



GRANTEK

**Ensuring Data Integrity in
Pharmaceutical Production**
Beyond Compliance with Grantek

Background

Regulatory agencies worldwide charge manufacturers in the life science industry with assuring that their products are manufactured in a manner that protects patient safety, product quality and data integrity. These concepts form the bedrock of the Good Manufacturing Practices (GMP) that govern the industry. In 2016, following an increase in the number of GMP violations specifically involving data integrity, the US Food and Drug Administration (FDA) issued a draft guidance on the topic of maintaining data integrity for pharmaceutical production. The changing regulatory focus has been picked up on by the industry and in turn, Grantek's customers. Newly elected Chairperson of the Board for the International Society of Pharmaceutical Engineers (ISPE), Fran Zipp, notes that data integrity "creates the trust required to discover, develop, commercialize, and distribute medicines successfully, and to ensure that products are safe and efficacious."

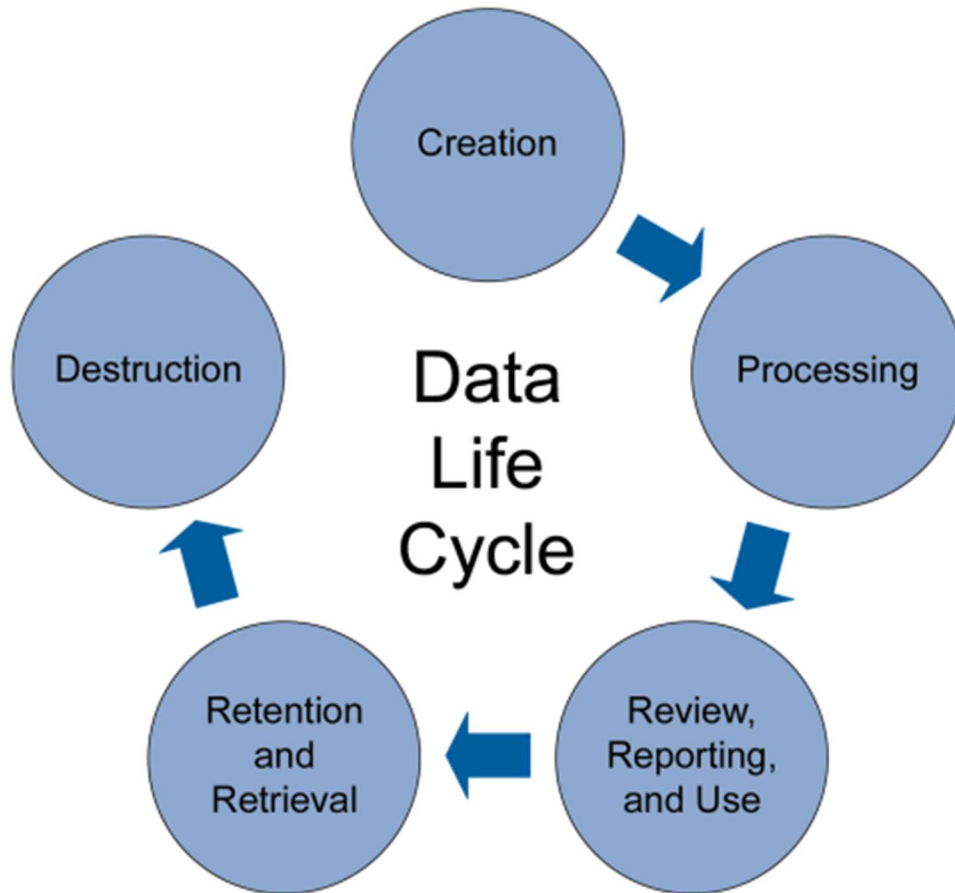
Regulators expect data and records to be accurate and complete, and that they are available and usable throughout the required retention period. It is no longer sufficient to just archive PDF copies of batch records. Process data must also be retained and available.

Regulatory agencies are focusing on the following areas that have the potential to compromise data integrity:

- Lack of basic access control and security measures that could allow unauthorized changes
- Shared user logins
- Missing or disabled audit trails
- Lack of contemporaneous recording of activities
- Failure to investigate data discrepancies
- Testing into compliance
- Incomplete collection, retention, and review of data for quality decisions
- Overwriting or deletion of original data
- Data falsification

Auditors and agency inspectors from the FDA and Health Canada are focusing on data integrity more so than previously. Both agencies have been issuing more observations on data integrity in recent years.

Pharmaceutical production data includes everything from machine-level reports to batch records to lab results—everything needed to prove that a pharmaceutical was made in a way that assures safety and efficacy.



Data integrity goes above and beyond 21 CFR Part 11 (electronic signatures) requirements. Manufacturers must ensure that recordkeeping requirements for completeness, consistency and accuracy of production data are maintained throughout a product’s lifecycle. These records include metadata as well as the final batch report.

How Grantek can help

Data integrity auditing is a service offering uniquely available from Grantek. Most system integrators do not have this expertise in-house. Grantek now offers data integrity auditing to help establish a baseline and identify gaps in data integrity that could result in failure to retain adequate records and/or potential regulatory agency observations. Grantek’s data integrity audit process includes 21 CFR compliance and GMP assessment.

Because Grantek has expertise in pharmaceutical manufacturing technology we have a full understanding of what the regulatory agencies are looking for, and are uniquely positioned to develop solutions to any data gaps revealed in the auditing process. Grantek is familiar with Canadian and US regulations as a result of our many years of cross-border experience. We work Level 0 to Level 4 of ISA95.

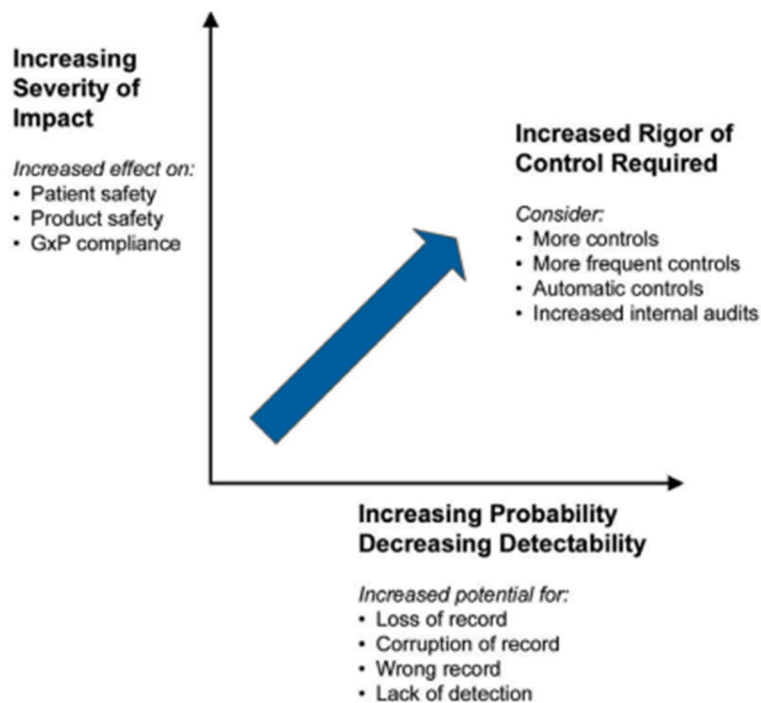
Methodology

Grantek's data integrity audits cover more than 21 CFR Part 11 compliance. We assess the computerized systems using checklists and methodologies that follow ISPE GAMP guidelines to ensure we evaluate the customer's systems against all applicable regulatory controls.

Grantek bases their data integrity audits on a checklist template that is tailored for each customer. The data integrity auditors tailor the checklist and assessment based on the architecture of the customer's computerized systems.

We may first ask the customer to complete a preliminary checklist to identify the facility assets, especially if the customer or facility is one we have not worked with previously. Generally, Grantek works with plant staff to get access to all systems.

Preliminary work may include defining the boundaries of the computerized systems in order to determine the elements that create the data and the flow of data, from sensor to Programmable Logic Controller (PLC), to Human-Machine Interface (HMI) and Historian and so on. The audit process also identifies how and where the data is backed up and stored, and how batch reports are generated.



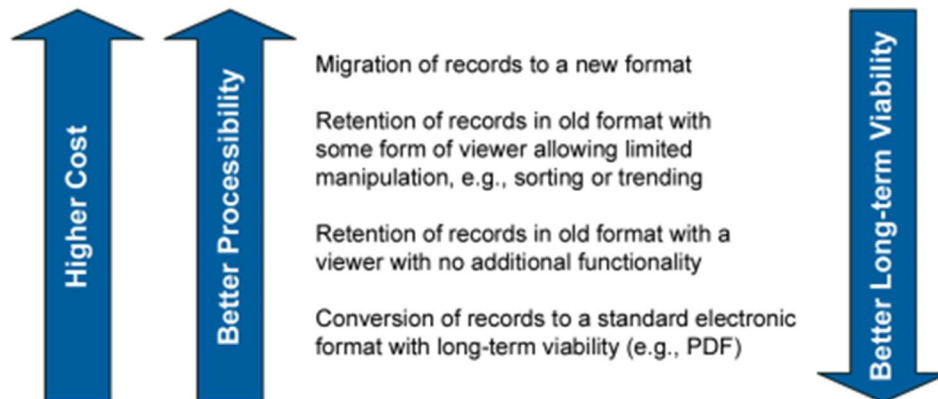
The data output is evaluated for each stage of production, from the machine PLCs all the way up to the Enterprise Resource Planning (ERP) reports. Each piece of equipment is assessed to identify gaps in data integrity and to ensure that it has a defined user requirement specification.

The task assessment and checklist are used to evaluate each piece of equipment for common causes of data integrity deficiencies, including:

- Is the facility using common passwords to access production equipment or systems?
- Are electronic records properly archived?
- Is equipment configured for auto logout to reduce the risk of mismatched credentials for those doing the work?
- Are there gaps in Original Equipment Manufacturer (OEM) systems that are 21 CFR Part 11 ready, but may be improperly configured?

Risk Identification

The audit includes a risk rating for each item and identifies equipment specifics such as OS and controller software version. It also includes a remediation list which is discussed with the customer to help prioritize corrective actions and to determine remediation that is best done by the customer, such as using domain logins to manage expiring passwords. Grantek will point out where we can help with remediation, and we will generate a cost estimate for doing the work.



Risks commonly identified during the data integrity audit include the following:

- **Administrative risks:** maintain accurate user access. When adding and removing users, ensure authorized users are the right users and remove access from users who no longer need it.
- **Configuration risk:** ensure that users have the correct access by assigning users the appropriate roles in the system.
- **Date and time synchronization risk:** ensure date and time are correct and are automatically updated from a network source to help ensure all equipment has the same time and date reference and to help prevent incorrect time/date stamps on production records. Ensure Daylight Savings Time adjustments are made automatically and from a NTS source.
- **E-record risk:** ensure that critical electronic records are properly stored.
- **Record storage risk:** reduce risks of single point of failure by working to eliminate local storage of records ensuring records are backed up to an external device, a redundant server, and/or a network center.
- **Report risks:** verify that accurate and complete reports are generated and printed appropriately at the end of each process.

- **Security risks:** eliminate generic logins such as “operator” instead of a unique username. Generic accounts should not be allowed.
- **Setup risks:** ensure and verify that the correct parameters are programmed when setting up machines. Require setup verification by someone other than the person performing setup.
- **Third-party vendor risk:** Grantek works with OEMs to ensure that customers do not lose warranty protection as a result of upgrade implementation or reprogramming needed to achieve data integrity.

Remediation

Grantek works with the customer to develop and analyze potential solutions from the standpoint of cost and risk. Ultimately it is up to the customer to select the solution that best fits their needs. Grantek provides a comprehensive report identifying deficiencies in data integrity.

Grantek then develops a remediation plan to provide a path to meeting the data integrity guidelines. The solutions typically involve ensuring that OEM equipment has the newest software installed, and that legacy equipment is modified as required to bring it up to current standards. Grantek can do custom modifications if needed. Equipment replacement may be needed, as a last resort. Typically, the proposed solution involves modifications/upgrades to monitoring and managing equipment, not the production machines.

Advantages of working with Grantek

Our client solution manager handles client engagement, discovery, preliminary engineering, and proposal generation. After client approval is received, the client solution manager then builds schedules and assembles the team to tackle the project.

The data integrity audit process is generally separate from Grantek’s system integration and automation work, allowing the data integrity audit to take place concurrently with another Grantek project. The data integrity audit typically takes about a month, depending on the amount and variety of equipment at a facility.

Grantek sets up a test environment at their office to test proposed solutions before rolling them out to the production floor. We use simulation modules to mimic the production machines. The tools were developed internally by Grantek. The simulations allow our engineers to step through programming changes to see impact of software design changes they made, without affecting customer operations.

We write all required documentation, including user requirement specifications, functional acceptance tests, and system acceptance tests. We work with the customer’s personnel to conduct acceptance testing and help leverage the SAT in order to reduce the effort needed for Installation Qualification/Production Qualification (IQ/OQ) testing.

All Grantek project personnel, including upper management, client solution management, and project managers, are technically trained engineers. Our organizational/project delivery model differs from that

of our competitors. At Grantek, we assign the same people to design and implement customer solutions, end-to-end. The engineer who programs PLC software in the office test environment is the same engineer who then goes onsite to perform the implementation and write the documentation. Our competitors split project responsibility: documentation, offsite work, onsite work, and service support may all be done by different people, resulting in knowledge gaps. Grantek keeps the same people on a project from start to finish, so our staff is better equipped to meet customer expectations and carry knowledge forward throughout the life cycle of each project.

For over 30 years, top manufacturers in Food & Beverage, CPG, Pharmaceuticals and Energy have called upon Grantek to solve their most complex business and manufacturing challenges. Grantek's team of professionals located in 17 offices across the globe deliver solutions to complex problems in Smart Manufacturing, Industrial Networking, Automation and Industrial Safety. Call 1.866.936.9509 or email info@grantek.com to learn more.