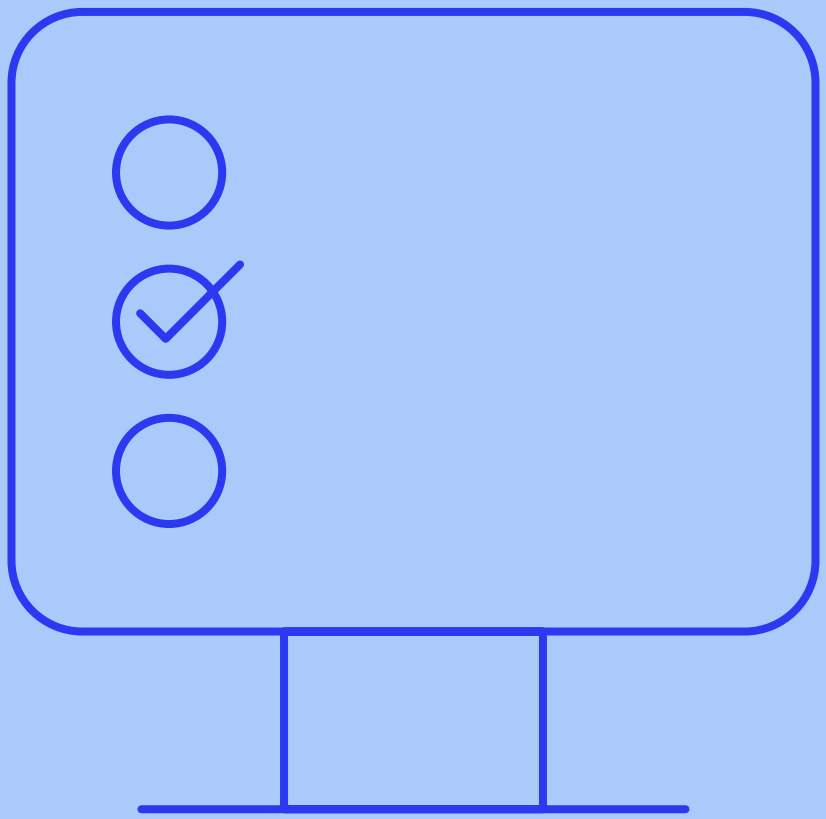
Considerations for using Benchling as a GxP system

White Paper



Benchling

Table of Contents

2 Executive summary

5 Introduction

7 Meeting GxP System Requirements
- Enterprise Security
- Infrastructure Security
- Threat Detection
- Disaster Recovery and Business Continuity Plan
- Data Protection and Retention

10 Product Features and Control
- Identity and Access Management
- Records and Audit Logs
- Electronic Signatures
- Use Case

12 Validation and Updates
- Software Development Lifecycle
- Infrastructure Qualification
- Initial Validation
- Maintaining Validation (Upgrades and Patches)

17 Audit and Inspection Support

18 Quality Management System
- Resource Management and Employee Training
- Vendor Management
- Risk Management
- Change Management
- Document Management
- CAPA

20 Conclusion

Executive Summary

Benchling provides cloud-native software solutions for life sciences research and development (R&D). These products are trusted by hundreds of companies across the globe who operate in highly regulated industries, including biopharmaceuticals, vaccines, agricultural products, and industrial biotechnology. Customers utilize Benchling to store and process critical data pertaining to the design and development of advanced life science products. Regulated industries typically require companies to comply with Good Laboratory Practices, Good Clinical Practices, and Good Manufacturing Practices ("GxP"), which extends to computer systems used in regulated processes. This whitepaper discusses considerations for companies that plan to utilize Benchling solutions in R&D workflows that fall under GxP regulations and require computer systems validation.

The intended audience for this document includes quality management and information technology (IT) professionals, as well as R&D leaders, who wish to learn more about how Benchling supports customers using its solutions in regulated IT environments. It will help customers understand primary considerations relating to:

Security and Privacy
Benchling's approach to enterprise security, infrastructure security, and the standards that are adhered to, such as ISO27001 and the Global Data Protection Regulation (GDPR).

Product Features & Control
A review of capabilities found in Benchling software applications that support GxP compliance, including identity and access management, electronic records and signatures, and audit logs.

Validation and Updates
Considerations for establishing Benchling as part of a validated computer system, including an understanding of Benchling's Software Development Lifecycle (SDLC), release management, initial validation methodology, and ongoing validation support.

Quality Management System
A review of Benchling's Quality Management System, including employee resource management and training, vendor controls, risk and change management, and Benchling's policies surrounding Corrective and Preventive Action (CAPA).

Audit and Inspection Support
An overview of the documentation and processes available to customers to support their obligations to conduct vendor quality audits and inspections.

This whitepaper aims to provide a general understanding of Benchling's principal methods to support customers in their computer systems validation.

Introduction

The life science industry has witnessed tremendous innovation over the past decade. Significant progress has been made in harnessing biology for advancing humanity's wellbeing with the introduction of cell and gene therapies, next-generation antibody therapeutics, mRNA vaccines, and innovative industrial products. While these types of innovations have been transformative, they also introduce an increased level of complexity to the companies committed to developing them. Both the products and the processes used to create them entail more complex biological structures, integrated process workflows, and an ever-increasing amount of structured data required to advance their development.

Benchling provides cloud-native software solutions to accelerate life sciences research and development. Hundreds of companies across the world rely on Benchling products to store, process, and analyze information pertaining to advanced life science products. Customers leverage the ability to model complex science within the software, adapt it to their unique processes, and unify their informatics to drive insights across programs. As a cloud-native solution, Benchling's customers benefit from the inherent scalability, configurability, and interoperability with existing IT solutions.

Cloud software adoption has been steadily increasing within the life science industry over the past decade. In parallel with this transformation, approaches to incorporating software solutions into GxP systems have also evolved considerably. Regulatory agencies have worked in concert with companies to propose more suitable methods to ensure quality throughout the end-to-end product development lifecycle. A recent example is the introduction of the Computer System Assurance guidance, aimed at reducing the documentation burden and increasing the focus on risk-based testing.

Even as validation methodologies continually evolve, many of the guiding principles remain the same. Companies must be able to work with their software vendors to ensure the products they are using are reliable, safe, and traceable. In a world with near-constant innovation, companies must be able to establish a well-defined process to incorporate new software updates within the context of a validated system.

This whitepaper reviews the primary considerations that customers frequently consider when selecting software as part of their regulated IT infrastructure. While the ultimate responsibility for maintaining validation resides with the customer, Benchling is committed to offering a comprehensive range of application controls, documentation, audit management, and infrastructure controls to support our customers globally that choose to trust Benchling in their regulated applications.

Meeting GxP System Requirements

Security and Privacy

Although the responsibility for GxP compliance ultimately lies with customers, Benchling works with customers to uphold an ever-evolving set of security, privacy, and compliance practices, policies, and procedures. Such a partnership can often reduce the effort and burden required for customers to ensure their system components remain in compliance.

Benchling's security and privacy programs are externally audited annually and maintain an ISO 27001 certification. The company also maintains a Privacy Shield certification and complies with the Global Data Protection Regulation (GDPR) as well as the California Consumer Privacy Act (CCPA).

In addition, Benchling aligns its security program and capabilities with the Cloud Computer Compliance Controls Catalogue (C5), National Cyber Security Center (NCSC) Cloud Security Principles, and National Institute of Standards and Technology (NIST) Cloud Computing Standards.

Enterprise Security
Benchling's IT services are automated and compartmentalized to limit the security risk of any single component. The company regularly tests, reviews, and monitors each step of its workflows, building detection and defense-in-depth into each of its IT services.

Additionally, Benchling practices a Zero Trust policy. Multiple security attributes are assigned to each Benchling team member and user account, and multi-factor authentication is required in order to access any of the company's IT services.

A final layer of security is provided by the NIST Security Risk Management Framework. Each security risk is assessed according to an internal risk management framework, with significant decisions requiring confirmation from Benchling's senior executive team.

Infrastructure Security
Benchling utilizes Amazon Web Services (AWS) for hosting. AWS is the industry standard in infrastructure security and maintains multiple security and compliance certifications including ISO 27001, SOC 1, and SOC 2 as detailed here. The use of AWS enables Benchling to quickly iterate and test the quality, performance, and security of its systems. and to maintain control over the security and compliance of data, systems, and services within its computing environments.

Within the production compute environments hosted on Benchling's AWS instances, multiple network security controls are enforced. These include, but are not limited to, network segmentation, firewalls, and traffic monitoring. Benchling's production compute environments are isolated from the public internet, and are segmented from the company's corporate enterprise networks, in order to safeguard data from external threats.

Threat Detection
Benchling's data-driven approach to security focuses on detecting well-defined anomalies in patterns of logged data. These high-fidelity alerts streamline threat detection, enabling more effective interventions.

Furthermore, Benchling augments vendor-supplied alerts with its own proprietary threat models, which leverage key learnings uncovered during penetration-testing and red-team exercises. The company's dedicated security data engineering team performs data modeling, acquisition, aggregation, analysis, and storage in accordance with the organization's overall commitment to confidentiality, integrity, and availability.

Disaster Recovery and Business Continuity Plan

Benchling has an established disaster recovery plan, as well as a business continuity plan. Annual testing ensures the company is prepared for black swan events, and can meet customer commitments including availability and performance SLAs, recovery time objectives (RTO), and recovery point objectives (RPO). Benchling designs its products and services to be resilient and effective, understanding that challenging external events are unpredictable. The enterprise IT services and business workflows have also been planned and architected with these goals in mind so customers' data is always safe.

Data Protection and Retention

Benchling's data records are designed not only for accuracy, but also for easy retrieval by its customers, in accordance with the Electronic Record and Electronic Signature (ERES) requirements outlined in the 21 CFR Part 11 guidance. Data and communication is protected at rest using AES 256-bit encryption, and in transit using Transport Layer Security (TLS) encryption or higher. By default, customer data is stored and processed in the United States, within a secure cloud environment hosted on AWS. On request, data storage and processing may be moved to other locations, such as within the E.U.

Within Benchling's AWS cloud environments, customer data is stored in S3 buckets, which provide granular, auditable control over data protection, along with programmatic verification of data security. Customer data is at minimal risk of loss due to Benchling's high-redundancy data storage practices. Raw files are stored in S3 buckets which are designed for 99.999999999% durability over a given year. Structured data is stored in Postgres databases, which are configured with synchronous replication to encrypted daily and weekly backups. Benchling content is indefinitely retained for as long as one is a Benchling customer. Daily backups are kept for 35 days or more, to allow for granular data restoration, while weekly backups are kept for at least a year. Furthermore, encrypted backups are replicated across multiple geographic regions for higher redundancy.

Product Features and Control

Benchling's system has been architected by a team of cloud software and regulatory experts to meet best-practice usability, scalability, performance, regulatory, and security requirements. In particular, the company's Validated Cloud is continually improved to ensure user compliance per 21 CFR Part 11 and Annex 11 regulations, in the U.S. and E.U., respectively.

Identity and Access Management
Configurable controls enable customer administrators to customize their tenant's product security, compliance, and quality posture in Benchling. Each user can be configured using a granular permission structure, which offers flexible customer-admin defined user roles, along with the ability to grant specific types of access to external users. User access controls can be integrated with a customer's existing single sign-on (SSO) and multi factor authentication (MFA) systems, to ensure that only authorized individuals can access and make authorized changes to the system, which further enhances security and mitigates risk.

Use Case: Benchling Notebook Application

The Benchling Notebook application is often used to store protocols or standard operating procedures (SOPs) in validated environments. Entry templates in the Notebook can be leveraged to give users a well-defined starting point for writing protocols or SOPs. All actions within the entry are assigned timestamps indicating the last modified date, along with the contributing author of any changes. Once a protocol or SOP in the Notebook has been completed, it can then be sent to auditors for review and approval. Auditors are able to leave comments, to which the author may respond by making updates and/or resubmitting. If necessary, the author may require auditors to apply specific review criteria when reviewing and approving an entry. Once an entry has been approved, it is locked, and can only be viewed in read-only form.

Timestamp	User	Item	Item ID	Item Type	Related Items	Description	Action Category	Action
2020-03-25T18:52:29.037442+00:00	anthony	NBK-02 (NBK-02-001)	etr_5jGIBNmy	entry		Created entry	CREATE	entry.created
2020-03-25T18:52:49.610470+00:00	anthony	NBK-02 (NBK-02-001)	etr_5jGIBNmy	entry		Updated entry	UPDATE	entry.updated_name
2020-03-25T18:52:49.610470+00:00	anthony	NBK-02 (NBK-02-001)	etr_5jGIBNmy	entry		Updated entry	UPDATE	entry.updated_content

Figure 6. The protocol, template with clear versioning, project and the entity being purified are connected using "smart links".

Records and Audit Logs

Complete audit trails are automatically generated for every action taken in the software. These trails include dates, times, and the names of users who undertook each action, along with automated data records. Strict versioning of all entries incorporates visible timestamps, and provides authorized users the ability to revert to a prior version. Audit trails and data can readily be accessed and exported to other systems in both human-readable and electronic forms, for backup and data governance. All data and content are retained throughout the customer lifecycle.

Electronic Signatures

Benchling requires electronic signatures, in accordance with 21 CFR Part 11 and Annex 11 in conjunction with SSO. All users are required to enter their username and password prior to electronically signing an entry with their own unique user key. Once an entry has been electronically signed and approved, it cannot be further modified, and can be viewed only in a read-only state.

Validation and Updates

To cater to varying regulations in R&D processes and use cases, Benchling offers two types of tenant accounts: Standard and Validated Cloud (Figure 2). Standard tenants receive daily updates, whereas Validated Cloud tenants receive more controlled updates on a quarterly release cycle, reducing the validation burden.

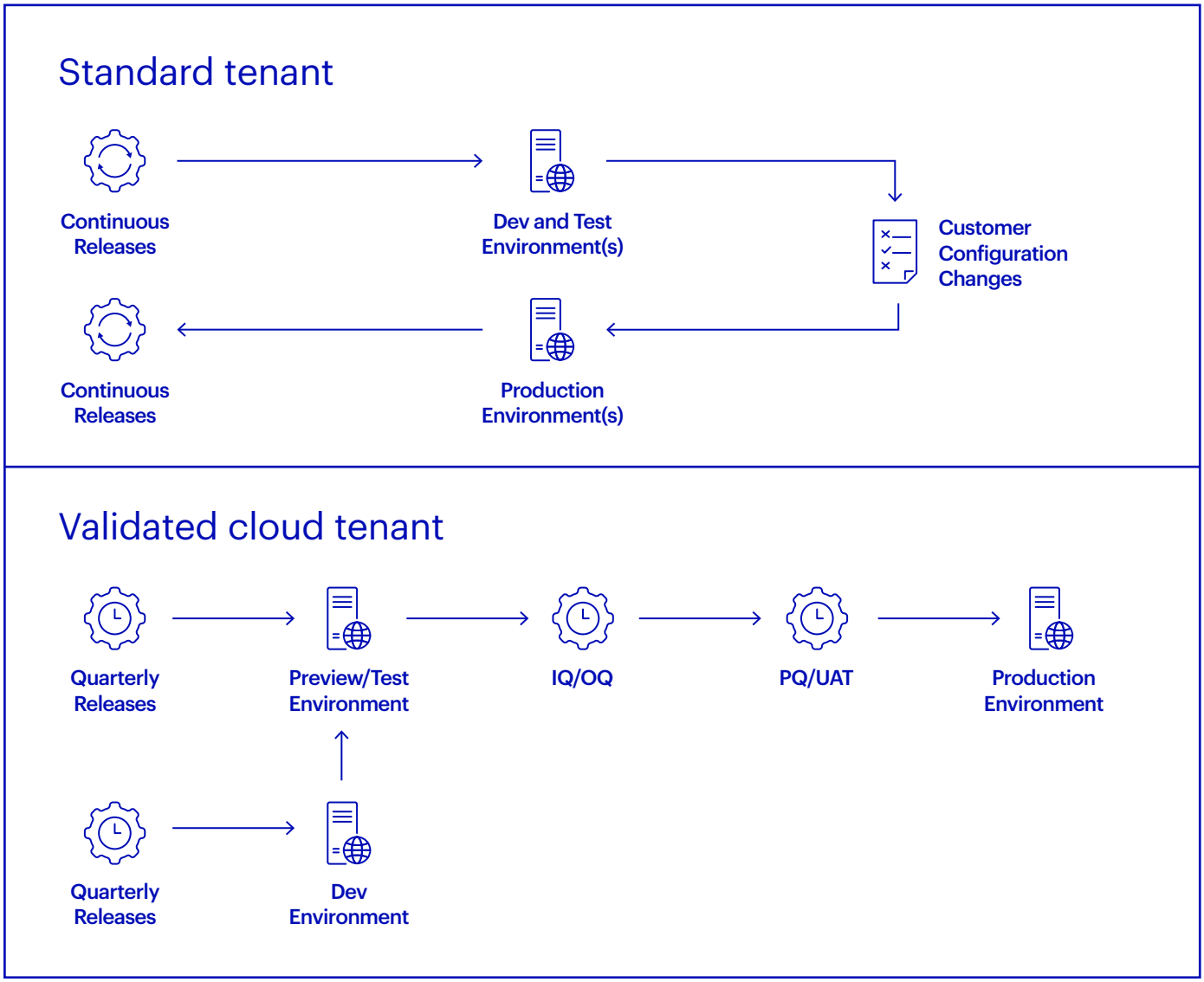


Figure 2. Details of the two types of tenant accounts Benchling offers — Standard and Validated Cloud — depending on customer needs.

Validated Cloud tenancy is designed to ensure compliance with applicable Electronic Records and Electronic Signatures (ERES) regulations set forth by the regulatory agencies (such as FDA, EPA, MHRA, EMEA) that govern the customer's line(s) of business. Benchling provides state-of-the-art documentation and evidence in alignment with FDA's Computer Software Validation (CSV) guidance, as well as the new risk-based Computer System Assurance (CSA) guidance, significantly reducing internal testing, time, and documentation burdens.

Although it is ultimately the customer's responsibility to validate the software for its intended use, Benchling takes a proactive role in deploying and helping maintain the compliance of its software. Benchling recommends that its validation be integrated into the customer organization's overall quality management system, following that system's life cycle or QMS framework and policies. Certain critical aspects and documentation required to support software validation are shown in Figure 3, and are discussed in detail below.

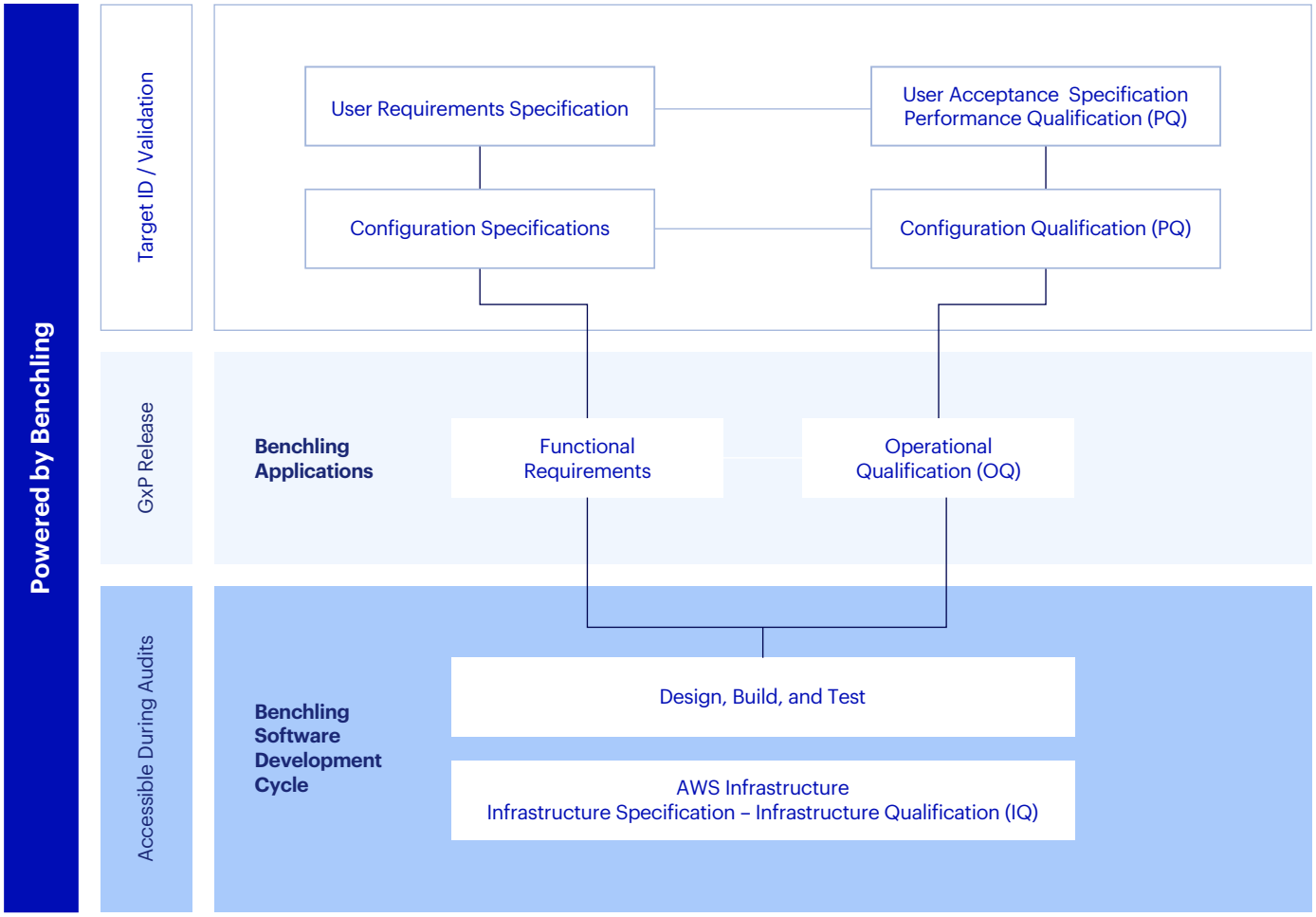


Figure 3. Benchling's qualification, testing, and validation approaches are aligned with industry best practices for CSV and CSA guidelines.

Software Development Lifecycle

Benchling follows an agile software development methodology, and performs extensive testing on all code prior to product delivery. Moreover, for customers who intend to use its software in a highly controlled environment, new releases to Benchling Validation Cloud follow a quarterly deployment model, which enables rapid and systematic responses to emerging threats, regulatory changes and trends.

Infrastructure Qualification

Along with AWS, Benchling partners with a range of industry-leading technology providers to deliver a highly secure and reliable infrastructure for its products. Data and servers are deployed into Virtual Private Clouds (VPCs) isolated from the internet, as well as from Benchling's corporate network. Benchling maintains 100% redundant hardware and data in geographically separate locations to ensure high availability. Content and data are encrypted, backed up daily, and kept for a 35-day rolling retention period. More details can be found in the Security and Privacy section above.

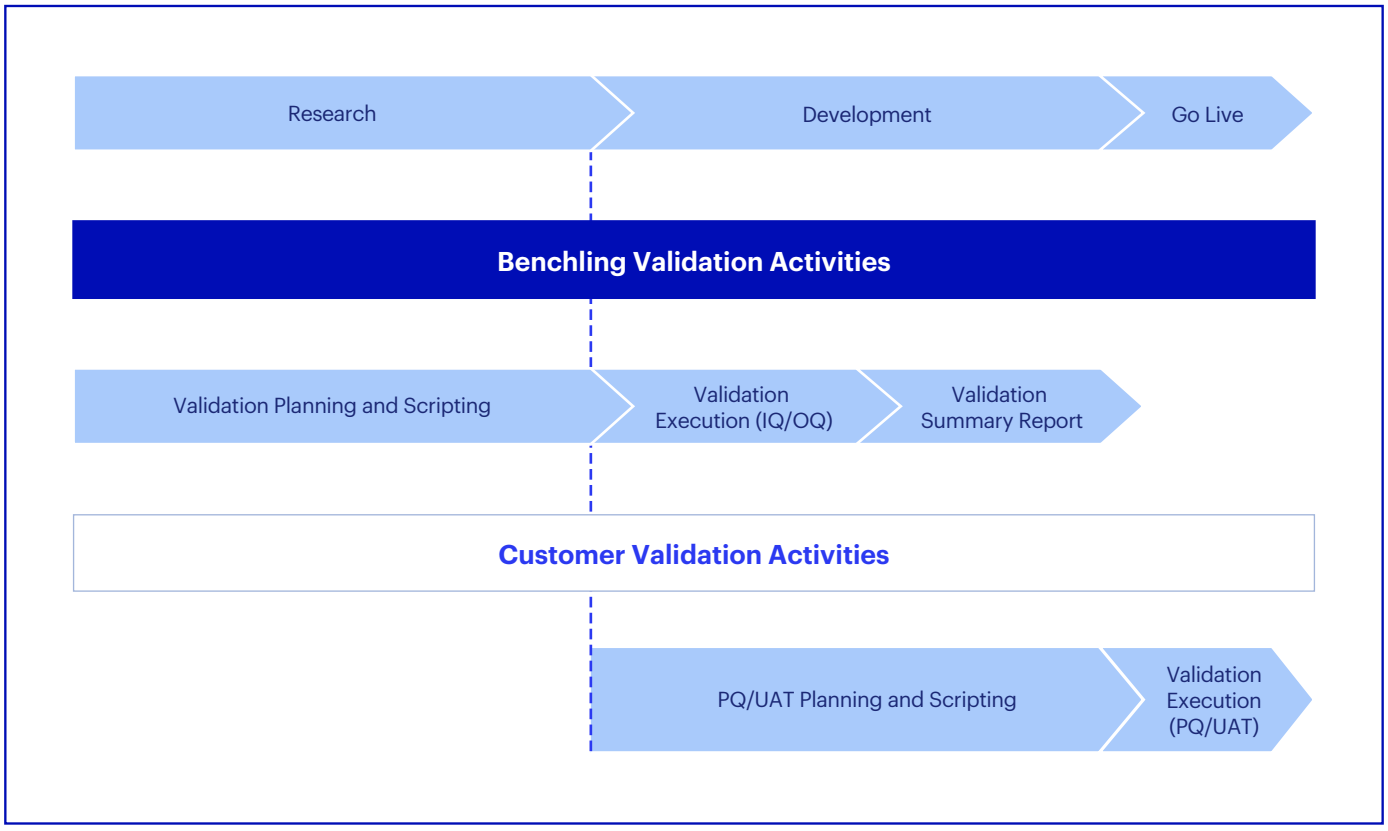


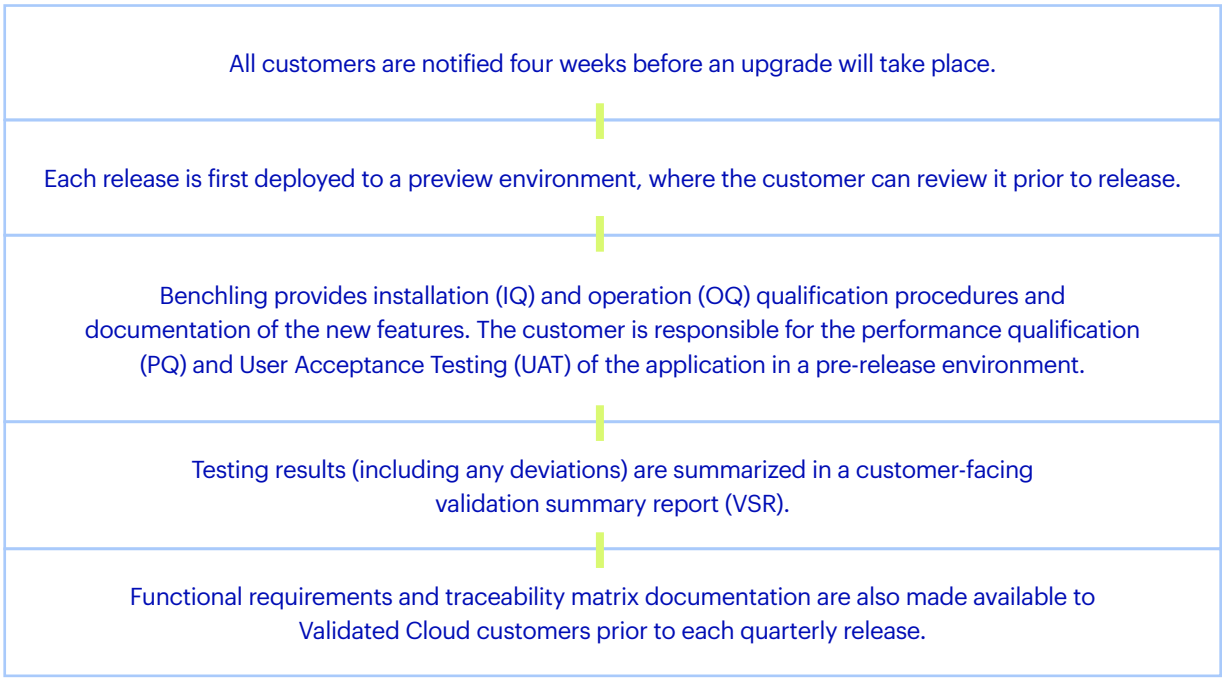
Figure 4. Validation timeline and activities for new releases.

Initial Validation

Throughout the implementation stage, Benchling helps customers establish a validation methodology that facilitates the adoption of software, while maintaining quality and addressing risk. Benchling's services team(s) can be leveraged for system implementation, including configuration of the system in accordance with customer requirements, as well as production of system configuration specification documents. Customers can leverage Benchling's quality validation documentation, Installation and Operational Qualification (IQ/OQ), to streamline the implementation process, freeing up resources to focus on system configuration definition and Performance Qualification (PQ) or User Acceptance Testing (UAT) for intended use. In addition, Benchling is equipped to assist in drafting and completion of intended use validation (i.e. PQ/UAT). Deliverables generated during project implementation, such as configuration specification or PQ/UAT documentation, can be managed by the customer, based on their internal quality guidelines and corresponding Quality Management System (QMS) framework.

Maintaining Validation (Upgrades and Patches)

Benchling Validated Cloud delivers a new version to all customers simultaneously, on a quarterly basis (every three months). The preview validation process is outlined in Figure 4, and proceeds according to the following steps:



Each release is accompanied by a Release Impact Assessment (RIA) detailing all changes, along with the potential impact of each (categorized as high, medium or low), to aid in the customer's risk assessment and determine the validation burden (Figure 5).

Benchling's Customer Success team proactively engages customers to help plan for validation activities and new feature implementation. Customers always have complete control of their validated tenant configuration, including the ability to decide which new features they want enabled, and when.

All new features are categorized into one of two categories: "automatically enabled" or "enabled through configuration." Automatically enabled features are available and activated for immediate use following the upgrade, whereas features requiring configuration can be manually activated by a Benchling representative at any time after the upgrade.

All major new features and functionality will be released behind a feature flag, and can only be enabled through configuration. Patches are released on an as-needed basis, and are designed to address critical and urgent issues uncovered after the General Availability (GA) release has been assessed. Patches do not introduce new functionality or system behavior.

Feature	Enablement	Default Impact	GxP Risk	Feature Description
Core Platform				
When indexing attachment names for search, the name is broken up with special characters like . and -	Auto-On	Visible to All Users	Low	Attachments with periods and dashes can have their text that is separated from individual "." and "-" searched.
Allow filtering by @-mentions	Auto-On	Visible to All Users	Medium	A user can filter results via @mentions.
Notebook				
Mixture preparation tables in notebook	Support	Visible to All Users	High	Mixture prep is a new type of notebook entry table used to prepare a mixture based off of a recipe and record the quantities of materials in the preparation process
Schema Editor				
Datetime is supported as a field type for registry schemas	Support	Visible to All Users	Medium	If enabled, datetime can now be used as a schema field for entities
Support starring entry schemas in filters	Auto-On	Visible to All Users	Low	Users can star entry schemas to be on top of the list for notebook entry schema filters

Figure 4. Validation timeline and activities for new releases.

Audit and Inspection Support

Organizations with GxP requirements are required to establish procedures for conducting quality audits when evaluating and selecting suppliers, contractors, and consultants. Such audits are undertaken to ensure that the company's quality systems are in compliance with GxP regulations, and to determine their overall effectiveness as per 21 CFR 820.22 guidelines.

In order to support compliance with these requirements, and provide vendor qualification audit and Computer System Validation (CSV) support for regulatory inspection. Benchling has established a customer audit program to facilitate and respond to audits conducted by its customers. The company maintains a repository of all necessary documentation, including the following:

Category	Deliverables
Informational Reports	ISO Certifications and Reports
Validation Documentation	Quarterly Release Validation Binders: • Validation Plans • Assessments • Specifications • Executed OQ Scripts • Validation Test Deviations • Traceability Matrices • Summary Reports
Operational Reports	Quarterly Performance Reports Quarterly Availability Reports Penetration Summary Reports DR Postmortem Reports

Figure 6. All necessary documentation - Information reports, validation documentation and operational reports - available to the customers for audit and inspection support.

Quality Management System

Benchling's Quality Management System (QMS) has been developed in alignment with ISO 9001 and ICH (Q9, Q10) guidelines. This quality management system includes SOPs, document management solutions, validation plans, completed-test documentation, and validation summaries. The implementation process is founded on industry best practices, including identification of requirements, continuous communication, training management, vendor management, risk management, change management, and Corrective and Preventative Actions (CAPA) system.

Resource Management and Employee Training

Benchling's resource management process entails structured interviews and rigorous assessments supported by functional area management, ensuring that personnel possess the necessary combination of education, skills and experience to perform their documented job function. Training is assigned based on job function, as well as significance of activities within the organization. Training curriculum includes security awareness, General Data Protection Regulation (GDPR) and regulatory training such as ERES, along with role-based job-specific training. Benchling maintains job descriptions, resumes, and training records for all its employees.

Vendor Management

In addition to AWS, Benchling partners with industry leading solution providers such as Jira and GitHub. Corporate compliance and security teams maintain procedures to ensure that vendors are reviewed and assessed for their quality and security framework, and that all vendors and services receive an appropriate level of oversight. The corporate compliance team conducts assessments, periodic reviews, and audits on all vendors, suppliers and contractors whose services may impact product or process quality.

Risk Management

Benchling's risk management methodology is aligned with ISO 27001 and ICH Q9 Quality Risk Management guidelines. The company maintains a corporate risk register to catalogue and evaluate risks associated with its products and processes. This register is reviewed annually, and is disseminated to the executive management team on a regular basis. Key process areas that employ risk management include Audit Management, Change Management, Computer Systems Validation, Non-conformance Management, Training Management, and Security Management.

Change Management

Benchling's change management program ensures that products, infrastructure, and critical internal business systems are maintained in a state of control with minimal disruption and cost-effective resource utilization.

Benchling's development processes are designed to ensure that all changes to product are evaluated for impact, adequately tested based on assessment, and released to production in a controlled manner. Moreover, changes to GxP impacting systems follow a well-documented change scope: technical and regulatory impact are assessed, pre-approvals are required prior to implementing any change, and testing is performed to assess each proposed change's risk and criticality. Changes are independently reviewed and approved by a corporate compliance team, and change documentation is maintained in a validated QMS.

Document Management

Benchling's process documents follow an ISO documentation hierarchy. The corporate compliance team maintains policies, procedures, and work instructions for each key process area, in a 21 CFR Part 11 compliant Electronic Document Management System (EDMS). This EDMS provides secure role-based access to Benchling's QMS documentation, and prevents unauthorized or unrecorded content changes.

Corrective and Preventive Action (CAPA)

Inputs to Benchling's CAPA policy come from a variety of sources, including internal personnel, process deviations, internal audits, and customer audits and feedback. This process ensures that deviations, gaps, and observations are accurately recorded, an investigation is conducted, root cause analysis (RCA) is captured, and appropriate response and actions are identified.

Conclusion

Life science organizations can utilize Benchling products and services to streamline product development and tech transfer across all phases of research and development, and to efficiently comply with FDA and other global regulatory requirements. Benchling's privacy, encryption, authentication, and business continuity measures help safeguard customer data and information. In addition, Benchling provides comprehensive documentation and packages for GxP environments to help achieve regulatory accreditation and reduce customers' validation burden. Across all these areas, Benchling is well-positioned to assist customers with stringent regulatory processes.