Waters™

Multiple Environments Bring More Control to Your Lab's Software Systems

Tracy Hibbs, Fiona O'Leary, and Lissa Wang
Waters Corporation, Milford, MA, USA

DEFINING AN ENVIRONMENT

In George Orwell's book *Animal Farm*, the slogan "Four legs good, two legs bad" is used to represent the philosophy of the new order. When applied to managing good practice guidelines and regulations (GxP), the slogan could be modified to "Multiple environments good, single environment bad".[1]

The Pharmaceutical Inspection Co-operation Scheme (PIC/S) defines a computerized system as the combination of the computer system (hardware, software, and firmware), the controlled function or process (operating procedures and people, equipment) and the operating environment (including other networked or standalone computerized systems, other systems, media, people, equipment, and procedures).[2]

A single instance of the computerized system may be referred to as an *environment*. The primary environment used in your day-to-day business operations and processes is often referred to as the *Production Environment*. This common language is applicable whether the environment is used for production data, in a QC lab, or elsewhere in your business.

At the go-live point, when the Production Environment enters the operational stage and begins its functional life supporting a GxP business process, every aspect of the environment has been controlled and verified. Figure 1 shows the project stages where the system has been implemented and validated, and the handover to the operational stage where changes will still need to occur to keep the system current.

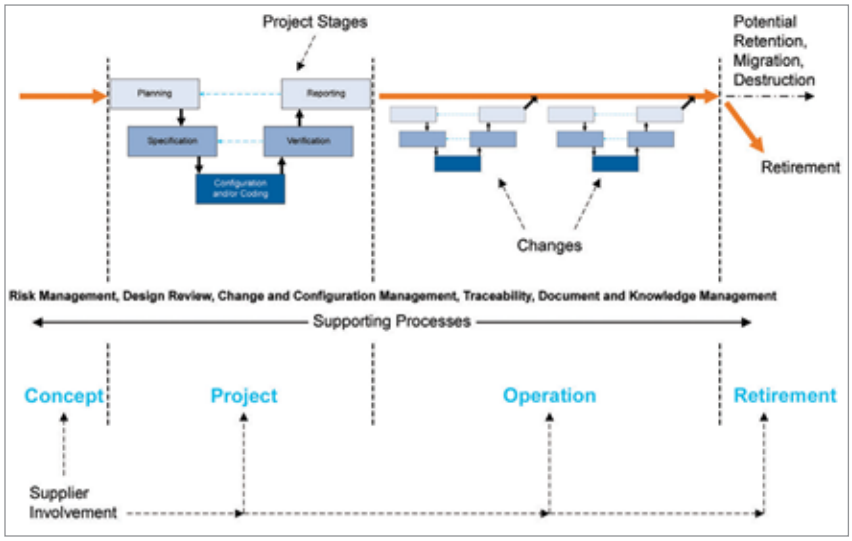

Figure 1. Project and Operational stages within the Computerized System Life Cycle
Source: Figure 4.1, ISPE GAMP® 5 (Second Edition).[3] Copyright ISPE 2022. All rights reserved, www.ISPE.org. Reproduced with permission from ISPE.

WHAT'S WRONG WITH A SINGLE ENVIRONMENT?

The problem is that a system, in this case your Production Environment, cannot remain static through its operational stage, which is often 10 years or more in duration, and will need:

- Operating system and underlying technology stack software patches and updates, to fix security flaws and protect against cyberattacks, and upkeep of infrastructure hardware
- Application and instrument driver updates to correct defects and bring in new features, as well as the introduction of additional system functionality, such as:
  - Empower™ Method Validation Manager (MVM)
  - waters_connect™ System Monitoring
  - Empower Sample Set Generator (SSG)
  - Services Toolkit Applications
- Empower Business Continuity (BC) LAC/E™ devices with SecureSync Software
- Periodic trial restore, to confirm data can be restored from backup in the event of a disaster
- Configuration changes and customization within the software applications themselves, such as:
  - New methods and custom fields developed in Empower Chromatography Data System (CDS)
  - New capture templates created and tested in NuGenesis™ Scientific Data Management System (SDMS)
  - New forms and serial device connections developed in Empower and NuGenesis Lab Management Systems (LMS)
  - New instrument/system configurations in Empower CDS
  - New LAC/E device configuration changes and updates in Empower CDS
  - Updating user permissions

Each of these essential tasks presents challenges and issues when performed directly in the Production Environment if this is the only environment available to you. At the same time, failing to execute on these tasks can leave your organization vulnerable to unnecessary risk and your data lacking durability.

OPERATING SYSTEM UPDATES

An operating system must be kept current to reduce the risk of cyberattack. In just a 12-month period during the pandemic, there were 13 documented cyberattacks[4] on companies and organizations involved in COVID-19 vaccine development, approval, and administration. As operating system vendors become aware of vulnerabilities in their product, they develop and release patches to resolve the vulnerabilities. When releasing the patch, the vendor also details the vulnerability, primarily so your IT department can assess both the vulnerability and criticality of the patch. These details also inadvertently provide potential hackers with insight and inspiration for new malware attacks.

While patches are critical to operating system security, they can introduce instability and bugs into your computerized system environment that pose a different risk. For example, a defect correction within the operating system relating to date handling could result in your application being unable to interpret system date-time stamps.

Think of all the critical GxP data within your Production Environment for Empower CDS as an example, including data on which your batch-release decisions have been made:

What would be the impact on your business if an operating system patch rendered all that data unreadable?

You may have to recall released batches for which the data has been lost. If you are also unable to test and release new batches, there are bigger implications. This could in turn create a shortage of the critical drugs you produce, impacting the treatment regimen for your end patients – worldwide.

In Animal Farm, the slogan "Four legs good, two legs bad" is used to represent the philosophy of the new order. When applied to managing GxP, the slogan could be modified to "Multiple environments good, single environment bad".

Risk	Outcome	Data Table Heading (WP)
Security patch not installed	Cyberattack involving theft of intellectual property or ransom	Share value decrease and/or financial loss to payment or ransome
Security patch installed but adversely impacts the application functionality	Application not running	Unable to test and release new batches, impacting company revenue and creating a drug shortage
	GxP data loss	Recall of released batches

Table 1. Summary of risks from operating system patches.

There are additional essential upkeep needs, for example infrastructure hardware components, which require changes to your system. Hardware updates to the system include, but are not limited to, network routers, printers, hardware server hosting infrastructure, LAN/WAN infrastructure, domain controllers, DNS, DHCP, etc. Upkeep of these technologies may also involve the use of virtual environments or cloud-based hosting. Other system components, such as web browsers, printer drivers, PDF readers, backup software, etc., may also need upkeep and updating. These need to be monitored for usage and updated with technological changes. Updates to system monitoring tools are also needed as technology changes, to allow adaptation and resilience to the newer system environments.

There is an ongoing need to adjust and adapt the system environment to different technology changes and availabilities.

APPLICATION AND INSTRUMENT DRIVER UPDATES

In the past, many regulated companies have been reluctant to accept application upgrades each time their application vendor releases a new version. The regulators are increasingly expecting industry to be proactive in adopting updates to both applications and operating systems, as suggested in statements such as:

- Article 23 of the EU Medicines Directive: *"After a marketing authorisation has been granted, the marketing authorisation holder shall, in respect of the methods of manufacture and control provided for in Article 8(3)(d) and (h), take account of scientific and technical progress and introduce any changes that may be required to enable the medicinal product to be manufactured and checked by means of generally accepted scientific methods."*[5]
- PIC/S PI 041-1 §9.3: *"Operating systems and network components (including hardware) should be updated in a timely manner according to vendor recommendations and migration of applications from older to newer platforms should be planned and conducted in advance of the time before the platforms reach an unsupported state which may affect the management and integrity of data generated by the system."*[6]

It is essential that upgrades occur, however the impact of each application and instrument driver update must be considered. If implemented, any new features available with an update will need to be assessed for risk to patient safety, product quality, and data integrity. Testing components of an update are expected to be commensurate with risk, and additional regression testing should be performed, if needed, to verify critical functionality. This also applies to the addition of new functionality and capabilities provided with add-on components to the system.

Modern risk-based approaches, leveraging vendor expertise and activities, and critical thinking, can all streamline the time and effort needed to maintain the validated status of a system through the update, but there will be some period of time between installation of the new version and confirmation that the new version remains fit for your intended use. Do you want to accept the risks with continued GxP use of the system during that time? If testing activities uncover a defect in the new version, or an interface no longer works due to the changes, what is the impact on data generated during that time? Simply put, the data cannot be trusted and therefore you cannot be certain of the quality of your product and may have to recall it.

The safer alternative may appear to be to stop using the system for the duration of the upgrade and validation work, but how long can your lab operate without its Empower Chromatography Data System (CDS)? Or be without NuGenesis Lab Management System (LMS)? This takes you right back to the concerns about being unable to release product and potentially creating a drug shortage impacting your end patient. Table 2 summarizes the risks around implementing application upgrades directly in the Production Environments.

Risk	Outcome	Long-term impact
Application is not upgraded	Lack of latest data integrity controls and latest features	Data may not be trusted, and issues during regulatory inspections
Application is upgraded while the system is still in GxP use	System may not be fit for intended use during the upgrade period	Data from that period may not be trusted leading to recall of released batches
System use suspended while application is upgraded	System not available for use during the upgrade period	Unable to test and release new batches, impacting company revenue and creating a drug shortage

Table 2. Summary of risks from application upgrades.

TRIAL RESTORE

No matter how confident you may be about your backup solution, it is both good practice and a regulatory expectation to confirm the ability to restore your data from backup. EU and PIC/S Annex 11 on Computerized Systems §7.2 states: *"Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically."* [7]

Trial restore can represent a paradox of risk to your Production Environment: you cannot be confident that you can restore from backup unless you do a trial restore, however running a trial restore into the production system is high-risk and not recommended as it brings potential for data loss if unsuccessful.

Risk	Outcome	Long-term impact
Restore not tested	Ability to restore data in the event of a disaster is unknown	Data may not be recoverable after a disaster, leading to recall of released batches
Restore tested in the Production Environment but there are problems during the restore.	The original GxP data in the Production Environment is lost or overwritten during the restore	Original GxP data is lost from the Production Environment leading to recall of released batches
System use suspended while application is upgraded	System not available for use during the upgrade period	Unable to test and release new batches, impacting company revenue and creating a drug shortage

Table 3. Summary of risks from trial restore.

CUSTOMIZATIONS AND DEVELOPMENTS WITHIN THE PRODUCTION ENVIRONMENT

GxP data is that data explicitly required under the predicate rules, e.g., US cGMP and GLP, EU and PIC/S GMP, ICH GCP, etc.

Even within a GxP system, there are activities that do not create GxP data but rather create data supporting the GxP use of the system and that data may itself be requested during an audit. These activities include computerized system validation testing, developing and validating custom fields in Empower CDS, configuring and validating capture templates in NuGenesis SDMS, and creating and validating forms and serial device connections in NuGenesis LMS. Even initial method development in Empower CDS is not GxP data, although the method validation would be GxP.

These activities all require access to additional functionality and/or higher privileges than routine use of the application. They may also require the occasional deletion of failed iterations of the developments.

However, it is an immediate 'red flag' to an inspector to have high-risk privileges granted to users in a Production Environment and even worse when there are deletions recorded in the audit trail of that environment.
While the presence of deletion records and users having access to high-risk privileges can ultimately be justified with explanations of the development and validation processes, actually ensuring these activities happen outside of the Production Environment eliminates the need for that anxious conversation with the inspector.

SEPARATING INTO MULTIPLE ENVIRONMENTS

As the ecosystem of your core applications evolve and expand, adding new software options and applications directly to your Product Environment creates unnecessary risk. A simple solution is to set up multiple environments for your Empower CDS or NuGenesis LMS system, each with a defined purpose, allowing you to segregate your activities and maintain control in your Production Environment. Figure 2 shows an example, generally applicable for either system, with three separate environments.

Risk	Outcome	Long-term impact
Customization and development occurring in Production Environment	Orphan data in the system and deletions in the audit trail	Concerns from an inspector during an audit
	Users have higher privileges and access to high-risk functionality	
Hardware and Software Technology Updates	Adaptability to technology changes and availabilities result to a need to advance and update the environment	Access to the environment when considering any technology update

Table 4. Summary of risks from development in the production environment.

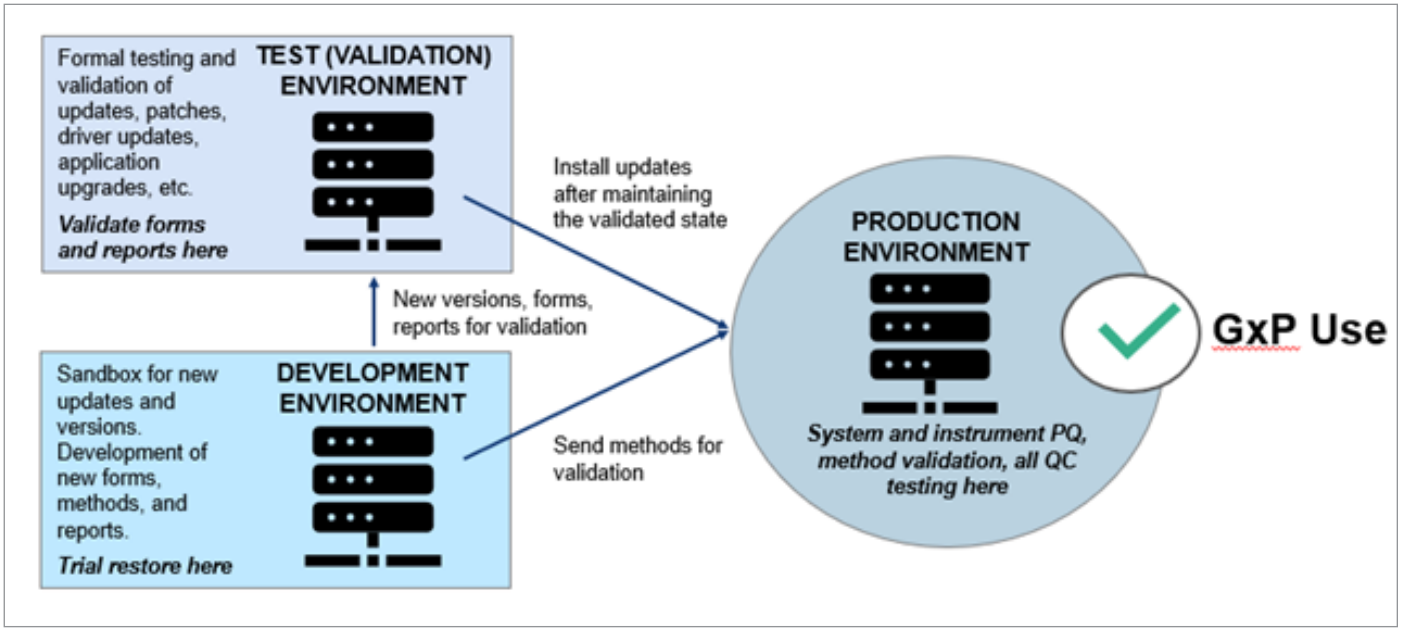

Figure 2. Leveraging multiple environments.

DEVELOPMENT ENVIRONMENT

The Development Environment is effectively a 'sandbox' area where new operating system patches and new application versions can be installed and assessed without any impact on GxP data or the Production and Test Environments. Any issues found can be investigated and assessed before accepting the changes into the Test Environment (where the changes will be validated) and eventually rolling the changes out to the Production Environment with minimal risk and disruption.

The Development Environment is useful to trial new user types and privileges, and to explore new functionality in new versions of the application with the intent of updating SOPs and creating new templates to reflect the new functionality and user types. New or updated instrument drivers can be assessed for new added features and impact on current functionality. The Development Environment is often limited to IT personnel and selected application superusers who can take advantage of the 'sandbox' philosophy (i.e., providing a safe place to play) to create, customize, and develop within the application, whether it be custom fields and reports in Empower CDS, capture templates in NuGenesis SDMS, or forms in NuGenesis LMS. Except for IT-level privileges (e.g., configuring new raw data shares or adding new file capture modules), the superusers can be given maximum privileges for maximum flexibility.

Developing new chromatographic methods will of course need representative instruments connected to the Empower Development Environment, just as developing new serial device connections to balances and pH meters is only feasible in the NuGenesis Development Environment if there are balances and pH meters connected to that system.

The Development Environment provides an ideal location for executing trial restores after any developed methods and forms have passed up to either the Test or Production Environments as applicable. With no GxP data in the system, any data lost during a restore issue has no impact on the business process.

TEST ENVIRONMENT

After initial testing and exploration of operating system patches and application versions has been completed, any agreed updates can be transferred to the Test Environment (also referred to as Validation Environment). Here, formal validation of the change occurs with confidence that the Production Environment is not impacted.

The Test Environment is also the destination for forms, custom fields, reports, etc. that have been created and refined in the Development Environment and now require validation before promotion to the Production Environment. The availability of relevant instruments will determine whether serial device connections are validated here. The Test Environment is also where there is testing and adaptation to newer hardware and software technologies, as needed.

An important distinction to note, data generated in the Test Environment must be kept and protected, as it is supporting data to the Production Environment and may be called for during an inspection.

PRODUCTION ENVIRONMENT

The Production Environment is the location where all GxP data is stored and secured. Any changes to the operating system or application versions must have been previously validated in the Test Environment before they can be implemented in the Production Environment. This minimizes downtime and disruption for the Production Environment while also minimizing risk to the GxP data.

System and instrument PQ should be completed within the Production Environment, as this is the GxP environment. There may also be specific test types that have to happen in the Production Environment, if the Test Environment cannot be classed as representative, for example:

- Running a backup test for subsequent restore into the Development Environment as that test must challenge the actual backup scheduling, execution, copying, and storage of the Production Environment data
- Stress or load testing, which requires production volumes of connected users, instruments, and data to be a representative test

After method development in the Development Environment, method validation should also occur within the Production Environment as the method validation data is GxP data. Of course, all routine QC testing should occur in the production system. QC data is the highest risk data within an organization, so users should have the least privileges to perform their routine tasks, and no one should have the ability to delete data within the Production Environment.

Risk	Outcome	Mitigation
Security patch installed but adversely impacts the application functionality	Application not running	Defects are discovered during initial testing in the Development Environment. Issued are resolved prior to validation in the Test Environment and so there are no issues when deployed to the Production Environment.
Application is upgraded while the system is still in GxP use	System may not be fit for intended use during the upgrade period	The Production Environment remains unaffected and in a validated state while the upgrade is evaluated in the Development Environment and validated in the Test Environment. The actual time to deploy the validated upgrade into the Production Environment and complete any Production Environment-specific testing is minimal and can be scheduled around routine system usage.
System use suspended while application is upgraded	System not available for use during the upgrade period	
Restore tested in the Production Environment but there are problems during the restore.	The original GxP data in the Production Environment is lost or overwritten during the restore.	Backup data from the Production Environment is restored into the Development Environment, ensuring the GxP data in the Production Environment cannot be impacted.
Customization and Development occurring in Production Environment	Orphan data in the system and deletions in the audit trail.	Customization and Development occurs in the Test Environment. Users in the Production Environment have the least privileges for their routine tasks, and there is no deletion or orphan data in this environment.
	Users have higher privileges and access to high-risk functionality.	

Table 5. Risk mitigation using multiple environments.

RISK MITIGATION THROUGH MULTIPLE ENVIRONMENTS

Using multiple environments can mitigate each of the risks of updating and managing the system as identified in this white paper, where the risk involves taking an action, e.g., updating or restoring, as shown in Table 5. This automatically removes the need to consider NOT taking the action and the risk associated with that.

PRACTICALITIES OF MULTIPLE ENVIRONMENTS

Delineation between Test and Production may change depending on whether instruments are attached to the Test Environment, e.g., forms may be validated in the Test Environment if they do not involve serial device connections or if instruments are not available in the Test Environment.

All three environments should be maintained at the same version and optional licenses (except when testing new versions). The Development and Test Environments will need just a few user licenses to cover IT and the superusers; there is no need for large numbers of users in these environments. Even in a large company, Development and Test Environments for Empower CDS could just be Empower Workgroup with a single instrument available for testing and development purposes, so they do not need to be cost-prohibitive.

CONCLUSION

Multiple environments mitigate a myriad of risks associated with the operational stage in a system lifecycle and remove many of the concerns regulated companies express when faced with the challenge of keeping the operating system and application up to date. For any Empower CDS network or NuGenesis Software system, multiple environments are a truly better approach.

Acknowledgements

Thanks to Charlie Wakeham, Co-Chair GAMP Steering Committee, for information used in this white paper.

REFERENCES

1. G. Orwell, Animal Farm, London: Secker and Warburg, 1945.
2. PIC/S, "PI 011-3 Good Practices for Computerised Systems in Regulated "GxP" Environments," 2007.
3. ISPE GAMP 5 Second Edition: A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE, 2022.
4. "Center for Strategic & International Studies," [Online]. Available: https://www.csis.org/. [Accessed August 2021].
5. European Commission, DIRECTIVE 2001/83/EC of the EUROPEAN PARLIAMENT and of the COUNCIL on the Community code relating to medicinal products for human use, EUR-lex, 2001.
6. PIC/S , PI 041-1 Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments, PIC/S, 2021.
7. Annex 11 Computerized Systems, EudraLEX Volume 4 / PIC/S GMP, 2011.

Learn More at waters.com/Empower

Waters™

Waters Corporation
34 Maple Street
Milford, MA 01757 U.S.A.
T: 1 508 478 2000
F: 1 508 872 1990
waters.com