



**Compliance and Validation  
for Global Systems:  
Putting the Puzzle Together**

## Reader ROI

- IT must be able to support international regulations that cover a multitude of topics from data integrity to security and data privacy.
- Developing standards can help decrease the complexity involved in managing compliance programs across the globe.
- Industry standards can be implemented to create a foundation for meeting multiple regulations while creating a consistent, cost-effective environment that supports the business needs.

# Compliance and Validation for Global Systems: Putting the Puzzle Together

Validating compliance for IT pharmaceutical systems means more than validating software. In most companies, IT must manage adherence to a variety of regulations that cover topics ranging from data integrity to security and privacy. And these regulations vary by country or region.

One method of meeting these business and regulatory needs is through the use of standardization—a framework for creating repeatable and verifiable IT processes. These processes facilitate IT system validation and provide an audit trail.

## Today's regulated it environment

System compliance can be viewed as a large puzzle with pieces scattered across the globe. With the addition of a new country or the adoption of a new regulation, the number of puzzle pieces increases. Achieving global compliance and validation requires an understanding of the individual pieces and an ability to bring them together in a cost-effective fashion.



## Challenges

Developing solutions for each regulation, independent of the others, may result in contradictory policies and procedures and will escalate the cost of maintaining compliant, validated, global systems. For example, focusing all resources on GCP compliance, which is based on data integrity and traceability, will not ensure a compliant data transfer between the GCP-compliant U.S. companies and their Safe Harbor country counterparts.

Similarly 21 CFR Part 11 focuses on creation and modification of electronic data, but does not require the companies to ensure data privacy, which is a crucial requirement for HIPPA compliance in the U.S. and Safe Harbor compliance in the European Union.

Ensuring that IT systems adhere to a defined System Development Life Cycle (SDLC) through all phases, from planning to retirement, is the first step to achieving quality control. Secondly, all compliance guidelines common to the major regulations need to be identified and grouped. Uniformly required controls include:

- **Audit trails:** The system must generate and maintain audit trails that are secure, computer-generated, time-stamped, and independent. The date and time of operator entries that create, modify, or delete records must be preserved. The previous values and reason for change must be retained in original form.
- **Traceability:** The system must support tracing any of the changes made to the data.
- **Data control:** Robust policies for creation, modification, and viewing must be designed and implemented in the system.
- **Reliability (Validation):** The system can be shown to produce consistent results when performing the same function.

## Standards program

Industry standards can be implemented to create a foundation for IT processes that meet multiple regulations and create a consistent, cost-effective environment that supports the business needs. These standards include:

- **IEEE System Lifecycle:** The IEEE has a number of global standards that can be applied to the system lifecycle. Examples include:
  - 829-1998 Standard for Software Test Documentation
  - 830-1998, Recommended Practice for Software Requirements Specifications
  - 1016-1998, Recommended Practice for Software Design Descriptions
  - 1058-1998, Standard for Software Project Management Plans
  - 1062-1998, Recommended Practice for Software Acquisition
  - 1074-1997, Standard for Developing Software Life Cycle Processes
  - 1219-1998, Standard for Software Maintenance
  - 1540-2001, Standard for Software Life Cycle Processes-Risk Management
- **CMMI:** Developed by the Software Engineering Institute at Carnegie Mellon University, CMMI describes the characteristics of successful processes. It consists of three constellations:
  - **CMMI Development:** Provides guidance for measuring, monitoring, and managing development processes
  - **CMMI Services:** Provides guidance for those supplying services within organizations and to external customers
  - **CMMI Acquisition:** Provides guidance that enables informed and decisive acquisition leadership
- **ISPE/GAMP:** ISPE/GAMP is an expert body in the computer system validation arena. There are specific GAMP guides for the validation of automated systems in pharmaceutical manufacturing, global information systems, IT infrastructure control and compliance, electronic records and signatures, and laboratory-computerized systems.
- **Security**
  - **ISO: ISO 17799:2005** “Information Technology - Security Techniques – Code of Practice for Information Security Management” is a code of practice for information security management guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.
  - **NIST:** NIST is the U.S. National Institute of Standards and Technology. The NIST provides a number of guidelines pertaining to Federal Agency Security Practices (FASP) and public/private security practices. It also provides various checklists and implementation guides.
- **Process Excellence**
  - **ITIL:** This is a framework of best-practice approaches intended to facilitate the delivery of high-quality information technology (IT) services. ITIL outlines an extensive set of management processes that are intended to help businesses achieve both high financial quality and value in IT operations. ITIL is composed of five core sections.
    - **Service Strategy:** focuses on understanding and translating business strategy into IT strategy, as well as selecting best practices for the industry
    - **Service Design:** focuses on the IT lifecycle including, roles, responsibilities, costs, risks, measurements, and buy versus build
    - **Service Transition:** covers creating a transition strategy from service design and transfers it to the production environment
    - **Service Operation:** embraces the basics of how to manage services in the production environment, including day-to-day issues and fire fighting for applications and infrastructure
    - **Continual Service Improvement:** principles, methods, best practices, and tools for improving a service after it is deployed

The size of an organization, regulations impacting the organization, time available for implementation, and costs should be analyzed before selecting or implementing a standards program.

## The solution: validation and compliance

Validation and compliance are an ongoing process that starts with the conception of the system or service and does not end until after the data, not just the system, is retired. Moreover, quality control should be enforced throughout the system's life.

Implementing standard IT processes across the company facilitates adherence to a range of regulatory requirements and lowers costs.



**EMC Corporation**  
Hopkinton  
Massachusetts  
01748-9103  
1-508-435-1000  
In North America 1-866-464-7381  
[www.EMC.com](http://www.EMC.com)