OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

TIPS AND TRENDS #2019-0003
MAY 2019

John A. Carey
Inspector General

Inspector General
Accredited

Data Integrity

Our recent audits have revealed that some municipalities lack controls to ensure integrity and protection of information in their computer systems, which increases the risk of inconsistent reporting, a data breach, fraud, waste, and abuse.

Municipalities may be able to improve the integrity of their systems' data by implementing appropriate policies and procedures, ensuring physical security, improving user access controls, performing periodic inventories, and testing data backups and recovery procedures.

Why is Data Integrity Important?

Data integrity refers to the accuracy and consistency (validity) of data over its lifecycle. Data integrity covers data in storage, during processing, and while in transit. In short, data integrity is the reliability and trustworthiness of data throughout its lifecycle no matter how long it is stored or how often it is accessed.

If an entity's data is altered, deleted, or lost without management detecting how, when, and by whom then the data may be unreliable. Unreliable data may have a major impact on data-driven decisions, financial reporting, and operations. A lack of controls over system data can lead to, but is not limited to: improper system calculations; erroneous reports or processing errors; undetected, unauthorized, or fraudulent transactions; master files with erroneous or improperly altered data; unauthorized program modifications; and access to the data by unauthorized persons.

Common threats to data integrity include:

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

How can data integrity risks be minimized?

Suggestions to Minimize Data Integrity Risks

- **Follow a software development cycle** – all computer systems should be appropriately developed, qualified, tested, and assessed on a regular basis.
- **Validate computer systems** – the performance of information system functions is independently verified.
- **Implement audit trails** – a secure, computer-generated, time-stamped audit trail records the identity, date, and time of data entries, changes, and deletions.
- **Limit system access** – all systems should require a login and password assigned to a single individual and the access should be determined by the individual's responsibilities with the entity.
- **Implement backup and recovery procedures** – such procedures ensure the recovery of data from unexpected events of data loss and application errors.
- **Design and implement policies and procedures** – effective policies and procedures build quality into the process by systematically controlling the process and ensuring clear accountability.
- **Protect the physical and logical security of systems** – controls are needed to protect the physical and logical security of systems, change management, service management, and system continuity.
- **Establish a vendor management program** – periodically evaluate vendors and their data integrity procedures.
- **Train users and maintain training records** – users should be properly trained on systems, policies and procedures, and cybersecurity awareness.
- **Conduct audits/reviews** – audits/reviews evaluate controls and promote compliance with policies and procedures.