zühlke
empowering ideas

Medical clouds

A case for continuous validation in healthcare, MedTech and pharma

zuhlke.com

Contents

Preface

Part I: Regulatory & technical background 05

1. Regulatory background
- 1.1 Overview 06
- 1.2 European regulations Medical devices & IVDs using cloud solutions 06
- 1.3 United States regulations 08
- 1.4 Standards and guidance 09
- 1.5 Regulatory challenges and solutions 11
- 1.6 Cloud Sovereignty 14

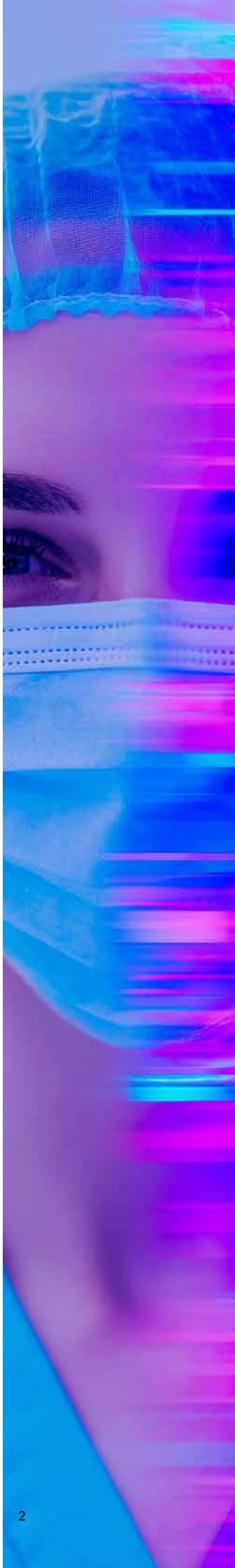
2. Technical background
- 2.1 Overview 15
- 2.2 Types of service 15
- 2.3 Shared responsibility model 15
- 2.4 Regulated landing zone 16
- 2.5 Digital health platforms 17
- 2.6 Regulatory and strategic summary 17

Part II: A practical guide to developing validated cloud-based solutions 20

3. The framework
- 3.1 Concept phase 21
- 3.2 Project phase 25
- 3.3 Live/Maintenance phase 28
- 3.4 Retirement phase 31

4. Appendix
- 4.1 Technical framework 32
- 4.2 Non-binding software validation & data integrity standards 36
- 4.3 Glossary 40

Literature and resources 43



Preface

In recent years, digitalisation has become a key success factor in the healthcare sector. And not just for vendors of dedicated healthcare IT systems. Digitalisation is just as important for medical device and drug manufacturers. The use of advanced digital systems is essential for achieving efficiency, availability and maintainability in almost every field of business. But what makes the health sector different is that, here, digitalisation is central to developing innovative solutions to help us master some of the key challenges facing society today – from an ageing society to ballooning healthcare costs.

With the rise of digitalisation and data-driven technologies, cloud solutions are becoming ever more important. The advantages are clear:

- With a range of well-established, off-the-shelf solutions available, cloud services enable rapid development and testing of new products.
- Compared to on-premise solutions, they are more easily scalable, enabling much shorter times-to-market and earlier profitability.
- Because cloud solutions don't require in-house hardware, companies can slim down their operational and maintenance capacities, potentially resulting in a significant reduction in development and maintenance costs.
- Cloud solutions enable new business models and revenue streams, such as outcome-based pricing, pay-per-use, etc.
- For digital or data ecosystems, using a cloud solution is much easier and faster than building the necessary infrastructure on-premise.
- Interoperability between cloud-based and on-premise solutions has become essential, so platforms can connect and bring related data together.

The advantages of cloud solutions are so great that for some applications they represent the optimal solution. This is especially true for post-market surveillance, which involves constantly feeding data to the solution provider to enable near real-time analysis and constant product improvement. Developing safe, future-proof solutions without predominantly cloud-based solutions and web-based services is becoming increasingly challenging.

Moving to the cloud carries real implications for companies that build safety-critical products in MedTech and pharma. Digitalisation has reshaped many sectors, but medical device and drug manufacturers face a moving regulatory target, and their deployment infrastructure demands rigorous supplier controls, validated systems, and continuous performance monitoring.

In this whitepaper, we demonstrate that it is absolutely possible for companies in the health sector to develop and use cloud solutions safely.

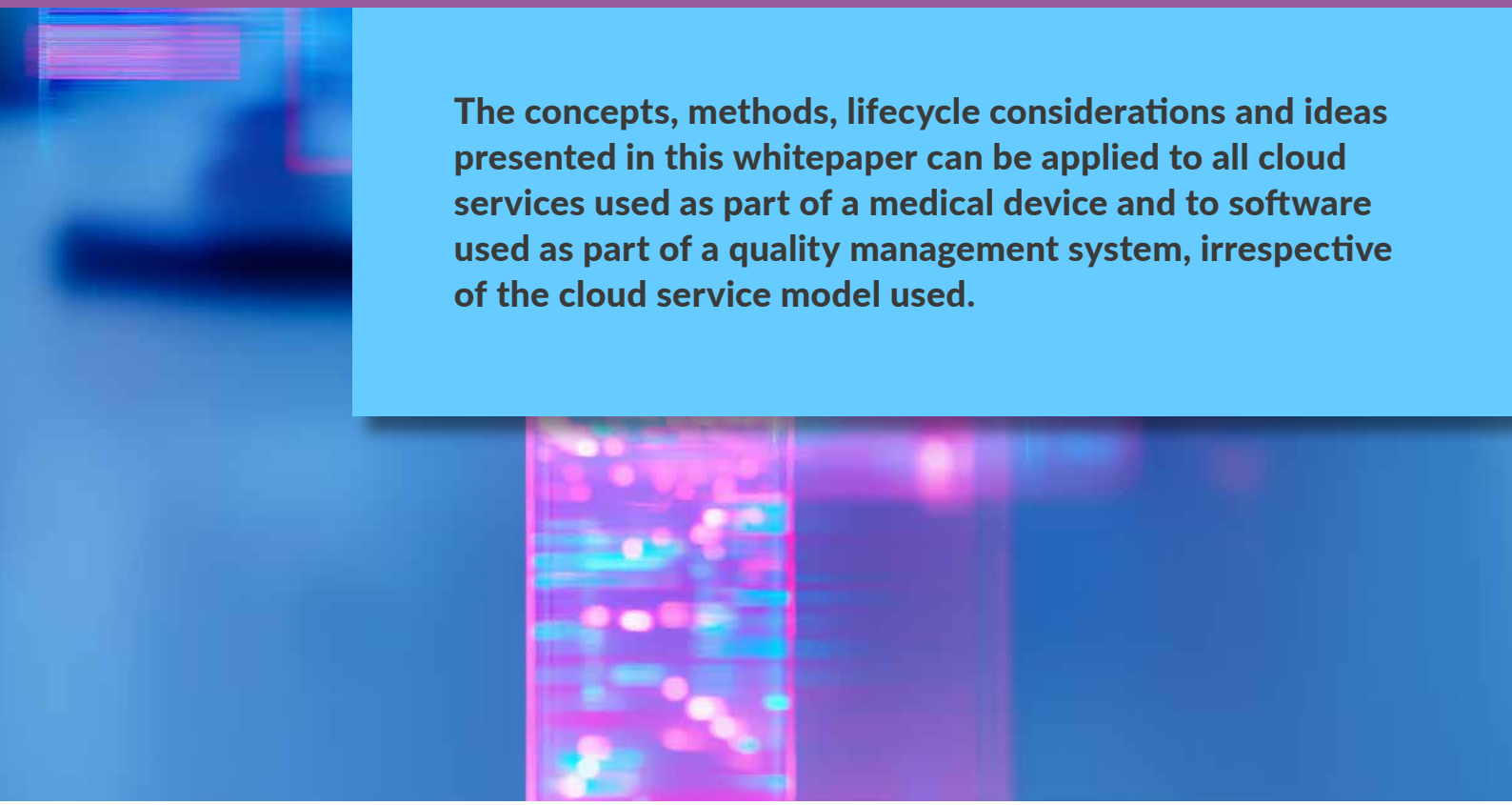
We do, however, have several recommendations for businesses intending to use cloud technologies in a regulated environment, the three most important being:

- Make sure you are familiar with and understand the technology. Companies need to develop a good understanding of data integrity, system ownership, verification and validation activities.
- It is crucial for companies to develop a software mindset when developing new products. Software is never finished – it always needs to be monitored and updated after launch. The same is true for medical products involving cloud technologies.
- Companies need to integrate critical thinking, interoperability, cybersecurity, and risk management into their processes and structures.

In Part I of this whitepaper, we set out a way to make full use of cloud-based systems while maintaining compliance with pharma or medical device regulations. After analysing regulations and cloud service models, we conclude that cloud infrastructure and software can be qualified and validated using a risk-based approach with a focus on critical thinking. By using a mix of controls, provider validation activities, and automated and manual validation tasks, it is possible to achieve continuous validation of cloud systems.

Part II is a guide to analysing and evaluating technical factors and validation and data-integrity factors throughout the lifecycle of a cloud software solution (see the lifecycle models defined in guides such as GAMP 5).

The lessons from Parts I and II are consolidated into a technical blueprint in chapter 4.1. The blueprint shows how Parts I and II come together in practice, using two different cloud providers as examples.



The concepts, methods, lifecycle considerations and ideas presented in this whitepaper can be applied to all cloud services used as part of a medical device and to software used as part of a quality management system, irrespective of the cloud service model used.

Part I

Regulatory background

1. Regulatory background

1.1 Overview

Use of cloud hosting does not by itself determine the regulatory status of a cloud infrastructure or cloud-based product. Rather, the assessment depends on the intended purpose and its functions, users, claims and the data processed. Regulated software in health-related areas covers a broad range of products, applications and services. These include medical devices and in vitro diagnostic medical devices (IVDs), software used in the manufacture, distribution or traceability of medicinal products, and software used for quality management or other regulated processes under ISO 13485, GMP and comparable frameworks.

The same software may be outside medical device regulation when it only supports administration or general wellness but may be regulated when it is intended for diagnosis, prediction, prognosis, monitoring, treatment selection or therapy support. Once a regulated use is identified, responsibility, validation evidence, supplier controls, monitoring, cybersecurity, privacy and change management must be organised accordingly.

For this whitepaper, the regulatory assessment is structured around three recurring situations in which cloud services may:

1. Host or form part of a medical device or IVD software function.
2. Support regulated processes, such as QMS, production, clinical trial, post-market, pharmacovigilance, laboratory or electronic record systems.
3. Store or process regulated data, including personal and health data, clinical trial data, device data and GxP records.

Cloud-based health software is expanding from back-office support into product functions, clinical workflows, remote monitoring, decentralised trial tools and AI-assisted services. For each system, the manufacturer or regulated organisation should first define the use case, user group, regulated output, data categories, system boundary and jurisdictions. These elements determine whether the cloud service is part of a medical device or IVD, supports a regulated process, or stores regulated data. They also define the required controls, evidence and lifecycle activities.

1.2 European regulations: Medical devices and IVDs using cloud solutions

European Union and Swiss regulations related to cloud solutions that host, or form part of, a medical device or IVD are largely governed by equivalent regulatory requirements. This is because Switzerland's Therapeutic Goods Act, Medical Device Ordinance, and Ordinance on In Vitro Diagnostic Medical Devices are, in most areas, based on the European Medical Device Regulation (EU) 2017/745 (EU MDR) and the In Vitro Diagnostic Regulation (EU) 2017/746 (EU IVDR).

Manufacturers are required to include the relevant cloud functions, interfaces, operating platform, supplier dependencies and service assumptions in the device's Technical Documentation that allows an assessment of the conformity to the EU MDR or IVDR. The Technical Documentation includes design and manufacturing information, identification of suppliers and subcontractors, applicable general safety, and performance requirements, the methods used to demonstrate conformity, risk management evidence, and product verification and validation.

The General Safety and Performance Requirements (GSPR) specified in the regulation's Annex I require that software that is part of a device or is a device by itself is designed for repeatability, reliability, and performance in line with its intended use. It must be developed and manufactured according to the state-of-the-art which includes following dedicated processes for software lifecycle, usability, risk management, information security.

The MDR and IVDR also require manufacturers to define minimum requirements for hardware, IT networks and IT security measures, including protection against unauthorised access, that are necessary to run the software as intended. When a medical function is hosted in the cloud the manufacturer remains responsible for risk management, clinical or performance evaluation, conformity assessment, post-market surveillance, vigilance and corrective actions. Cloud infrastructure may support post-market surveillance, but only if data flows, records, access rights, monitoring and service changes are properly controlled.

Cloud-based QMS, GxP and regulated operational systems

Manufacturers of medical devices and IVDs must implement and maintain a quality management system (QMS), which today, with global operations and remote working, is often operated in the cloud. Systems used for design and development, complaint handling, CAPA, supplier control, training, documentation or post-market surveillance need to be covered by the QMS and require computer system validation (CSV) according to their role and risk.

For medicinal products, EU GMP Annex 11 requires computerised systems used in GMP-regulated activities to be appropriately controlled. In practice, this means that the relevant applications must be validated and the supporting IT infrastructure must be qualified. It also requires that replacing a manual operation with a computerised system does not reduce product quality, process control or quality assurance, and does not increase the overall process risk. Annex 11 turns this principle into operational requirements: documented risk management, system inventory, system descriptions for critical systems, user requirements based on documented risk assessment and GMP impact, traceability of requirements, appropriate supplier assessment, validation documentation, data checks, secure data storage, backup and restore checks, change and configuration management, periodic evaluation, access control, audit trails, incident management, business continuity, and archiving.

EU GMP Annex 15 adds the validation structure for facilities, equipment, utilities and processes used in medicinal product manufacturing. It requires qualification and validation to be planned, documented and approved, with change control and revalidation where needed. For cloud systems used in GMP processes, Annex 15 is relevant when defining validation planning, qualification rationale, change impact assessment and evidence needed to support continued validated state.

Annex IX of the MDR obliges manufacturers to establish methods for monitoring the efficiency of the quality management system, particularly when achieving the required product quality and conformity. This can be interpreted as including cloud solutions used in a quality management context. The IVDR mandates the validation of software used as part of a product, but does not make stipulations regarding software used during production.

Storing and processing regulated data

The European Data Protection Regulation (GDPR) applies where personal data is processed in the EU or where the processing falls within its territorial scope. For cloud use, the actionable requirements are to define controller, processor and sub-processor roles; document a lawful basis for processing; define a condition for processing health data or other special-category data; implement processor contracts; use appropriate technical and organisational measures; respect data subject rights; assess cross-border transfer mechanisms; and perform a Data Protection Impact Assessment (DPIA) where processing is likely to result in high risk, for example large-scale processing of sensitive data.

Additional EU rules may apply depending on the organisation and use case. NIS2, which applies to organisations with 50+ employees or more than €10 million in turnover, requires cybersecurity risk-management measures and reporting obligations for in-scope sectors, including health and digital infrastructure.

The EU Data Act creates obligations for providers of data processing services, including cloud and edge services, with a focus on switching, exportable data and reducing contractual, technical and organisational barriers to switching.

The EU AI Act applies to AI systems placed on the EU market or used in the EU, which means most AI-based software intended for medical purposes is rated high-risk and therefore requires dedicated AI-related risk management, high-quality data sets, user information, and human oversight.

The European Health Data Space (EHDS) came into force in March 2025 and will introduce phased rules for electronic health data access, exchange, secondary use and Electronic Health Record (EHR) system interoperability.

The Swiss Federal Act on Data Protection (FADP) applies to Swiss personal data processing and has been operational since September 2023. It should be assessed together with the GDPR where systems cover both EU and Swiss persons. Cloud use usually requires clear allocation of controller and processor roles, data processing agreements, transparency, proportionality, adequate security, cross-border transfer controls and retention rules.

For clinical research involving EU or Swiss individuals, cloud-based clinical trial systems must maintain subject protection, privacy, data quality, traceability, retention, and inspection access in line with the EU Clinical Trials Regulation or the Swiss Human Research Act (HRA), as applicable.

1.3 United States regulations

Medical devices and IVDs using cloud solutions

Where a cloud-hosted function is a device software function, meaning it meets the definition of a device per US Federal Food, Drug, and Cosmetic Act (FD&C Act), the manufacturer must determine the applicable classification, product code, premarket pathway and post-market obligations. FDA lists examples of device software functions that are the focus of FDA oversight, including software that transforms a mobile platform into a regulated device, controls another device, or analyses patient data for medical purposes. Cloud-hosted algorithms and cloud-connected control functions should therefore be included in the software documentation's requirements specifications, device architecture, detailed design, risk analysis, verification and validation evidence, cybersecurity documentation and labelling as applicable.

Cyber devices are classified as devices that include software, can connect to the internet, and have characteristics that could expose them to cybersecurity threats. This category covers all cloud solutions. For these devices, section 524B of the FD&C Act establishes additional premarket submission obligations. Submissions must provide information showing that cybersecurity requirements are met, including a plan to monitor, identify and address post-market cybersecurity vulnerabilities and exploits, and processes to provide reasonable assurance that the device and related systems are cybersecure, including updates and patches.

Cloud-based QMS, GxP and regulated operational systems

Cloud software used in production or the QMS must be controlled under the FDA Quality Management System Regulation (QMSR), which recently incorporated ISO 13485 by reference. Consequently, the same requirements as for Europe apply to such systems.

For drug manufacturing, 21 CFR 211.68 permits the use of computers and related systems if they are routinely calibrated and inspected or checked under a written programme. Written records of those checks and inspections must be maintained. For computer and related systems, appropriate controls must ensure that changes to master production and control records or other records are made only by authorised personnel. Input and output must be checked for accuracy, with the degree and frequency based on system complexity and reliability.

For clinical investigations, the applicable FDA rules depend on product type and trial role. Cloud systems used in clinical investigations need to preserve records required by the applicable clinical investigation regulations and, where electronic records or signatures replace paper, 21 CFR Part 11

applies. FDA guidance on electronic systems, records and signatures in clinical investigations is non-binding, but it explains how FDA evaluates trustworthiness, reliability and equivalence of electronic records and signatures in clinical investigations.

Storing and processing regulated data

The Health Insurance Portability and Accountability Act (HIPAA) applies to covered entities and business associates that create, receive, maintain or transmit electronic protected health information. HIPAA covered entities or business associates may use cloud services to store or process electronic Personal Health Information (ePHI) if it enters into a HIPAA-compliant business associate agreement with the cloud service provider and otherwise complies with the HIPAA rules. A cloud service provider is a business associate when it creates, receives, maintains or transmits ePHI on behalf of a HIPAA covered entity or another business associate, including where the ePHI is encrypted and the provider does not hold the decryption key.

The HIPAA Security Rule requires regulated entities to implement administrative, physical, and technical safeguards that protect the confidentiality, integrity and availability of ePHI. For cloud use, this translates into documented risk analysis and risk management, access controls, audit controls, transmission security, contingency planning, incident response, and management of business associates.

The HIPAA Privacy Rule sets limits and conditions on uses and disclosures of protected health information and gives individuals rights over their health information. For cloud systems, this affects data minimisation, role-based access, disclosure controls, patient access, correction processes and downstream sharing. The Privacy Rule requires reasonable steps to limit uses, disclosures and requests to the minimum necessary for the intended purpose, subject to specified exceptions.

1.4 Standards and guidance

Standards and guidance documents do not have the same legal status as regulations. Some standards support presumption of conformity, some are incorporated by reference, and some guidance documentation describes regulatory or industry expectations. For cloud use, their practical value is that they translate regulatory requirements into controls and evidence that can be planned, implemented, reviewed and inspected.

This section maps the most relevant standards and guidance documents to the different cloud-use situations. Appendix 4.2 provides short descriptions of the individual documents and explains their relevance for validation, data integrity, supplier control, infrastructure qualification, cybersecurity and privacy.

Cloud services that host or form part of a medical device or IVD software function

Documents relevant for the quality management system, risk management, software lifecycle processes, health software product requirements, cybersecurity activities, software qualification and classification, technical documentation, verification and validation evidence:

- ISO 13485 (Medical device QMS)
- ISO 14971 (Medical device risk management)
- IEC 62304 (Medical device software lifecycle)
- IEC 82304-1 (Health software product safety)
- IEC 81001-5-1 (Health software cybersecurity)
- MDCG 2019-11 (Software qualification and class)
- MDCG 2019-16 (Medical device cybersecurity)
- FDA Off-The-Shelf Software guidance (OTS software evidence)
- FDA device software guidance (Device software evidence)
- FDA cybersecurity guidance (Premarket cyber evidence)

Cloud services that support QMS, production, GxP or regulated operational systems
Documents relevant for computerised-system validation / assurance, GMP system validation, IT infrastructure qualification, supplier oversight, data integrity, quality risk management, periodic review, change control, backup, restore, business continuity and archiving:

- ISO 13485 (Medical device QMS)
- AAMI TIR 36 (Regulated software validation)
- ISO/TR 80002-2 (QMS software validation)
- FDA CSA guidance (Risk-based software assurance)
- EU GMP Annex 11 (GMP computerised systems)
- EU GMP Annex 15 (Qualification and validation)
- ISPE GAMP 5 Second Edition (GxP system validation)
- ISPE IT Infrastructure Guide (GxP infrastructure control)
- PIC/S PI 011 (GxP computerised systems)
- PIC/S PI 041 (GMP/GDP data integrity)
- ICH Q9(R1) (Quality risk management)
- ICH Q10 (Pharmaceutical quality system)

Cloud services that support clinical-trial or healthcare service systems
Documents relevant for cloud-based EDC, eSource, eConsent, ePRO, eCOA, eTMF and remote-trial systems through sponsor oversight, data lifecycle control, audit trails, access control, retention and inspection readiness:

- EMA eSystems trial guideline (Clinical trial e-system control)
- FDA clinical eSystems guidance (US trial e-records control)
- ISPE GCP Systems Guide (Computerised GCP systems)
- ICH E6(R3) (GCP trial records and data)

Cloud services that store or process regulated data
Documents relevant for cloud security governance, provider and customer control allocation, privacy controls, PII protection, HIPAA safeguards, incident handling and risk-based security management:

- ISO/IEC 27001 (Information security management)
- ISO/IEC 27017 (Cloud security controls)
- ISO/IEC 27018 (PII protection in public cloud)
- ISO/IEC 27701 (Privacy information management)
- NIST CSF 2.0 (Cybersecurity risk framework)
- NIST SP 800-66 (HIPAA security implementation)
- HHS HIPAA cloud guidance (HIPAA cloud service duties)

Cloud services that include AI or LLM-supported regulated workflows
Documents relevant for the classification, change control, model update planning, cybersecurity, monitoring, GxP impact assessment and lifecycle evidence for AI or LLM functions operated in cloud environments:

- ISO 42001 (AI management system)
- AAMI TIR 34971 (AI / ML risk management)
- IEC 81001-5-1 (Health software cybersecurity)
- EU AI Act guidances (AI system definition, prohibited practices)
- ISPE GAMP 5 Second Edition (GxP system validation)
- FDA PCCP guidance (AI change control plans)
- FDA device software guidance (Device software evidence)

1.5 Regulatory challenges and solutions

Cloud use in regulated health software should be linked to defined regulatory decisions. The table below identifies those decisions, states the control issue behind them and points to the sections that describe their implementation. Part 1 defines the regulatory background as well as the technical background, including cloud service models, shared responsibility and regulated landing zones. Part II describes the implementation of regulated cloud applications during concept, project, live, maintenance and retirement phases.

Regulatory Challenge	Solution / Implementation
Scope and classification A cloud service can host data, execute a medical algorithm, support QMS, support manufacturing, provide clinical-trial functionality or enable a healthcare service. Treating all cloud services alike leads to unclear scope and excessive or insufficient controls.	**Determine cloud role** Document the intended use, regulated functions, user groups, data categories, interfaces, jurisdictions, records, suppliers and system boundary. Use this boundary for software classification, validation scope, data protection assessment and supplier control. Part II, 3.1 Concept phase
Device evidence Cloud-hosted device functions must still meet device requirements for safety, performance, risk management, software lifecycle, information security, verification, validation and technical documentation. The cloud platform, interfaces and service assumptions can affect that evidence.	**Maintain technical documentation** Include cloud functions, interfaces, operating platform, service assumptions, supplier dependencies, cybersecurity controls and verification or validation evidence in the technical documentation. ➔ Part I, 2.2 Types of service ➔ Part I, 2.3 Shared responsibility model ➔ Part II, 3.2 Project phase
Cloud-based QMS and operations QMS and production systems often rely on outsourced cloud services. Regulations and incorporated QMS requirements expect supplier and outsourced-process controls where those services affect product conformity, records or regulated processes.	**Supplier controls** Define supplier qualification, responsibility split, service scope, quality agreement, SLA, audit or assurance evidence, change notification and record access. Keep the level of control risk-based and documented. ➔ Part I, 2.3 Shared responsibility model ➔ Part II, 3.1 / 3.2 Concept / Project phase
GMP computer systems Cloud systems used in GMP activities are computerised systems. EU GMP Annex 11 requires validated applications, qualified IT infrastructure, risk management, supplier agreements, system inventory, data controls, backup, restore checks, access control, audit trails, incident management, business continuity and archiving.	**Validate GMP systems** Define intended GMP use, user requirements, risk assessment, validation plan, infrastructure qualification rationale, supplier responsibilities, data integrity controls and periodic evaluation. Keep evidence linked to product quality, patient safety and data integrity. ➔ Part I, 2.4 Regulated landing zone ➔ Part II, 3.1 to 3.3

Change frequency and control Cloud services change more frequently than many on-premise systems. This is normal for modern software operations. The regulatory question is how changes are detected, assessed and documented when they may affect intended use, safety, performance, data integrity, cybersecurity, privacy or regulated records.	**Monitoring and impact assessment** Monitor provider notices, release notes, service health, security advisories and configuration logs. Assess impact on intended use, safety, performance, data integrity, cybersecurity, privacy and records. Trigger verification, validation or a documented rationale. Part II, 3.3 Operations and maintenance phase Appendix 4.1 Technical framework
Data integrity and electronic records Electronic records must remain authentic, accurate, complete, retrievable and protected. This requires validation, accurate copies, retention, authorised access, audit trails, authority checks, training, accountability policies and documentation controls for closed systems.	**Build record controls** Specify access rights, authentication, audit trails, time synchronisation, record copies, retention, backup, restore testing, electronic signatures, administrator actions and inspection access before implementation. ➔ Part I, 2.4 Regulated landing zone ➔ Part II, 3.3 to 3.4 Live to Retirement phase
Clinical-trial records Cloud trial systems must preserve trial conduct evidence and data quality. The EU CTR requires a clinical trial master file that is readily available and directly accessible, with archiving for at least 25 years. US IND and IDE rules require adequate, accurate, complete and retained records.	**Define ownership and control** Define record ownership, eTMF or trial-system scope, access control, audit trails, retention period, export, archive format, migration control and inspection access. Ensure that transfer of custody is documented where applicable. ➔ Part II, depending on trial
Privacy and health data Cloud systems may process personal data, health data or special-category data. GDPR requires processor selection with sufficient guarantees, processor contracts, security measures appropriate to risk and DPIA where processing is likely to result in high risk.	**Set privacy controls** Define controller, processor and sub-processor roles. Establish processing agreements, lawful basis, health-data conditions, transfer mechanisms, retention rules, data subject processes, security controls and DPIA where required. ➔ Part II, 3.1 Concept phase ➔ Part II, 3.4 Retirement phase
HIPAA cloud hosting A cloud service provider is a business associate when it creates, receives, maintains or transmits ePHI on behalf of a covered entity or business associate, including encrypted ePHI where the provider lacks the decryption key.	**Execute BAA and safeguards** Execute a HIPAA-compliant Business Associate Agreement (BAA). Define risk analysis, risk management, access controls, audit controls, integrity controls, authentication, transmission security, incident response and business associate oversight. ➔ Part II, 3.1 to 3.3 Concept to Live phase

Cybersecurity duties Connected device functions, healthcare services and in-scope digital infrastructure require cybersecurity controls. EU NIS2 requires proportionate technical, operational and organisational measures. FDA section 524B requires cyber-device submission information, including post-market vulnerability handling and cybersecure related systems.	**Run security controls** Define cybersecurity requirements, a threat model, access control, vulnerability handling, incident response, backup, disaster recovery, supply-chain security, update process and security monitoring according to the applicable framework. ➔ Part II, 3.1 to 3.3 Concept to Live phase
Availability and continuity Cloud-hosted regulated functions and records must remain available according to their intended use and retention needs. Loss of availability can affect patient safety, product quality, trial data, ePHI, regulated records or business continuity.	**Define continuity controls** Define availability targets, backup, restore testing, disaster recovery, failover, manual workarounds, continuity responsibilities and recovery evidence. Align these controls with system criticality and supplier commitments. ➔ Part I, 2.4 Regulated landing zone ➔ Part II, 3.1 to 3.3 Concept to Live phase
Incident and reporting duties Cloud incidents can trigger different response paths, including device vigilance, field safety action, GxP deviation, CAPA, data breach notification, HIPAA breach handling, NIS2 reporting or cybersecurity vulnerability handling.	**Define incident routes** Map incident types to regulatory reporting, escalation and CAPA processes. Include provider notification timelines, evidence preservation, technical triage, business impact assessment and communication responsibilities. ➔ Part II, 3.2 / 3.3 Project / Live phase
Cloud exit and switching Regulated data and records must remain available after provider change, service termination or system retirement. The EU Data Act also requires providers of data processing services to remove switching obstacles and include switching terms in contracts.	**Plan exit and export** Define exportable data, digital assets, formats, retrieval period, transition support, deletion, retention, archive access, migration validation, business continuity and responsibilities before go-live. ➔ Part II, 3.4 Retirement phase.
Use of AI / LLM AI or LLM functionality has different regulatory consequences depending on the intended use. Under the EU AI Act, an AI system is high-risk where the Article 6 criteria are met, including certain product or safety-component uses linked to Annex I legislation and third-party conformity assessment.	**Classify AI function** Classify each AI or LLM function by intended purpose, user, output, data type, human oversight, regulated decision impact and jurisdiction. Align AI controls with device, QMS, GxP, clinical or privacy requirements. ➔ Part II, 3.1 to 3.2 Concept to Live phase

1.6 Cloud Sovereignty

Let's briefly look at how each of the major Cloud Providers are addressing this concern.

Amazon AWS

AWS European Sovereign Cloud (ESC) — launched 2026, a fully independent cloud operated by a German legal entity with EU-only personnel.

- Separate partition architecture
- EU-only key management
- Designed for GDPR, DORA, NIS2 compliance
- Digital Sovereignty Pledge — commitments around data residency, encryption, and customer control.
- Existing EU regions still support residency requirements for less strict workloads

2. Technical background

2.1 Overview

Over the last couple of years, large volumes of investment in cloud technologies have given rise to a number of different cloud solutions. The wide range of solutions can make it hard to identify the best solution for the task at hand. For selected services, cloud providers are taking on responsibilities which usually reside with the legal manufacturer. For you as the user, taking advantage of provider services and avoiding duplication of validation activities performed by the provider can reduce your own validation workload. There is no right or wrong answer. The key is that the chosen solution should meet your organisation's requirements to the maximum extent possible.

To ensure that you are able to identify potential pitfalls and understand and evaluate the impact of cloud-based services and infrastructure, it is important to familiarise yourself with the unique characteristics of and basic concepts underpinning different cloud offerings. This will help you select the most efficient, most pragmatic approach and help ensure that your cloud systems are qualified and safe.

2.2 Types of service

A characteristic of cloud services is that they offer various levels of integration. Most sources distinguish three levels, which differ in how responsibility is split between the cloud service provider and the regulated user (figure 2).

Infrastructure as a Service (IaaS)
The Infrastructure as a Service (IaaS) model represents the lowest level of dependency on and integration with the cloud provider. In this model, the client makes use of basic cloud IT building blocks only, typically including networking features, computers (virtual or on dedicated hardware) and storage. Services and products are built on top of the cloud infrastructure and remain entirely under the client's control. The cloud service provider patches and updates the underlying infrastructure only.

Examples include virtual networking components like elastic load balancers and firewalls. Patching the operating system and software installed on a virtual machine instance for example, would remain the responsibility of the client.

Platform as a Service (PaaS)
Platform as a Service (PaaS) consists of the infrastructure from the IaaS model, with the addition of services and tools for deploying and managing your applications.

Software as a Service (SaaS)
Software as a Service (SaaS) provides the client with a complete product run and managed by the service provider. The term Software as a Service is generally used to refer to end-user applications. SaaS includes the integration of fully developed user-facing components provided by the cloud service provider. A common example of a SaaS application is webmail.

2.3 Shared responsibility model

Large cloud providers are aware that their services may also be used in regulated environments and have adapted their services to accommodate the needs of these environments. While this does not include the ability to block or restrict updates to services, which for security reasons in particular would not be a viable solution for the cloud provider, they have developed a model to delineate responsibilities of the provider and of the regulated user. This is generally referred to as the shared responsibility model.

The idea behind this model is simple. Cloud service providers take responsibility for properly developing, maintaining and updating their services. The regulated user is responsible for products or services built us these services and for configuring these services. The cloud provider therefore offers the client guarantees that the service will work exactly as specified and will feature a stable interface. What goes on behind the interface is invisible to and cannot be managed by the client. The client is responsible for verifying and validating the solution based on the interface specification.

All major cloud service providers have outlined how they manage the responsibilities assigned to them under the shared responsibility model and how they comply with regulations for developing and updating cloud services and infrastructure. We strongly recommend using your cloud service provider's certification status as part of your validation activities.

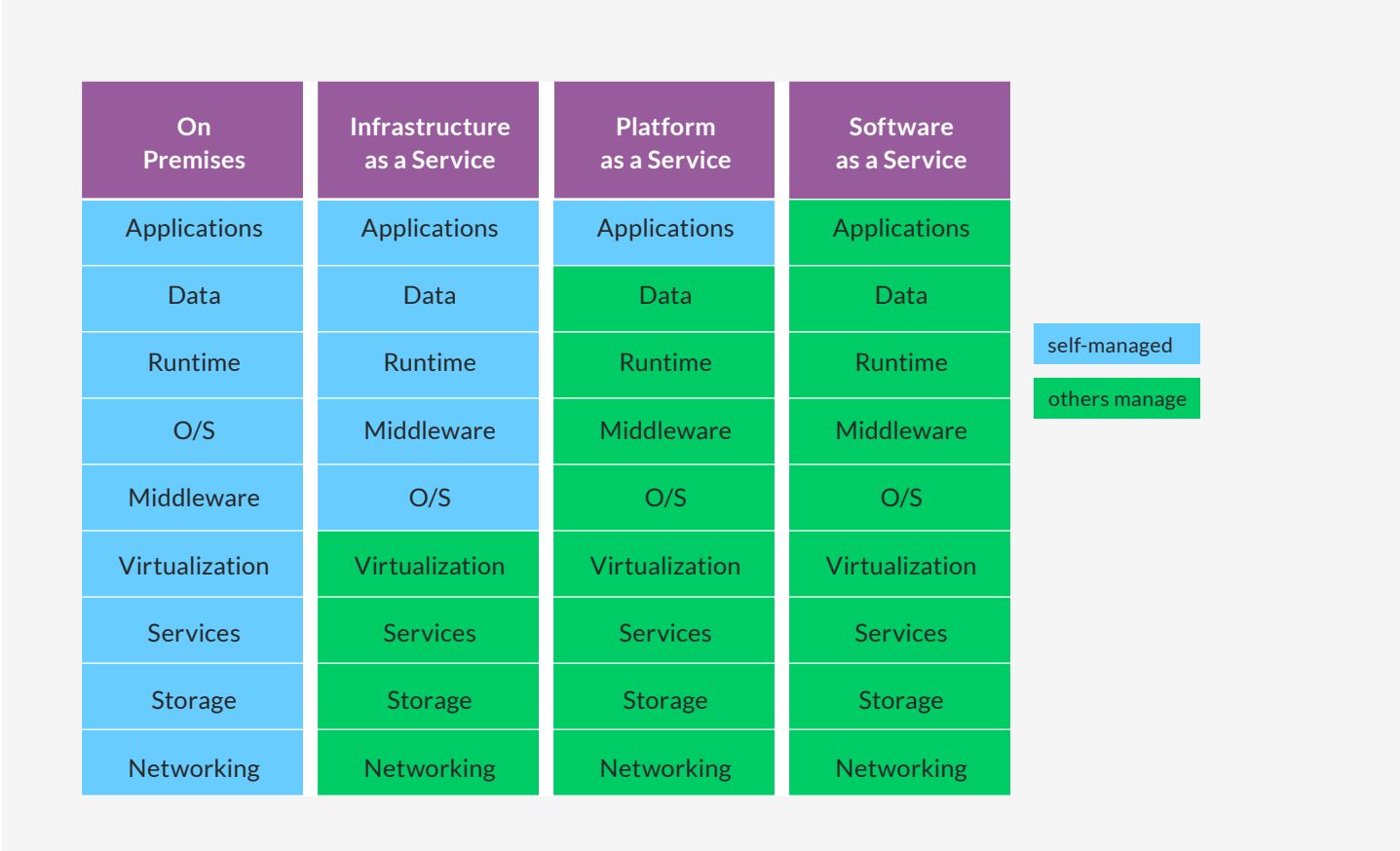


Figure 2: Differences between On Premises, IaaS, PaaS and SaaS.c.

2.4 Regulated landing zone

As mentioned previously, regulated users have additional requirements when integrating or using a cloud-based system. A GxP compliant system, for example, requires features such as the ability to back up and restore data, the ability to properly manage access rights and the ability to produce an audit trail showing interactions with the system (figure 3). Because these requirements apply to all cloud-based products a regulated user develops or uses, the functions and services required to meet these requirements can be centralised and reused for other products. Bundled together and centralised, these capabilities are commonly referred to as a regulated landing zone, i.e. a well-architected, multi-account environment that is scalable and secure, is based on cloud infrastructure, but is not part of a specific system.

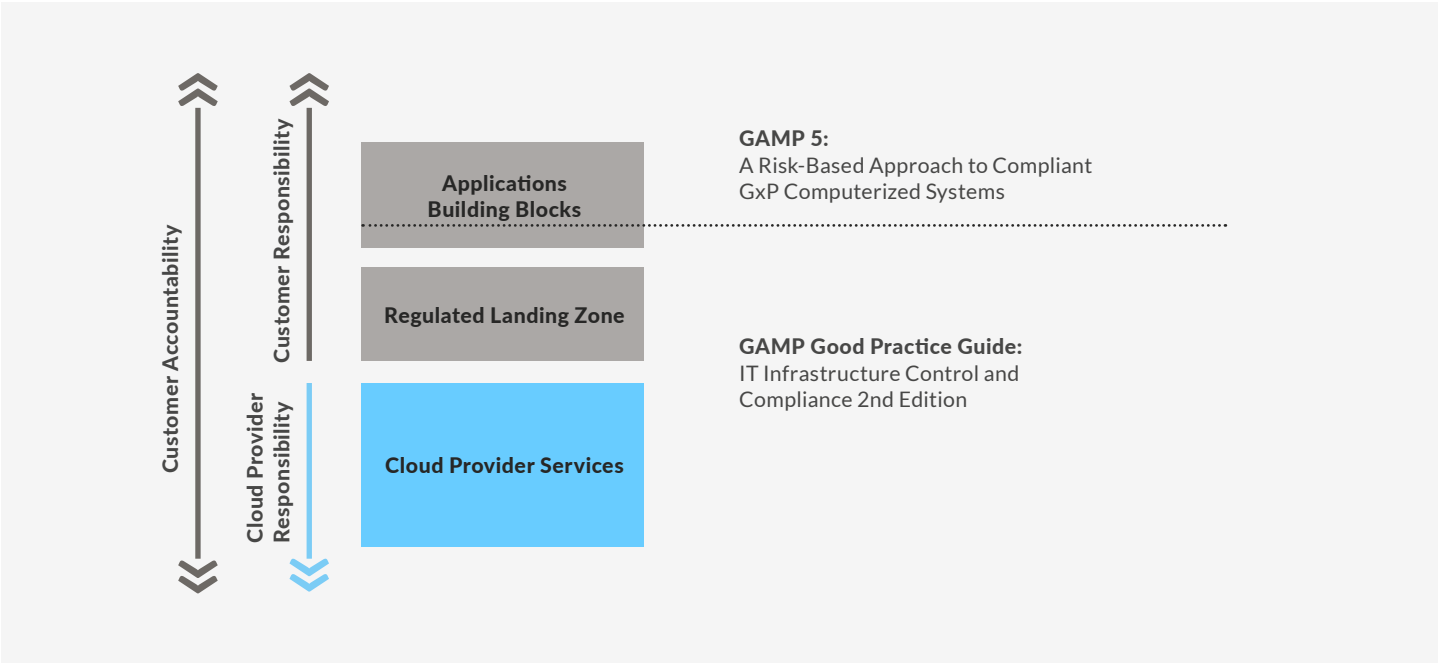


Figure 3: Requirements of compliant systems.

2.5 Digital health platforms

For a regulated user thinking about building multiple cloud-service-based products, digital health platforms (DHP) are well worth a look. These platforms generally include a regulated landing zone and assume responsibility for and manage the infrastructure. In systems based on digital health platforms, the line between provider and client responsibilities is shifted towards the actual healthcare application. Digital health platform providers are usually ISO 13485 certified, thereby simplifying supplier qualification. ISO 13485 certification can also be taken into consideration for validation activities.

For a comprehensive guide to choosing the right digital health platform for your products, see our companion whitepaper *Digital health platforms: for a future of more connected end-to-end patient experiences.*

2.6 Regulatory and strategic summary

The use of cloud solutions means adopting a fundamentally different perspective on data integrity, system ownership, verification and validation. Once a regulated company starts to employ cloud infrastructure or services, it no longer has direct control over systems and data. Added to this, existing regulations and guidance documents still leave plenty of room for interpretation, as they do not generally set out specific requirements for cloud systems. This, in combination with a reluctance to move away from established qualification and validation models, has resulted in considerable uncertainty around the use of cloud services and significant pushback.

Regulators in Europe and the US already accept the use of cloud systems as part of a medical device or as part of quality management software subject to validation. Newer guidance documents and standards are starting to be adapted for cloud systems, and to cover areas such as cybersecurity, data integrity and qualification/validation. The advent of a new, risk-based approach requires a new understanding of computer system validation. This goes hand in hand with a paradigm shift in computerised systems validation, which elevates critical thinking governed by computer system assurance (CSA) above extensive testing through computer system validation (CSV).

Still under development is the long-awaited Computer Software Assurance guidance document, which advocates a software validation approach based on critical thinking, rather than solely on execution of validation test cases for every bit of software functionality and infrastructure. The FDA

has also launched multiple strategic initiatives and programmes centred around the regulation of new technologies in pharmaceutical and medical device development and production (for example the Strategic plan on regulatory science and the Emerging Technology Program). Their aim is to facilitate the use and promote the adoption of new technologies. They take the view that new technologies offer significant potential for achieving improved product safety and more reliable provision of medicinal products and devices.

The FDA's CSA approach signposts the direction needed to meet the challenge of validating cloud applications and infrastructure. Medical device manufacturers should tackle cloud validation by using a risk-based approach, as has long been proposed in standards and guidance.

A thorough understanding of the technology is a key factor. It is important to be clear about the differences between IaaS, PaaS and SaaS. It is important to understand the key elements of cloud system design and how cloud technology and service models can be used to build solutions able to satisfy medical device requirements. Concepts such as the regulated landing zone and the shared responsibility model facilitate the creation of such solutions. Major cloud service providers offer guidance for regulated companies on putting these concepts into practice. Alternatively, some DHP providers guarantee that their services are regulatory compliant, though these providers may charge more for their services.

Lifecycle activities for medical device products and for software systems used as part of quality management systems need to be extended to include cloud-based software. These can be complemented by cloud-specific activities and quality management processes.

1. Incorporate an evaluation of cloud service providers into the initial concept phase. Be aware, however, that conventional auditing and qualification of cloud service providers may be impossible or at least very cumbersome. Get the QA department involved, define the level of supplier qualification, and adapt and establish SOPs for connecting to external services and/or infrastructure. Use a consistent, risk-based approach right from the development phase.

2. The process used during the development phase should take into account the capabilities required for and risks involved in implementing functionality such as user management, audit trails, change logs and scripting for infrastructure backup. Make the maximum possible use of tools and services provided by the cloud provider. Perform risk-based analysis to determine which verification/validation tasks are critical for patient safety and data security. In the event of system changes, these tasks should undergo extensive automated checks and testing. Don't re-invent the wheel. Keep reusability of cloud infrastructure in mind.

3. The operational phase of cloud infrastructure or systems needs to be modified to take into account frequent changes to components ranging from hardware (IaaS) to the application itself (SaaS). Scheduling of monitoring activities should be based on update frequency and system criticality. Perform evaluation and revalidation activities, ranging from weekly evaluation of release notes to continuous validation using automated checks and tests. Use automation to shift the revalidation workload from human to computer. Use cloud-native services to monitor your virtual infrastructure for changes, intrusions or failure. Scan for, assess and close vulnerabilities regularly according to your security requirements.

4. During the retirement phase, particular consideration should be given to data archiving. Patient and quality-related data may need to remain available for inspection by regulatory authorities and therefore needs to be either archived or available in any new system. Also be aware that once you retire your solution you are pulling the plug for all users worldwide. Users will no longer be able to use the previously provided cloud services. Make sure the retirement is properly communicated and prepared.

The lifecycle considerations outlined in this whitepaper apply equally to cloud services used as part of a medical device or IVD software functions, regulated operational systems such as QMS, or regulated data hosting. In practice, cloud infrastructure used to operate a cloud-based medical device always at some level becomes infrastructure software, which is subject to the validation process for computerised systems defined in the quality management system. Key factors for establishing a validation procedure for cloud-based systems used in regulated medical devices are proper application of the shared responsibility concept, trust and contract-based supplier management, an understanding of system design, cybersecurity and data integrity-related technologies and continuous validation based on periodic evaluations and test automation.

Our proposed approach to achieving regulatory compliance

Taking into account the technical nature of cloud applications and infrastructure (explored in chapter 2), an approach to validation that relies on extensive testing and complete control over infrastructure is difficult, if not impossible. Where non-cloud systems typically undergo full validation once, with revalidation tailored to change impact and risk, cloud systems require constant monitoring and validation testing because cloud solutions are subject to frequent updates and frequent changes to the underlying infrastructure and services. Building test-automation solutions for all application layers of a cloud application would be too time-consuming and would require a high maintenance workload. Under the regulations and guidance set out above, the use of cloud systems is not prohibited, and there is no requirement to set up extensive test-automation solutions.

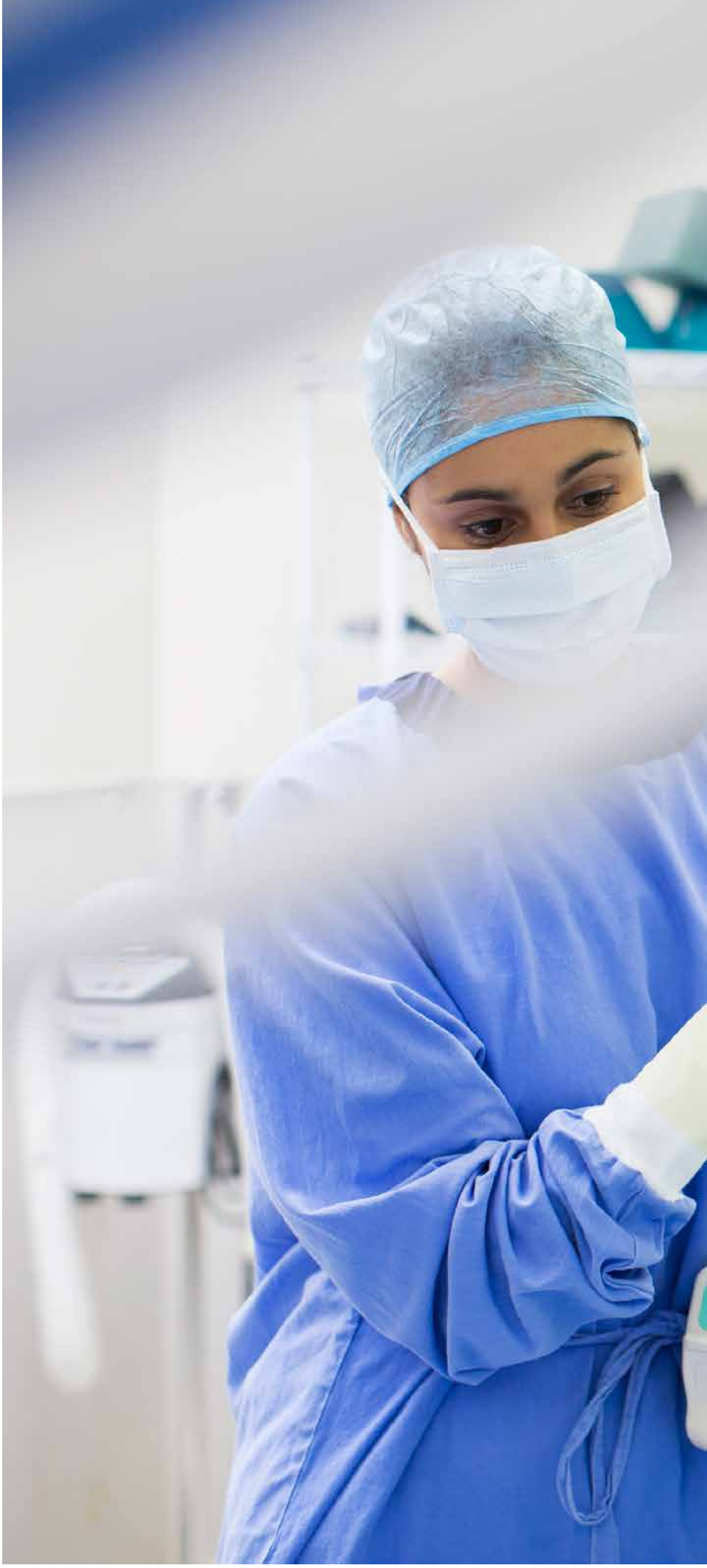
We suggest a validation approach that combines different activities, as described in computerised system validation (CSV). Our approach has the following main elements:

- Use critical thinking and risk management to identify the appropriate validation activities.
- Where feasible, continuously implement cloud test automation using the standard tools your cloud provider already offers.
- Reuse architectural patterns established by your cloud service provider.
- Continuously monitor and evaluate changes by running regular assessments based on system criticality and risk.
- Make use of cloud service provider management artefacts: request the required certificates, establish service contracts, and perform audits.

Suggested tasks for each lifecycle phase are examined in Part II of this whitepaper.

Part II

A practical guide to developing validated cloud-based solutions



3. The framework

For regulated users, there is still a considerable degree of uncertainty around the use of cloud services and products. In Part I of this whitepaper, we discussed existing regulatory guidelines and standards and explored a potential strategy for meeting regulatory requirements. Below, we discuss key questions and specific points that need to be considered during development or integration of cloud solutions. These key questions then lead to the technical blueprint described in chapter 4.1 We also discuss technical approaches to and procedures for each project phase from concept through to retirement.

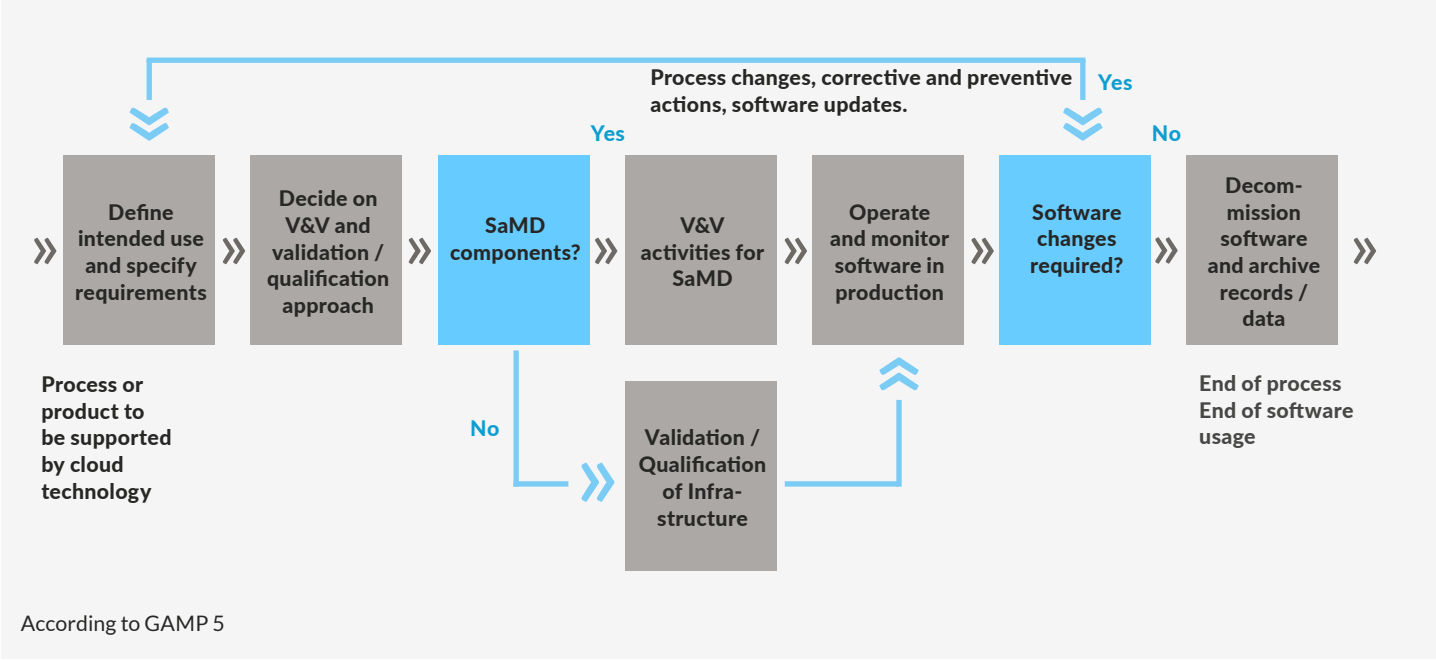


Figure 4: Verification and validation lifecycle activities for SaMD, cloud based software as part of QM and corresponding cloud infrastructure.

3.1 Concept phase

The concept phase is an important step in any project. A key outcome is defining the cornerstones of the planned solution. This phase is perhaps one of the most important when developing or introducing a cloud-based solution. It is also an opportune moment to ensure that the management team and quality assurance and regulatory departments are on board.

Evaluate and choose the right cloud service provider for your project.
Because of the additional requirements and complexity involved in using a cloud-based system, the cloud service provider for your project needs to be thoroughly evaluated and carefully chosen. Your choice of provider might be influenced by factors such as the regulatory environment, safety, security, and privacy requirements, server locations, and supplier quality management activities and certifications.

Process considerations	QMS considerations	Technical considerations
Identify requirements likely to influence selection of a cloud service provider: ■ Location ■ Availability ■ Performance ■ Auditability ■ Certifications ■ Training, change control, testing, configuration documentation, periodic controls ■ Logging and audit trails ■ Other specific to your needs	**Establish processes and guidelines:** ■ Data handling and storage (records management), which now involves external providers and third-party data storage providers. ■ Depending on the type of cloud service model, SOPs need to be updated to take into account the involvement of and responsibilities of the cloud provider. ■ Supplier management and contracts (e.g. SLAs) with cloud service providers. ■ Risk-based approaches and proven-in-use assessment to limit workload and process complexity.	■ Identify what landing zones (described in section 4.3) certified to the standards required for the project are available from the potential cloud service provider. ■ Think about data sovereignty – can the potential cloud service provider guarantee that data is physically stored in the required country or countries only. ■ Identify availability and capacity requirements and check that the cloud service provider infrastructure meets these. Example requirements include: hot failover, zero downtime, multi-regional deployments.

Understand cloud-specific additional requirements and risks

Cloud systems come with additional categories of requirements and risks that may not be familiar to a first-time user. It is important to evaluate these requirements and risks at an early stage, as they will affect both the architecture of the cloud system and the choice of cloud service provider.

Process considerations	QMS considerations	Technical considerations
■ Focus on requirements which are crucial to the quality of the product (see box). **Consider specific risks associated with cloud-based solutions as early as possible (see right box on page 31).** ■ With cloud solutions new risks can arise if functions are reliant on cloud functionality. A feature as simple as cloud-based authentication, for example, could cause a patient to suffer a delay in treatment.	**The product risk management process may need to be modified to deal with cloud-based systems:** ■ Areas to be considered should include physically external components and infrastructure and privacy laws relating to cross-border data flows. ■ The frequency with which periodic reviews and evaluations are performed should be based on how critical the external services are for your product, the availability of in-house resources and the extent to which the provider guarantees the service provided. ■ Establish cybersecurity protocols for cloud systems or extend existing protocols. ■ Incorporate an assessment of controls which are the responsibility of the cloud provider.	■ Involve the cloud service provider and/or other experts in requirements engineering and risk analysis. ■ Cloud service providers often offer whitepapers, checklists and blueprints to support this process. ■ Use a zero-trust approach to security.

Work on a first draft of your verification or validation strategy

The controls and rationales around which manufacturers build their validation processes are based on the assumption that the manufacturer has full control over installed software and the hardware on which the software runs. Switching to a cloud-based solution usually requires cloud and validation expertise provided by an experienced quality assurance specialist.

Process considerations	QMS considerations	Technical considerations
Consider test automation and define the level of automation and coverage early in the project. ■ Risks should be treated as critical requirements. It is important to identify risks that require automated validation. ■ Identify critical services and functions and focus validation activities on these items.	**Establish guidelines and processes for:** ■ Defining which parts of the cloud service are critical and should be subject to continuous monitoring and validation. ■ Qualifying and monitoring infrastructure. This should be tailored to cloud infrastructure. ■ Scheduling regular re-evaluation of the cloud system. Intervals should be from one to six months, depending on how critical the system is.	■ Identify cloud services able to support continuous validation and define the validation chain architecture.

Understand the difference between infrastructure, runtime services and SOUP

Process considerations	QMS considerations	Technical considerations
Understanding the difference between infrastructure, runtime and SOUP is key, as this determines the development and qualification processes and the workload. ■ With cloud systems, by using a smart architecture it is possible to shift the boundaries between these categories. This should be leveraged to minimise future qualification and documentation workload.	■ Establish architecture guidelines and checklists for properly identifying and documenting infrastructure, runtime and SOUP elements. ■ Define which processes and documentation need to be applied to which category.	■ Minimise the use of SOUP and base your architecture on cloud services which use the shared responsibility model.

Typical points for consideration when selecting a cloud service provider:

- provider location (data protection legislation)
- performance
- required features (e.g. data-base with audit trail)
- scalability (planned features need to be able to grow)
- cloud provider auditability
- any mitigations from the risk assessment

Typical points for consideration during risk assessment include:

- cloud system availability
- risk of data loss
- risk of data falsification
- cybersecurity risks
- risk that the cloud provider ceases operations (e.g. bankruptcy)
- risk that essential cloud functionality will be deprecated
- risk of privacy breach by cloud provider documentation

3.2 Project phase

The project phase is where specification, implementation, verification and validation of the software system takes place. The documentation model is typically a V–model. Building products or software systems containing a cloud component which are to be used in quality management systems is no different, but there are a few additional checkpoints.

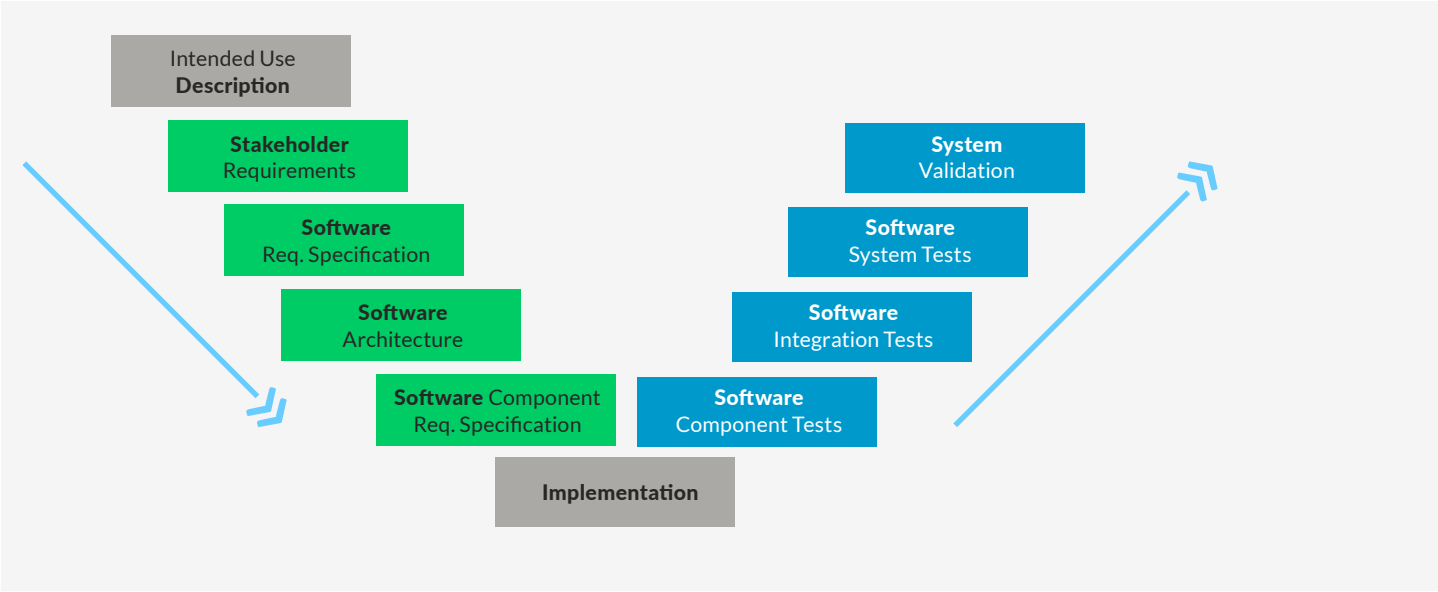


Figure 5: A general V-model for documentation of software used in a quality management system or medical device. Intended use and top-level requirements represent the baseline against which validation is performed. Technical design of the software is verified at all levels through software testing activities.

Build long lead times for time-consuming activities into the project plan

Cloud solutions may increase the workload involved in supplier management and in drawing up contracts and agreements. This is because some responsibilities are shared or outsourced to the cloud service provider.

Establishing a sound legal relationship may take time and may require a new approach, since cloud service providers rarely allow audits or access to their code base.

Process considerations	QMS considerations	Technical considerations
Identify processes, tasks and responsibilities involving the cloud service provider and ensure that these are properly regulated in the contract with the cloud provider. Typical points include: ■ supplier qualification ■ NDAs ■ data agreements ■ contracts for cloud service provider responsibilities under the shared responsibility model	■ Establish SLA and quality agreements. ■ Establish servicing, maintenance and monitoring procedures for the cloud service used. ■ Incorporate cloud service considerations into PMS activities.	■ Use the standard set of monitoring and audit tools (e.g., Amazon CloudWatch & CloudTrail, Microsoft Defender for Cloud & Azure Monitor) to maintain and monitor the SLA commitments.

Ensure that requirements and risks are reflected in your solution architecture

You need to ensure that the architecture of your cloud solution meets your identified requirements, and that patient safety and data integrity risks are mitigated by design as far as is reasonably possible. Architecture drivers must be identified and documented.

Process considerations	QMS considerations	Technical considerations
■ There should be a particular focus on cybersecurity risks, as these risks are hard to mitigate at a later stage if there are gaps in the architecture. ■ Start SOUP analysis early in the project. All SOUP carries potential risks, and these need to be assessed and where necessary mitigated.	■ Ensure that cybersecurity risks are properly covered by processes and guidelines. ■ For software as a medical device, define SOPs for managing SOUP.	■ Use the standard set of monitoring and audit tools (e.g., Amazon CloudWatch & CloudTrail, Microsoft Defender for Cloud & Azure Monitor) to maintain and monitor the SLA commitments.

Understand the potential of reusability

At this stage it is important to think about future products and solutions which may be able to reuse work implemented in this phase. Be sure to identify potentially reusable infrastructure. Automation enables easier, faster testing and delivers more reliable results.

Process considerations	QMS considerations	Technical considerations
To minimise the documentation and revalidation workload, carefully evaluate: ■ which parts of a product might be reusable in future projects. ■ whether multiple products could use the same basic functionality and infrastructure (see for example regulated landing zone in section 4.3). ■ whether you can reduce costs by using a well-defined common infrastructure which can be deployed and tested automatically.	**Define strategy, guidelines and processes for decoupling the infrastructure from the product or service:** ■ It may be possible to document and control some feature sets in dedicated files. Such modules can be reused in future products without needing to reverify their functionality.	■ Choose and implement an Infrastructure as Code solution (AWS CloudFormation, Azure Resource Manager, Chef, Puppet, Ansible, etc).

Make full use of the potential of automated testing

In the maintenance phase, automated testing can be key for rapid product verification and building trust in cloud infrastructure. To make full use of the potential of automated testing, define and validate your test infrastructure, and ensure that test case implementation and test coverage are specified as part of the development process. Any decision on automation should be based on an evaluation of risks and the automation workload (building and maintaining automation).

Process considerations	QMS considerations	Technical considerations
■ Define and introduce a continuous integration and deployment concept with a focus on an appropriate level of test automation. ■ Specify test levels and coverage and produce guidelines for establishing where test automation should be required/encouraged. ■ Define and introduce a test automation tool able to orchestrate and run all your tests and which can be triggered when cloud services notify you of updates to services and interfaces.	■ Ensure that your validation guidelines for infrastructure and tooling include tools for test automation. ■ Define triggers for and frequency of automated tests, and make sure you formulate documentation requirements. ■ To support engineers and more senior stakeholders in the event of serious constraint violations, define processes for setting thresholds for alerts.	■ Use static code analysis to automatically identify potential bugs and performance issues, and ensure adherence to best coding practices. ■ Set up static code analysis and relevant alerts (SonarQube, etc). Define a minimum code-coverage percentage for unit tests and automatically fail the build if this minimum is not reached. ■ Use automated system testing to reduce the workload for regression and other testing which was previously carried out manually by humans (GUI testing etc.). ■ To accompany automated testing, set up automated publishing of reports, either by email or to cloud storage (S3, Azure Storage, etc.).

Understand and define the release and deployment process
Be aware that cloud solutions have a higher release frequency and ensure that you set up an efficient deployment process. Ideally you should build a full continuous integration & continuous deployment (CI/CD) pipeline that deploys the software automatically when merged into the production branch of your version control system.

Process considerations	QMS considerations	Technical considerations
■ Essential security and performance patches result in a high update frequency. We therefore strongly recommend defining an automated or semi-automated release and deployment pipeline. ■ The pipeline should include automated regression and security testing, scripted infrastructures for building and configuring your solution, and for populating test data and users in a staging environment. It should automatically generate IQ and OQ protocols.	■ Ensure that processes and guidelines cover automated or semi-automated deployment and define the quality thresholds that need to be overcome prior to release. In the event of patches or fixes, remember that cloud-solutions may necessitate very quick reaction times.	■ Choose and implement an appropriate CI/CD solution (AWS CodeBuild & CodePipeline, Azure DevOps, Jenkins, Octopus, etc.). ■ Set up automated deployment to integration environments on merging from the integration branch in your version control system and deployment to production on merging to the production branch.

3.3 Live/Maintenance phase

The primary focus in the live or maintenance phase is on ensuring that an existing solution remains safe, validated and fast. In planning this phase, it is important to understand the dynamics of updates to cloud services and to define a schema for handling frequent changes to the cloud infrastructure.

Define a schema for monitoring changes to cloud services and specify how they trigger testing
With cloud services, minor updates in particular are often unannounced and do not follow a fixed release schedule. It is therefore crucial to define a schema for monitoring your cloud services and ensuring that changes do not go undetected. When changes to cloud services are detected or announced, there needs to be a mechanism for ensuring that the verification and validation activities specified in the strategy are completed. Where automated tests are specified, they must run against the service and results should be documented automatically.

Make sure that maintenance and monitoring are covered and that SLAs are in place where these activities are outsourced.

Process considerations	QMS considerations	Technical considerations
■ Make sure you have a mechanism in place for detecting unannounced updates using provider tools for detecting, tracing and logging updates to the services used. ■ Specify whether and under what circumstances changes to these services should trigger (automated) testing against the services. ■ Create a test bed which either tests services and interfaces regularly or trig-gers on-demand tests.	**With cloud systems, the operational phase involves performing the monitoring activities defined in the concept phase. This consists of regular analysis of the system and service provider and where necessary revalidation. You should there-fore ensure that:** ■ monitoring activities are covered in your processes, SOPs and validation plan. ■ required revalidation and documentation is defined for all update types (see box).	■ Use tools provided by the cloud service provider to monitor the cloud environment and send alerts in the event of any changes to setup or configuration. (e.g., Amazon CloudWatch & CloudTrail, Microsoft Defender for Cloud & Azure Monitor). ■ Use the change logs (listing all changes) maintained by the service to facilitate auditing.

Understand the consequences of failed tests or disruptive changes.
Define communication flows and immediate corrective actions in the event that automated tests against a service are failed or a disruptive change is announced. It may be necessary to temporarily shut down part of a cloud application in the event of an unplanned issue such as a 0-day exploit or a serious bug with a negative impact on patients.

Process considerations	QMS considerations	Technical considerations
In the event that automated or manual tests are failed, the cloud system may no longer be validated. Ensure that: ■ you have a procedure in place defining how to react in such a situation and that this procedure is understood by the maintenance team. ■ there is a dedicated team ready for action within a time frame appropriate to the criticality of the impacted features.	■ Ensure that proper procedures for evaluating failed tests are in place and that immediate actions and communications are defined.	■ Microservices architectures can be designed so that they are resilient in the event of the loss of one or more constituent service. This offers a means of temporarily mitigating an event in which one or more services becomes non-compliant. ■ Ensure the software architecture supports partial shutdowns.

Actions to be taken during live phase

- Perform planned assessments and evaluate feature changes and new bugs in your cloud services.
- Perform cloud supplier controls as planned in your strategy.
- Perform revalidations as defined in your strategy.

Possible types of updates:

- Extension update: Usually non-critical since it introduces a new feature which is not yet used by any applications. It is the cloud service provider's responsibility to ensure that the extension does not modify the behaviour of existing features, though some refactoring of shared code or the architecture may occur.
- Enhancement updates and bug fixes: These updates are the focus of this guideline, since they can impact system performance and behaviour.
- Deprecation update: These updates will definitely affect system functionality and/or performance, but are always announced well in advance. Receipt of a deprecation notice needs to trigger a change process which must include an impact assessment.
- Security updates: Security updates fix critical vulnerabilities and, particularly where a vulnerability is already being exploited, require a very rapid response. They may result in the temporary suspension of specific cloud functionality. In such cases a very efficient CI/CD process is crucial for either fixing the vulnerability or bringing the functionality back online.

3.4 Retirement phase

The retirement phase marks the end of life of a cloud solution or product. While retiring software is less complicated than retiring physical devices, there are still a number of points to consider.

Persistent data storage in accordance with regulations

Depending on the solution and configuration, it may be possible to delete stored data, logs, audit trails and protocols from cloud storage when a cloud solution is retired. Where applicable regulations mandate persistent storage of data, this data may need to be copied to new storage.

Process considerations	QMS considerations	Technical considerations
■ Identify a location for long-term storage of any data that needs to be retained for regulatory reasons.	■ Data which may need to be inspected by regulators must be accessible for the specified time period. A decision will need to be taken on whether the system can be trusted and used in read-only mode, or whether the data needs to be migrated to an alternative system.	■ For added security, archived data should be encrypted (AWS Glacier or Azure Storage may be good options).

Produce a plan detailing how you will retire all instances and configurations

While retiring a cloud solution is made easier by the fact that the software is executed centrally, the use of multiple tenants and multiple server locations means that proper retirement planning is still essential. Be aware that your clients' systems may be dependent on your solution. Have these systems been updated so that they are no longer dependent on the system scheduled for retirement?

Process considerations	QMS considerations	Technical considerations
■ Ensure that you are aware of all dependencies on your cloud system. ■ Users need to be made aware of the planned retirement well in advance to give them a chance to adapt their systems for when your system is no longer available. ■ Crucial third party functionality may be dependent on the system scheduled for retirement.	■ Ensure IT/QA managers at the company and at the cloud service provider are involved in retirement planning for cloud systems. ■ Migration of data to a new system, e.g. for archiving, needs to be validated and documented. ■ If new systems are introduced for archiving, they must be validated and qualified. ■ Retirement of a system must be documented in the software inventory list.	■ If your application uses a shared Identity Access Management (IAM) solution, ensure user data specific to the retired application is removed from the IAM.

4. Appendix

4.1 Technical framework

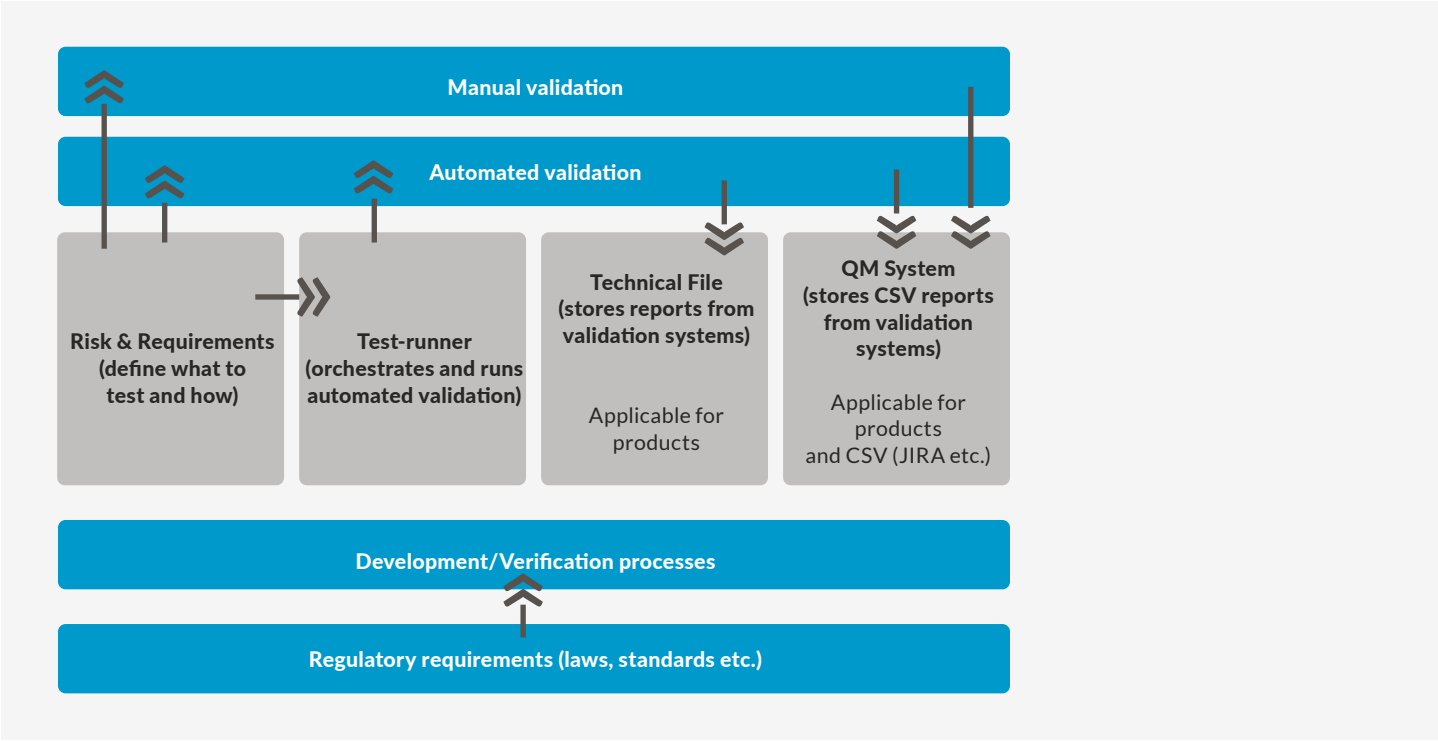


Figure 6:
1. Evolving regulatory requirements are considered and incorporated into verification processes.
2. Teams identify requirements of the cloud-application and evaluate which of them represent risk and therefore need continuous verification and validation (this is the most important phase).
3. A 'test plan' is created based on these requirements.
4. This test plan is then actioned by an automated test runner.
5. These tests are performed against the product that lives in the cloud (and can be triggered automatically based on a series of variables).
6. The test runner then reports the results to a technical file and/or logs them in the QM system for auditing.

As discussed above, automated validation is a powerful tool for ensuring that your product or service is still workin gas required, requirements are still met and risks are still mitigated. In this framework, the authors provide evidence to show that where automated validation is useful or necessary, best practices and advanced components to make the job easier are already available. Don't attempt to build everything from scratch. Take a close look at the toolset provided by your cloud provider.

We will focus on the options provided by the two big players in the market, but most providers offer similar functionality.

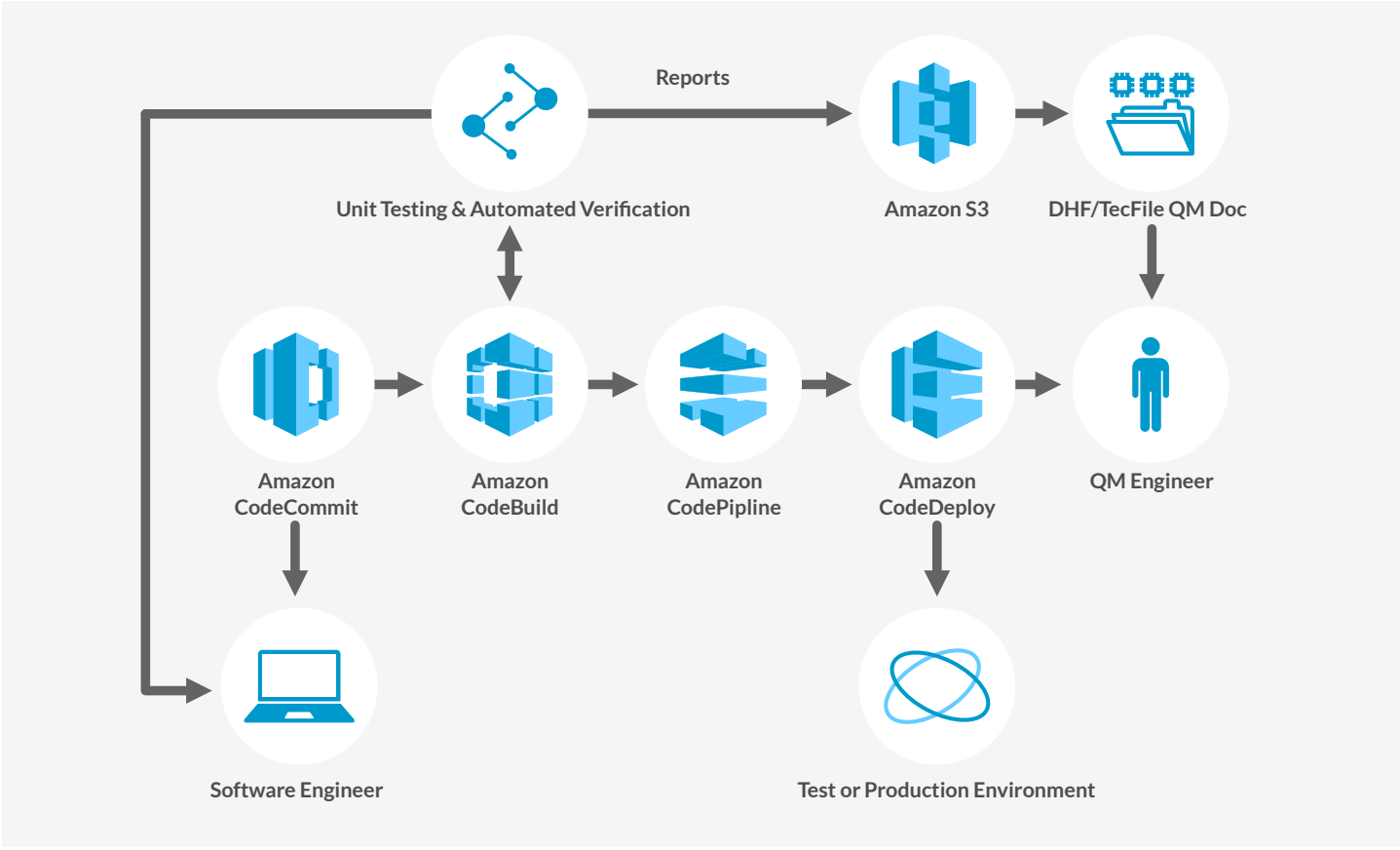


Figure 7: AWS CI/CD Example: On AWS you can set up CI/CD using cloud-native services such as Amazon CodeCommit (or Git or another version control system), CodeBuild, CodePipeline (CI) and CodeDeploy (CD).

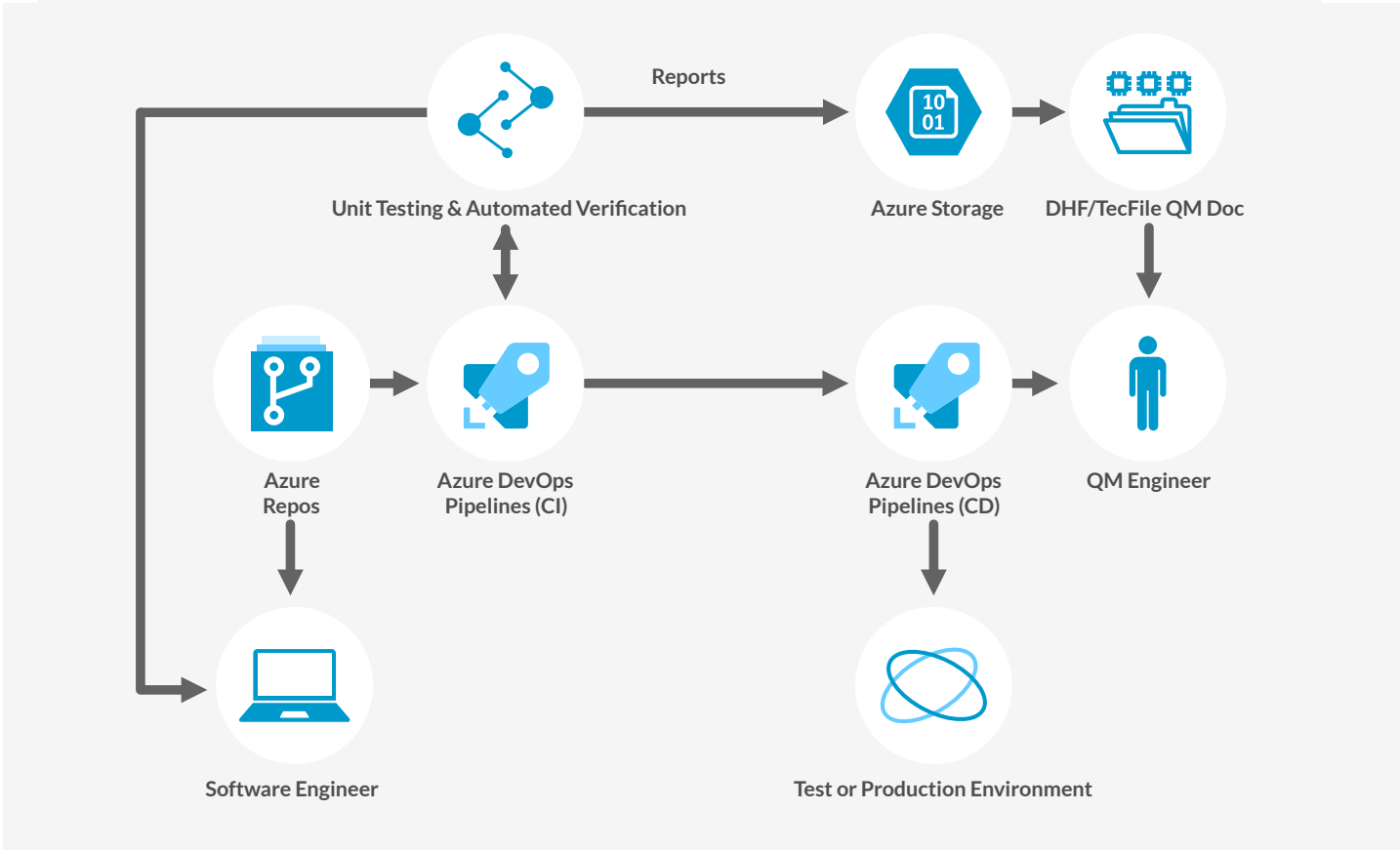


Figure 8: Azure CI/CD Example: Setup on Azure is somewhat simpler, as Azure DevOps Pipelines deals with both CI and CD.

Minimum blueprint for compliant cloud production deployment

There is no one-size-fits-all solution, but below we offer basic blueprints for AWS and Azure, detailing a minimum set of cloud-native services for each service provider to ensure a level of security, logging, monitoring and audit trail availability sufficient to meet basic compliance requirements.

On AWS, services that help to achieve compliance are:

- Amazon Inspector – automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.
- Amazon CloudTrail – monitors and records account activity across your AWS infrastructure, giving you insight into used resources, analysis, and remediation actions.
- Amazon CloudWatch – collects monitoring and operational data in the form of logs, metrics, and events.
- Amazon Flow Logs – is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you create a flow log, you can retrieve and view its data in the chosen destination.
- Amazon Identity and Access Management – (IAM) provides fine-grained access control across all of AWS. With IAM, you can specify who can access which services and resources, and under which conditions. With IAM policies, you manage permissions to your workforce and systems to ensure least-privilege permissions.

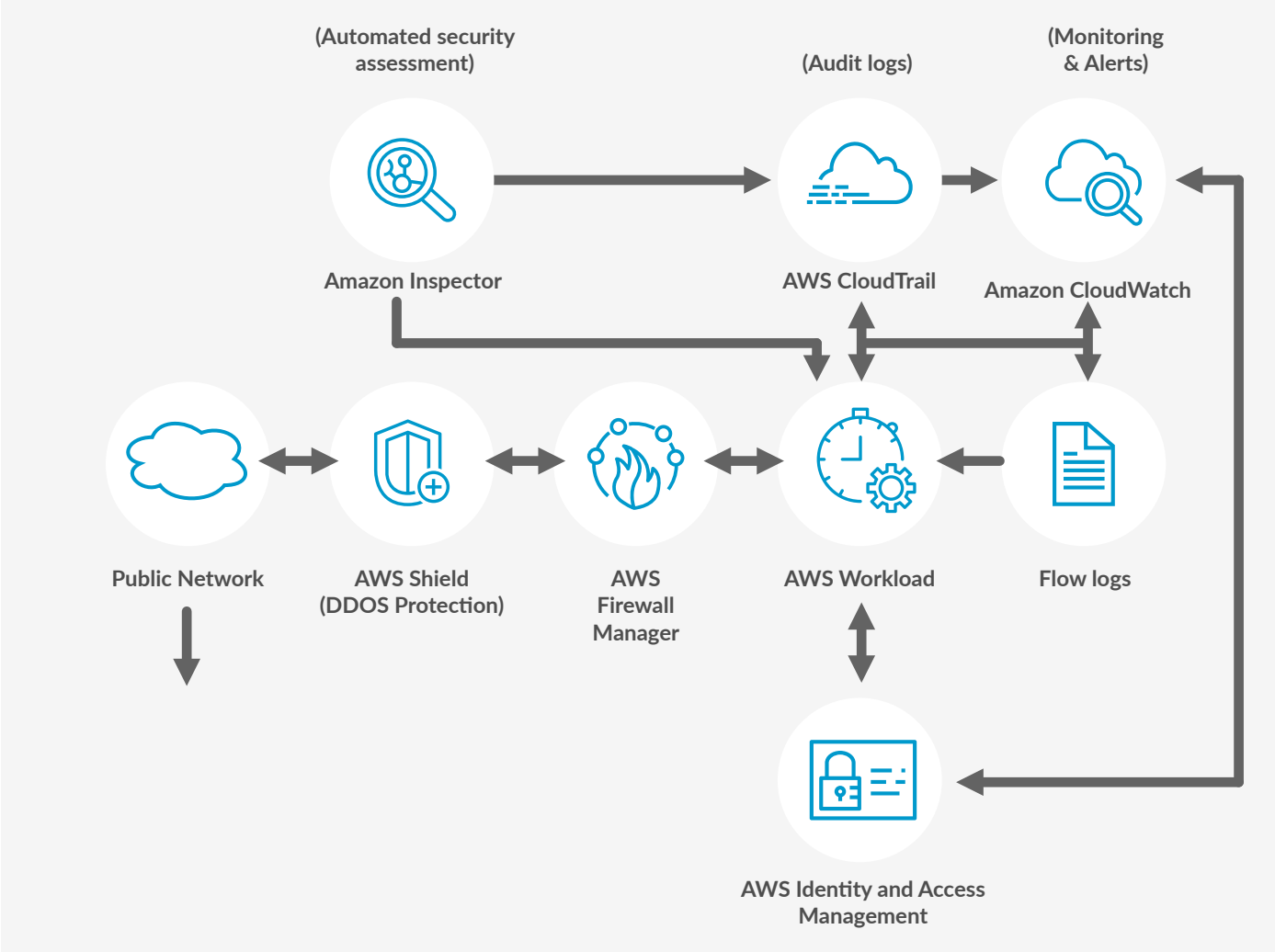


Figure 9: Sample AWS blueprint

On Azure, services that help to achieve compliance are:

- Microsoft Defender for Cloud – is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources. Microsoft Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms.

- Azure Activity – is a platform log in Azure that provides insight into subscription-level events. Activity log includes such information as when a resource is modified or when a virtual machine is started.

- Azure Monitor – helps you maximize the availability and performance of your applications and services. It delivers a comprehensive solution for collecting, analysing, and acting on telemetry from your cloud and on-premises environments.

- Microsoft Entra ID: the enterprise identity service that provides single sign-on, multifactor authentication, and conditional access.

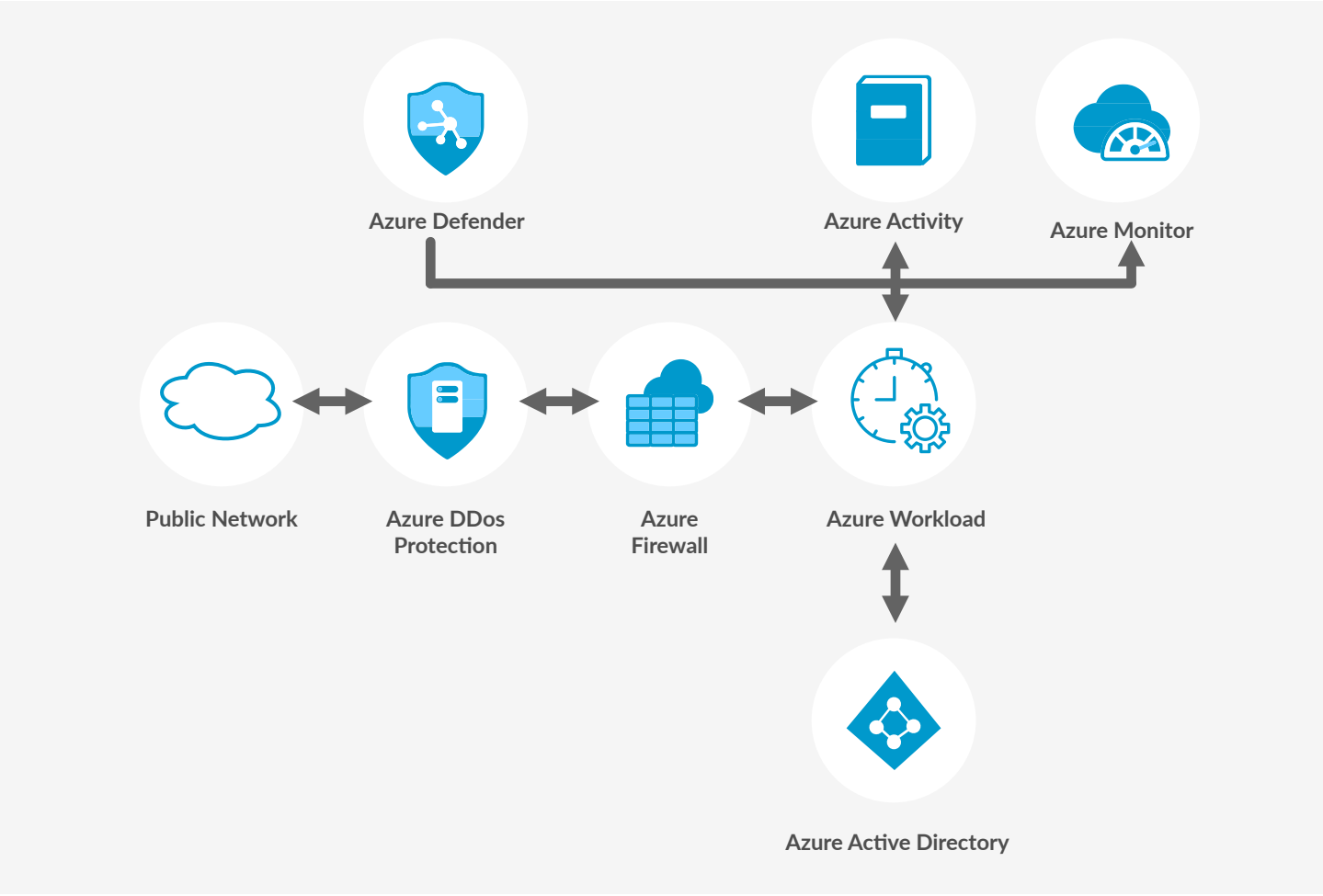


Figure 10: Sample Azure blueprint

4.2 Non-binding software validation and data integrity standards and guidance documents

- **EN ISO 13485:2016+A11:2021 Medical devices - Quality management systems - Requirements for regulatory purposes** specifies QMS requirements for organisations providing medical devices and related services that must consistently meet customer and regulatory requirements. For cloud applications, it is relevant to outsourced-process control, supplier qualification, software validation, documentation control, complaint handling, CAPA, PMS records and design-development controls where cloud services support product conformity or regulated QMS processes.

- **ISO 14971:2019 Medical devices - Application of risk management to medical devices** specifies terminology, principles and a lifecycle process for medical device risk management, including software as a medical device and IVD medical devices. For cloud applications, it supports identification and control of hazards related to availability, latency, cybersecurity, data integrity, third-party dependencies, incorrect outputs, service degradation, updates, and decommissioning.

- **IEC 62304:2006+AMD1:2015 Medical device software - Software life cycle processes** defines software lifecycle processes, activities and tasks for medical device software development and maintenance. For cloud applications, it is relevant where cloud-hosted or cloud-connected software is itself a medical device or part of one, supporting software planning, requirements, architecture, implementation, verification, maintenance, problem resolution and change control.

- **IEC 82304-1:2016 Health software - Part 1: General requirements for product safety** addresses safety and security of health software products intended to run on general computing platforms without dedicated hardware. For cloud applications, it is relevant to standalone health software, SaaS health products and web-based services because it links product requirements, intended use, validation, instructions for use, maintenance and post-market activities.

- **IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle defines security** lifecycle activities for health software and health IT systems. For cloud applications, it is relevant to secure development, maintenance, vulnerability handling, security risk control, supplier interaction, update management and protection of connected health software across the product lifecycle.

- **MDCG 2019-11 Rev.1 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 - MDR and Regulation (EU) 2017/746 - IVDR** explains when software qualifies as medical device software or IVD software and how classification rules apply. For cloud applications, it is relevant when cloud-hosted functions perform diagnosis, prediction, monitoring, decision support or other medical purposes.

- **MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices** provides EU guidance on MDR/IVDR cybersecurity requirements across pre-market and post-market phases. For cloud applications, it is relevant to security-by-design, secure configuration, access control, vulnerability management, update processes, IT environment assumptions, operator responsibilities and post-market cybersecurity monitoring for connected medical devices and cloud-hosted device software.

- **FDA Off-The-Shelf Software Use in Medical Devices Guidance for Industry and Food and Drug Administration Staff, August 2023** describes recommended premarket documentation for OTS software used in medical devices. For cloud applications, it is relevant where cloud services, third-party components, managed services or commercial software elements are incorporated into device software and require documented risk assessment, hazard mitigation and evidence supporting safe and effective performance.

- **FDA Content of Premarket Submissions for Device Software Functions Guidance for Industry and Food and Drug Administration Staff, June 2023** describes software information generally needed for FDA premarket review of device software functions. For cloud applications, it is relevant to requirements, architecture, risk management, software documentation level, verification, validation, unresolved anomalies, cybersecurity relationships and cloud-hosted software functions submitted as part of a medical device.

- **FDA Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions Guidance for Industry and Food and Drug Administration Staff** provides FDA recommendations for cybersecurity design, development, maintenance and premarket submission content for cyber devices. For cloud applications, it is relevant to threat modelling, SBOM, vulnerability management, security architecture, patching, monitoring, coordinated disclosure and assurance that connected device functions remain cybersecure.

- **AAMI TIR36:2007 Validation of software for regulated processes** provides guidance for validating software used to automate medical device regulated processes and quality-system activities. For cloud applications, it is relevant to SaaS or cloud-hosted tools used for design, production, testing, complaint handling, distribution, electronic records or signatures, supporting a risk-based approach to validation effort, supplier controls and intended-use evidence.

- **ISO/TR 80002-2:2017 Medical device software - Part 2: Validation of software for medical device quality systems** provides a risk-based approach to validating software used in medical device QMS processes. For cloud applications, it is relevant to QMS SaaS, hosted production tools, document management, training, CAPA, complaint, supplier and monitoring systems because validation activities can be scaled based on intended use, risk and supplier evidence.

- **FDA Computer Software Assurance for Production and Quality Management System Software Guidance for Industry and Food and Drug Administration Staff** provides recommendations for risk-based assurance of computers and automated data processing systems used in medical device production or QMS activities. For cloud applications, it is relevant to focusing testing and evidence on high-risk features while using supplier activities, automation and critical thinking to maintain confidence.

- **EudraLex Volume 4 Annex 11: Computerised Systems** provides EU GMP requirements for computerised systems used in GMP-regulated activities, including validation, qualified infrastructure, supplier assessment, data integrity, access control, audit trails, backup, business continuity and change control. For cloud applications, it is directly relevant where hosted applications or infrastructure create, process, store, retrieve or transmit GMP records or control GMP processes.

- **EudraLex Volume 4 Annex 15: Qualification and Validation** describes EU GMP principles for qualification and validation applicable to facilities, equipment, utilities, processes and related changes. For cloud applications, it is relevant where cloud systems support medicinal product manufacture because validation planning, acceptance criteria, change impact assessment, revalidation, lifecycle documentation and continued process control must remain justified and documented.

- **ISPE GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, Second Edition** provides a lifecycle and risk-based framework for achieving fit-for-intended-use GxP computerised systems. For cloud applications, it is relevant because it addresses service providers, agile methods, automation, critical thinking, supplier leveraging, scalable documentation and maintenance of validated state in modern outsourced and frequently changing technology environments.

- **ISPE GAMP Good Practice Guide: IT Infrastructure Control and Compliance, Second Edition** provides guidance for compliant IT infrastructure platforms, including traditional and cloud-based infrastructure. For cloud applications, it is relevant to infrastructure qualification, shared responsibility, IaaS/PaaS/SaaS control allocation, outsourcing, virtualisation, third-party data centres, configuration management, operational controls and evidence needed to support GxP applications running on cloud platforms.

- **PIC/S PI 011-3 Good Practices for Computerised Systems in Regulated "GXP" Environments** provides inspector-oriented guidance on computerised systems used in regulated pharmaceutical GxP environments. For cloud applications, it is relevant to validation, system ownership, supplier responsibilities, documentation, security, data handling, change control, backup, disaster recovery and operational control of outsourced or hosted systems supporting regulated pharmaceutical activities.

- **PIC/S PI 041-1 Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments** provides guidance on data governance and data integrity for GMP/GDP-regulated environments. For cloud applications, it is relevant to ensuring that records remain attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring and available, including hosted data, audit trails, administrator actions, backup, retention, review and supplier-managed storage.

- **ICH Q9(R1) Quality Risk Management** provides principles and examples of tools for pharmaceutical quality risk management across development, manufacturing, distribution, inspection and lifecycle activities. For cloud applications, it is relevant because validation depth, supplier oversight, data integrity controls, cybersecurity measures, change assessment and periodic review can be justified according to risk to patient safety, product quality and data reliability.

- **ICH Q10 Pharmaceutical Quality System** describes a model for an effective pharmaceutical quality system across the product lifecycle. For cloud applications, it is relevant where hosted systems support pharmaceutical development, manufacturing, quality monitoring or continual improvement because management responsibility, outsourced activity control, CAPA, change management, knowledge management and lifecycle process performance must remain integrated in the pharmaceutical quality system.

- **EMA Guideline on computerised systems and electronic data in clinical trials** defines expectations for computerised systems, including software and "as-a-service" systems, used to create or control electronic clinical trial data and processes affecting participant protection or trial-data reliability. For cloud applications, it is relevant to EDC, eSource, eCOA, ePRO, eConsent, IRT, audit trails, validation, user management, security and archiving.

- **FDA Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers Guidance for Industry, October 2024** explains FDA expectations for electronic systems, records and signatures in clinical investigations. For cloud applications, it is relevant to sponsor, investigator, IRB and CRO systems that create, modify, maintain, archive, retrieve or transmit regulated trial records, including access control, audit trails, validation and record reliability.

- **ISPE GAMP Good Practice Guide: Validation and Compliance of Computerized GCP Systems and Data - Good eClinical Practice, Second Edition** provides a risk-based framework for validating computerised systems and data used in GCP environments. For cloud applications, it is relevant to clinical-trial SaaS, decentralised-trial tools, investigator site systems, sponsor oversight, supplier assessment, data integrity, participant protection and credibility of clinical data.

- **ICH E6(R3) Guideline for Good Clinical Practice** establishes an international standard for designing, conducting, recording and reporting clinical trials involving human participants. For cloud applications, it is relevant because trial systems must support participant rights, safety and well-being, data integrity, traceability, proportionate quality management, sponsor oversight, investigator responsibilities, record retention and reliable use of technology in modern clinical trials.

- **ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements** specifies requirements for establishing, implementing, maintaining and continually improving an information security management system. For cloud applications, it is relevant to security governance, risk assessment, control selection, access management, incident response, supplier security, monitoring and continual improvement of cloud environments processing regulated or sensitive data.

- **ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services** provides implementation guidance and additional controls for cloud service providers and cloud service customers. For cloud applications, it is directly relevant to shared responsibility, virtualisation, administrator access, tenant isolation, monitoring, asset ownership, configuration and cloud-specific security control allocation.

- **ISO/IEC 27018:2025 Information security, cybersecurity and privacy protection - Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors** provides privacy control guidance for public cloud providers processing PII. For cloud applications, it is relevant where cloud providers process personal or health data on behalf of customers, supporting confidentiality, transparency, subcontractor control, data deletion, disclosure limits and privacy governance.

- **ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection - Privacy information management systems - Requirements and guidance** specifies requirements and guidance for privacy information management for PII controllers and processors. For cloud applications, it is relevant to privacy governance, accountability, processor and sub-processor controls, data subject rights support, privacy risk management, documentation and integration of privacy controls with information security management.

- **NIST Cybersecurity Framework 2.0** provides high-level cybersecurity outcomes and guidance for organisations to understand, assess, prioritise and communicate cybersecurity risk management. For cloud applications, it is relevant as a flexible framework for governance, identification, protection, detection, response and recovery activities, helping align cloud security programmes, supplier oversight, incident management and continuous monitoring with organisational risk objectives.

- **NIST SP 800-66 Rev. 2 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide** provides practical guidance for regulated entities safeguarding electronic protected health information. For cloud applications, it is relevant to HIPAA-covered cloud workloads, supporting risk analysis, safeguards, access control, audit controls, transmission security, contingency planning and mapping cloud controls to Security Rule expectations.

- **HHS Guidance on HIPAA & Cloud Computing** explains HIPAA obligations for covered entities, business associates and cloud service providers handling electronic protected health information. For cloud applications, it is relevant because a cloud service provider can be a business associate when creating, receiving, maintaining or transmitting ePHI, requiring business associate agreements, safeguards, breach handling and compliant cloud service management.

- **ISO/IEC 42001:2023 Information technology - Artificial intelligence - Management system** specifies requirements for establishing, implementing, maintaining and continually improving an AI management system. For cloud applications, it is relevant where AI services, models or LLM-supported workflows are developed or operated in cloud environments, supporting governance, risk management, accountability, monitoring, transparency, supplier control and responsible AI lifecycle management.

- **AAMI TIR34971:2023 Application of ISO 14971 to machine learning in artificial intelligence - Guide** provides guidance for applying ISO 14971 risk management to ML or AI in medical devices. For cloud applications, it is relevant where AI models are trained, deployed, monitored or updated in cloud environments, supporting hazard analysis, data-related risks, performance drift, model updates, monitoring and risk-control verification.

- **European Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act) and Guidelines on prohibited artificial intelligence practices defined by the AI Act** clarify AI-system scope and unacceptable-risk practices. For cloud applications, they are relevant where hosted AI or LLM functions may fall within the AI Act, requiring early classification, prohibited-use screening and governance before deployment.

- **FDA Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions Guidance for Industry and Food and Drug Administration Staff, August 2025** provides recommendations for PCCPs in marketing submissions for AI-enabled device software. For cloud applications, it is relevant where cloud-deployed AI models require planned, controlled post-market updates without undermining safety, effectiveness or regulatory transparency.

4.3 Glossary Literature and resources

0-day exploits	These are exploits for computer software vulnerabilities which are either unknown to those who should be interested in their mitigation (including the vendor of the target software) or known and without a patch to correct them.
Cloud solution	A cloud-based application that is fully deployed in the cloud and all parts of which run in the cloud. Applications in the cloud have either been created in the cloud or migrated from an existing infrastructure to take advantage of the benefits of cloud computing. Cloud-based applications can be built on low-level infrastructure pieces or can use higher level services that provide abstraction from the management, architecting, and scaling requirements of core infrastructure.
DHF	The design history file (DHF) is a collection of documents encompassing plans, requirements, design review records and results of design verification. The DHF is referenced in 21 CFR Part 820.30 and is now referenced in the latest version of ISO 13485, section 7.3.10. ISO 13485 requires the establishment of design and development files. The DHF specifically relates to design controls and represents the final step of compiling documents from the design and development process.

GxP	Good “x” practice. Framework of guidelines including good manufacturing practice, good clinical practice, good distribution practice, etc
Hybrid solutions	A hybrid deployment is a way to connect infrastructure and applications between cloud-based resources and existing resources that are not deployed in the cloud. The most common meth-od of hybrid deployment is between the cloud and existing on-premises infrastructure to ex-tend and grow an organisation’s infrastructure into the cloud while connecting cloud resources to the internal system.
IaaS	Infrastructure as a Service (IaaS) contains the basic building blocks for cloud IT and typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space. IaaS provides you with the highest level of flexibility and management control over your IT resources and is most like existing IT resources that many IT departments and developers are familiar with today.
ISPE	The International Society for Pharmaceutical Engineering serves its members by leading scientific, technical, and regulatory advancement throughout the pharmaceutical lifecycle.
Medical device	Any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: Diagnosis, prevention or treatment of diseases.
Medicinal product	A substance or combination of substances that is intended to treat, prevent or diagnose a disease, or to restore, correct or modify physiological functions by exerting a pharmacological, immunological or metabolic action.
On-premise	The deployment of resources on-premise, using virtualization and resource management tools, is sometimes sought for its ability to provide dedicated resources. In most cases this deployment model is the same as legacy IT infrastructure with the added use of application management and virtualization technologies to try and increase resource utilization.
PaaS	Platform as a Service (PaaS) removes the need for organisations to manage the underlying infrastructure (usually hardware and operating systems) and allows you to focus on the deployment and management of your applications. This helps you to be more efficient, as you don’t need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

SaaS	Software as a Service (SaaS) provides you with a complete product run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering, the client does not need to know how the service is maintained or how the infrastructure is managed. A common example of a SaaS application is webmail which can be used to send and receive email without having to manage feature additions to the email product or to maintain the servers and operating systems on which the email program runs.
SaMD	Software as medical device – a medical device consisting purely of a software solution and which does not include any hardware (other than accessories).
SLA	A Service Level Agreement (SLA) is a documented contract between a service provider and a customer that defines the expected level of service, including performance metrics, responsibilities, and remedies for failures. It ensures alignment on quality, such as uptime, response times, and penalties for non-compliance, typically fostering accountability and building trust.
SOUP	Software of unknown provenance. A software item that is already developed and generally available and that has not been developed for the purpose of being incorporated into the Medical Device (also known as 'off-the-shelf software') or a software item previously developed but for which adequate records of the development processes are not available. (IEC 62304 3.29)
OTS	Off-the-shelf software: a generally available software component used by a medical device manufacturer for which the manufacturer cannot claim complete software-lifecycle control.
Zero Trust	The zero trust security model describes an approach to the design and implementation of IT systems. The main concept behind the zero-trust security model is 'never trust, always verify', which means that devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified.

Literature and resources

[1] REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017
[2] 21 CFR Part 11: Electronic Records, Electronic Signatures, FDA, 1997
[3] GAMP 5: A Risk-based Approach to GxP Compliant Computerised Systems, ISPE, Second Edition, 2022
[4] GAMP Good Practice Guide: IT Infrastructure Control and Compliance 2nd Edition, 2017
[5] "Medical device software - Software life cycle processes", International Standard IEC 62304:2006 + A1 2015.
[6] "Health Software – Part 1: General requirements for product safety", IEC 82304-1:2016.
[7] General Principles of Software Validation; Final Guidance for Industry and FDA Staff, January 11, 2002
[8] Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, CRDH, January 14, 2015
[9] CDRH Proposed Guidances for Fiscal Year 2022 (FY2022) | FDA
[10] Are Hosted Systems Open Or Closed Under 21 CFR Part 11? (perficient.com)

Published by
Zühlke Engineering AG,
Zürcherstrasse 39J,
8952 Schlieren (Zürich), Switzerland

Contact:
info@zuehlke.com.
www.zuehlke.com

CEO:
Stefan Sarbach.

Pictures:
Getty Images Deutschland GmbH
and AI generated

Version 2, June 2026