view. The rest of the database is out of bounds to them.

The different permissions for authorizations available are:

- **Primary Permission -** This is granted to users publicly and directly.
- **Secondary Permission -** This is granted to groups and automatically awarded to a user if he is a member of the group.
- **Public Permission -** This is publicly granted to all the users.
- **Context sensitive permission -** This is related to sensitive content and only granted to a select users.

The categories of authorization that can be given to users are:

- **System Administrator -** This is the highest administrative authorization for a user. Users with this authorization can also execute some database administrator commands such as restore or upgrade a database.
- **System Control -** This is the highest control authorization for a user. This allows maintenance operations on the database but not direct access to data.
- **System Maintenance -** This is the lower level of system control authority. It also allows users to maintain the database but within a database manager instance.
- **System Monitor -** Using this authority, the user can monitor the database and take snapshots of it.

Database Integrity

Data integrity in the database is the correctness, consistency and completeness of data. Data integrity is enforced using the following three integrity constraints:

- **Entity Integrity -** This is related to the concept of primary keys. All tables should have their own primary keys which should uniquely identify a row and not be NULL.
- **Referential Integrity -** This is related to the concept of foreign keys. A foreign key is a key of a relation that is referred in another relation.
- **Domain Integrity -** This means that there should be a defined domain for all the columns in a database.