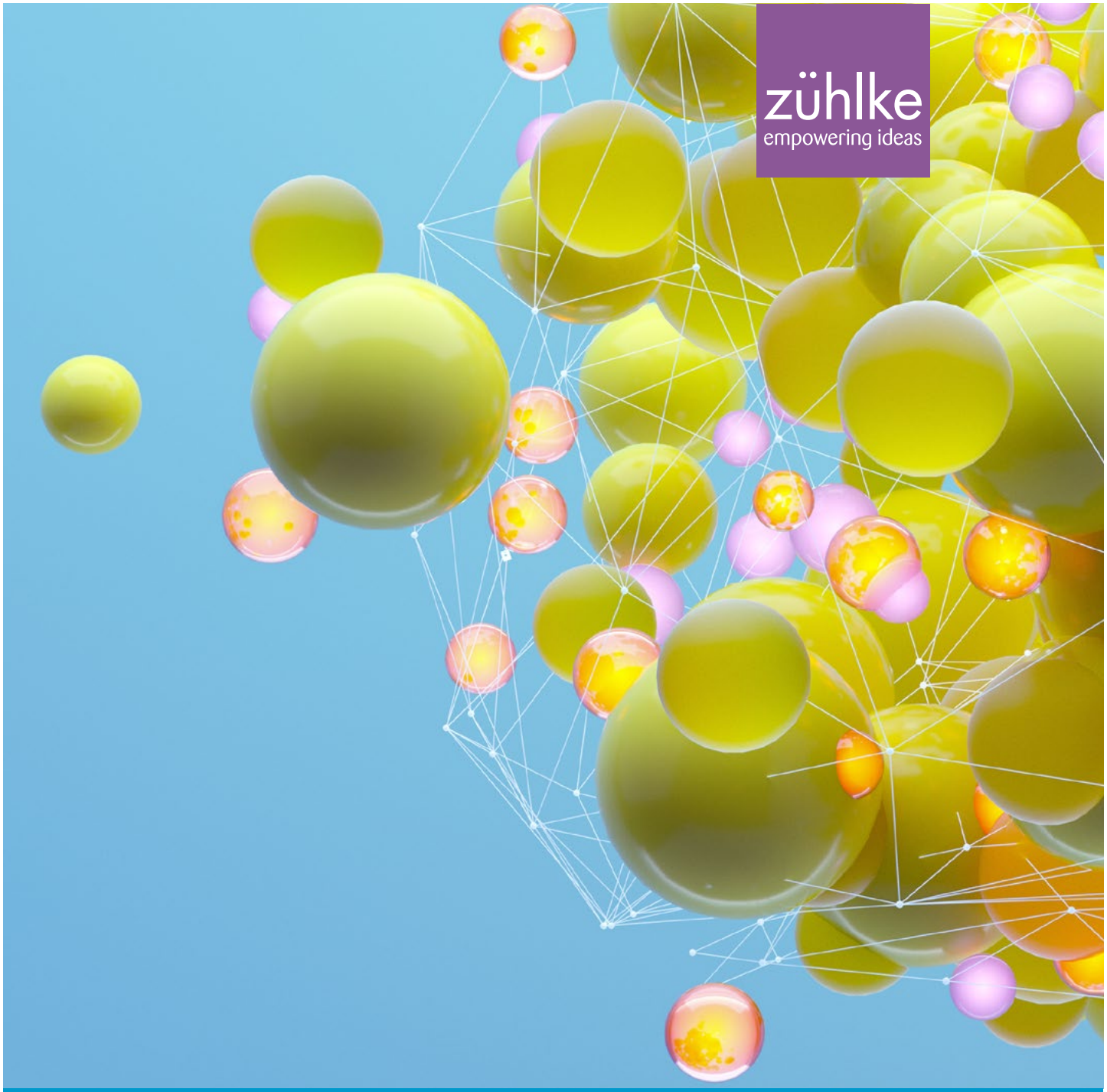


Whitepaper

Medical Clouds: A Case for Continuous Validation in Medtech & Pharma

Urs Müller (Johner Institut), Patrick Steiner (RetinAI), Peter Bäck (Zühlke), Christian Berger (Zühlke)

In collaboration with Johner Institut

Table of contents

Preface

In recent years – and during the COVID-19 pandemic in particular – 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 aging society to ballooning health care 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.**

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 harder and harder.**

However, moving to the cloud can also have significant implications, especially for companies producing safety critical products in industries with very strict safety regulations, such as medtech and pharma. Digitalisation has made huge inroads in many other business areas, but medical device and drug manufacturers have been hampered by the fact that the current regulatory environment makes it unclear to what extent the use of cloud systems or cloud components in medical devices is permissible.

In this white paper, we demonstrate that **it is absolutely possible for companies in the healthcare sector to develop and use cloud solutions safely.**

We do, however, have a number of 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 and verification and validation activities.
- Companies need 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 and risk management into their processes and structures.

In Part I of this white paper, we suggest a solution for effectively leveraging the advantages 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 represents a guide to analysing and evaluating technical factors and validation and data integrity-related factors throughout the lifecycle of a cloud software solution (Cf. the life cycle models defined in guides such as GAMP 5).

The learnings from Part I & II are consolidated into a technical blueprint in chapter 4.1. This blueprint demonstrates, how Part I & II can be integrated into the real world using the examples of two different cloud providers.

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

Part I

Regulatory background

Manufacturers of medical or pharmaceutical products are required to validate applications used in their processes and must verify and validate their products. If manufacturers operate products or product components in the cloud, they become operators. In this case, they are generally required to ensure that the underlying infrastructure has been qualified.

This looks, at first glance, incompatible with existing company practices, as well as with regulatory requirements which imply that, since each update has to be qualified and validated, qualified infrastructure, validated tools and products must be under the manufacturer's control. As a result, many manufacturers of medicinal products or medical devices are cautious when it comes to using cloud infrastructure and tend to favour on-premise solutions which place control and planning of system updates and control over the computer system firmly in the hands of the operator.

In this whitepaper, we start with a tour of existing regulations, standards and guidance documents, and evaluate their relevance and applicability for cloud infrastructure and software. We then take a look at some of the technical aspects of cloud services and software. The first section of the whitepaper concludes with our recommended approach to validating cloud software.

1.1 Overview

Software support for quality management processes at medical device manufacturers has traditionally focused on labour-intensive and medicinal product validation tasks. Manufacturers are required to prove that software functions correctly within the scope of the intended use and to ensure that system hardware is setup and functions correctly. Drawing on guidance documents, manufacturers build validation and qualification processes around controls and rationales, under the assumption that they have complete control over the hardware and the software installed on it. The use of computerized systems which are outside the manufacturer's control, such as cloud infrastructure and software, was considered to pose an increased risk and was expected to result in a dramatic increase in the validation workload. It was therefore generally avoided.

The use of cloud applications and infrastructure requires a paradigm shift. There remains considerable uncertainty around cloud usage, and regulators and manufacturers are looking for clear guidance. Auditors have in some cases prohibited the use of cloud software, arguing that its use is incompatible with current regulations. But guidance on managing cloud applications and infrastructure in a regulated environment is available, as are a number of case studies. Additionally, many medical devices include lower-risk cloud components, such as server backends operating on cloud infrastructure. By using such components, manufacturers take on the role of medical device manufacturers, which means **they are obliged to treat cloud infrastructure in the same way as IT infrastructure used as part of their quality management processes.**

Manufacturers need to look carefully at how existing regulations, guidance documents and non-binding standards for managing software and IT infrastructure apply to cloud solutions. In particular:

- What requirements does the European Union's recently adopted Medical Device Regulation (MDR) impose on cloud usage by medical device manufacturers and what provision does it make for such use?

- What are the implications of FDA regulations and recently launched FDA programs and initiatives on the adoption of new technology for cloud usage in the medical device sector?

For medical device manufacturers, it is helpful to look at European and US guidance documents, and at the experiences of the pharmaceutical industry. The pharmaceutical industry is closely allied with the medical device sector and has always placed greater emphasis on data integrity and on IT and software infrastructure usage.

Regulations and standards for medical devices should be considered from the following perspectives:

- cloud solutions used as part of a medical device
- cloud solutions used as part of infrastructure for supporting or manufacturing medical devices, or used in other quality management processes by medical device companies
- general legal requirements on data use, cyber security and critical infrastructure

1.2 European regulations

The Medical Device Regulation (MDR) and the In-vitro Diagnostics Regulation (IVDR) do not prohibit the use of cloud infrastructure and software. The MDR and IVDR do not address cloud systems specifically, but the general requirements they impose on IT infrastructure, software and IT security apply equally to cloud infrastructure and applications. New standards and new versions of existing standards are starting to consider the use of cloud applications in product development.

This chapter focuses on medical device manufacturers. Please note that medicinal product manufacturers have to comply with their relevant GxP national regulations (e.g. EU GMP Annex 11).

MDR/IVDR

The MDR and the IVDR are the main regulations for medical devices in Europe, with the exception of the United Kingdom, where the older Medical Device Directive (MDD) is still the primary medical device legislation. The MDR and IVDR require manufacturers to consider the design and operation of software and IT networks, as well as IT security, during device design. Manufacturers are also required to establish controls as part of their quality management processes. Based on European Unions approach, manufacturers have to consider harmonized standards, EU published common specifications or generally the state of the art when developing, operating and manufacturing medical devices. They have to look in relevant standards, the mentioned common specifications and recent guidance documents for deriving requirements concerning the application of cloud based solutions.

- Annex IX of the MDR obliges manufacturers to establish methods for monitoring the efficiency of the quality management system, in particular with respect to 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.

- Medical devices must fulfil basic safety and performance requirements set out in the MDR and IVDR. This means that **medical device manufacturers must consider risks arising from the IT environment and software, and must employ a state-of-the-art software development process, perform verification and validation, and employ a risk management process which also covers IT security risks. They must also formulate requirements for portable devices, IT networks and software security measures, and this must be clearly set out in the user manual.** All of these points also need to be addressed when using cloud infrastructure and services as part of a medical device.

National Laws

Each European Union member state is able to impose additional regulations for medical devices. Medical device manufacturers will need to check the applicability of national laws and regulations in each EU country in which they intend to market their device or software. Germany, for example, has a national law which imposes conditions additional to those imposed by the MDR/IVDR *(Medizinprodukteanpassungsgesetz)* and an additional regulation for medical device operators *(Medizinproduktebetreiberverordnung).*

Standards applicable to quality management systems: ISO 13485

Manufacturers in Europe can achieve conformity with European regulations by implementing a quality management system. When implementing a quality management system, manufacturers should be guided by ISO 13485, which is harmonized with the MDR. The 2016 edition of this standard was the first version to mandate validation of software used in quality management systems, specifically:

- implementation of a standard operating procedure (SOP)
- validation of software prior to use and after changes
- the validation workload should be risk-oriented

Any software, including cloud software and infrastructure, used to support quality management processes must therefore be properly validated. Implementation of a risk-based computerized system validation procedure, creation of a software inventory and validation of specific software systems used as part of the quality management system should be performed in accordance with the approaches set out in the guidance documents and non–binding standards presented in section 3.4.

Standards applicable during product development

Compliance with the General Safety and Performance Requirements (GSPRs) set out in the MDR and IVDR is usually achieved by ensuring compliance with the latest standards:

- Compliance with software-related GSPRs is ensured by adhering to IEC 62304 “Medical device software – Software life cycle processes”, which describes the activities and processes that need to be followed or performed when developing medical device software. These range from software requirements to functional software testing.
- For standalone software as a medical device, customer requirements and validation-related points not covered by the above are dealt with in IEC 82304-1 “Health Software – Part 1, general requirements” (figure 1). **This standard explicitly deals with health software such as cloud services which is not under the control of the manufacturer.** It sets out how manufacturers and operators should apply critical thinking to and document risks arising from the range of different uses and frequency of platform changes (e.g. updates).
- IEC 62304 and IEC 82304-1 can be viewed as describing general pointers for software development processes. They do not contain specific technical requirements for software in general or cloud systems in particular.

IT security is outside the scope of this white paper, but IT security for medical devices must be addressed during life-cycle and development activities and must include cloud systems. One standard worth mentioning in this context is

- IEC 81001-5-1 “Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle”, which is expected to be harmonised with the MDR. It introduces no new concepts for managing IT security, but provides guidance on which activities to perform during the health software lifecycle, and also covers cloud solutions.

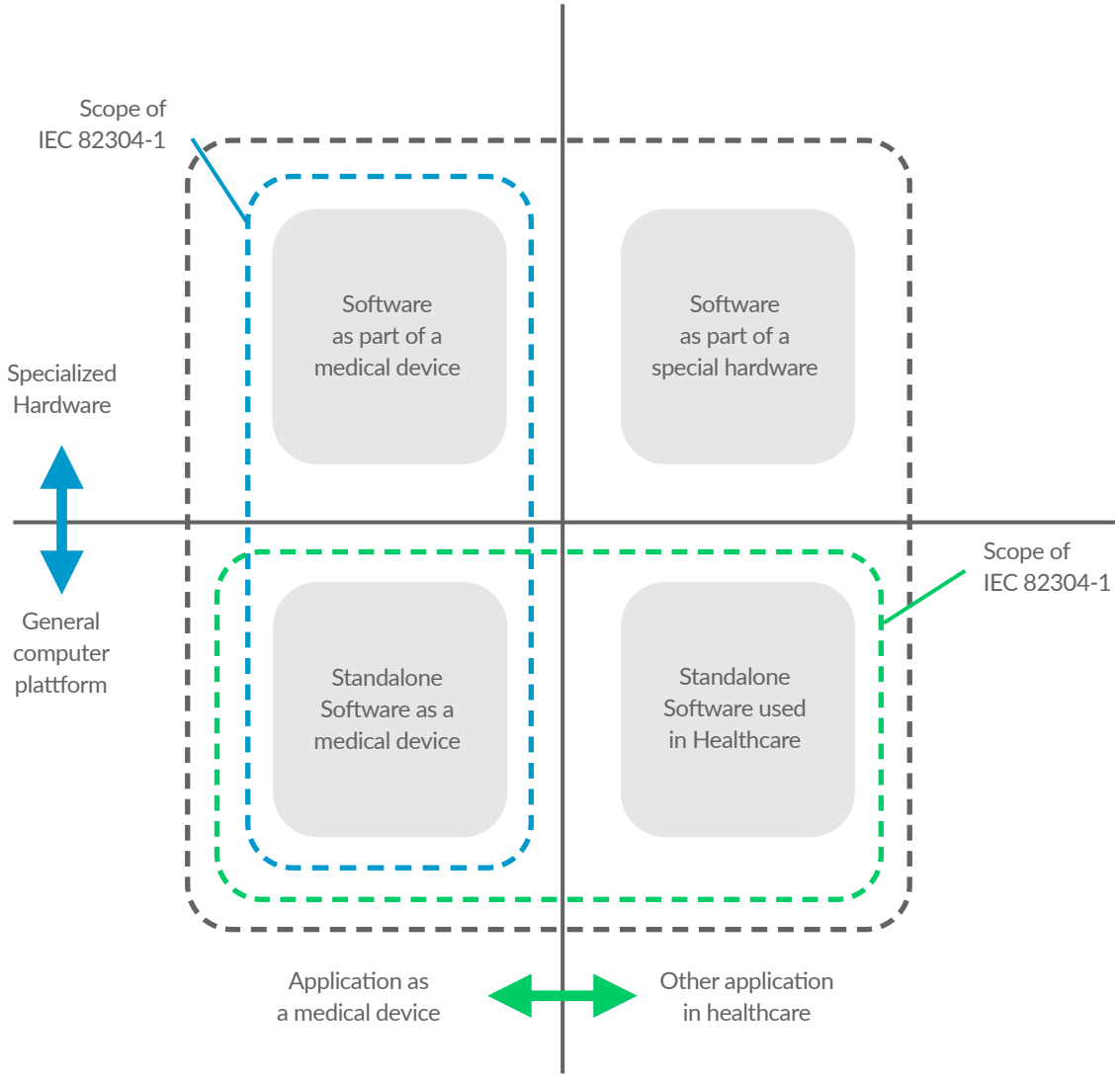


Figure 1: Domains of Health Software and scope of application of software development standards. Source-reference: Graphic originates from IEC 82304-1:2016, Annex A.2

1.3 USA

As with European regulations, US regulations do not prohibit the use of cloud infrastructure or applications relevant for medical device and pharmaceutical manufacturers. **FDA regulatory requirements for and guidance documents on software (validation, electronic records) have long played a major role in shaping how software is used and validated in the healthcare sector.** 21 CFR Part 11 has covered external software systems since 1997.

21 CFR Part 820 and 21 CFR Part 11

Requirements for and guidance on managing software in medical devices or as part of a medical device manufacturer's quality management system are set out in 21 CFR Part 820 and 21 CFR Part 11.

- 21 CFR Part 820 mandates the implementation of design controls (820.30) and the validation of computer software used as part of production or quality systems (820.70)

- The requirements set out in 21 CFR Part 11 have played a major role in shaping how computerized systems in quality management systems or used as part of a product are used and validated. Published in 1997, 21 CFR Part 11 is relevant for medical device and pharmaceutical manufacturers and distinguishes between open and closed systems. In closed systems, access is controlled by the person responsible for the content of electronic records. Open systems are systems in which controlled access cannot be fully guaranteed.

Controls for closed and open systems are:

- Systems need to be validated (accuracy, reliability, identification of altered or invalid records) according to 21 CFR Part 11, §11.30
- Generate human readable copies of electronic records (including audit trail)
- Records must be protected
- Limit system access and perform authorisation
- Use a secure, timestamped audit trail, which tracks changes to records
- Operational system checks as appropriate
- Device checks to determine the validity of data input sources and operational instructions
- Verifying that people developing or using systems that handle electronic records are properly trained and educated
- Appropriate control of system documentation, i.e. access to system operation and maintenance documentation and control procedures, access to development and system documentation

Part 11 requirements have undoubtedly had a significant impact on the debate over whether cloud systems can be used as part of and during production of a medical device and what sorts of cloud systems are permissible.

Part 11 contains the important concept of open and closed systems and already in 1997 discussed the potential use of external systems not under the vendor's control in electronic data processing. Some providers have even gone so far as to claim that, under the terms of their contracts, their services should be considered closed systems, depending on how personnel, system access, documentation and validation state are split between the regulated company and the cloud-service provider.[10]

FDA Guidance Documents

FDA guidance documents are non-binding in nature, but offer valuable insights into and additional information on how the FDA understands specific legal requirements. The FDA has published the following documents on software validation and Part 11, which are relevant for medical device manufacturers:

- General Principles of Software Validation; Final Guidance for Industry and FDA Staff, January 11, 2002
- Guidance for Industry Part 11, Electronic Records; Electronic Signatures – Scope and Application, August 2003

While the Part 11 guidance provides clarification concerning electronic records and signatures and addresses pharmaceutical manufacturers as well, the validation guidance is relevant for medical device manufacturers only and is intended to address software validation in a similar manner to ISO 13485.

Notably, the FDA first released guidance on cybersecurity for medical devices in 2005 and has released new cybersecurity guidance regularly. Although they do not address cloud services used as part of a medical device specifically, **FDA guidance documents should also be taken into account when designing cloud-based solutions.**

1.4 Additional laws, standards and guidance documents

Medical and pharmaceutical device manufacturers are left to their own devices when it comes to implementing a specific process for computerized system validation. Help is at hand, however, in the form of non-binding standards and guidance documents produced by experts for the medical device and pharmaceutical sectors. Guidance documents offer especially the advantage that they can be updated more frequently and more flexibly than regulations and are therefore more precise and more in keeping with the current state of technology.

When setting up software validation processes for software applications and infrastructure used as part of a medical device or drug manufacturer's quality management system, it is worth considering the following guidance documents and standards:

- ISO 80002-2 "Validation of software for medical device quality systems"
- AAMI TIR 36 "Validation for software for regulated processes"
- "GAMP 5 - a risk-based approach to compliant GxP computerized systems"
- ISPE guidance documents, e.g. "IT Infrastructure control and compliance", which explicitly looks at management of cloud applications and infrastructure
- PIC/S, ICH, MHRA and FDA guidance documents on data integrity
- Data protection regulations, e.g. the European Union's General Data Protection Regulation (GDPR)

Newer versions of guidance documents on validation or data integrity are starting to address the use of cloud software solutions.

See Appendix page 42 for a detailed overview of these guidance documents.

1.5 Regulatory challenges and trends in cloud usage

In section 1.2, we discussed the absence of specific requirements for and restrictions on the use of cloud software solutions in European laws and regulations. We also saw that current standards and guidance documents are applicable and newer editions are starting to address cloud components.

US regulations, which date back to 1997, also don't provide specific requirements for the use of cloud systems. 21 CFR Part 11 lists requirements that need to be met when using open systems, and that therefore also need to be considered when using cloud systems.

The debate around whether cloud-based applications or infrastructure can be used at all can therefore be considered to be closed. **Nonetheless, it's important to identify and review cloud-related risks critically. Deciding whether or not to employ a cloud solution always depends on the individual case, and it will always be important to establish appropriate controls for the specific case.**

US regulators are aware of the challenges involved in applying new technology and are eager to provide manufacturers with guidance. To this end they are devising new guidance documents and submission procedures. The FDA's draft guidance on Data Integrity and Compliance with CGMP, published in 2017, is one of the first, if not the first, regulatory guidance documents to use the term "cloud".

Still under development is the long-awaited Computer Software Assurance guidance document, which will advocate 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[9]. The FDA has also launched multiple strategic initiatives and programs centred around the regulation of new technologies in pharmaceutical and medical device development and production (e.g. **Strategic plan on regulatory science, 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.

There is nonetheless still considerable uncertainty around how to manage cloud infrastructure and software, especially where this software plays a role in quality management. Current standards and guidance documents do not specifically address cloud systems. Would additional regulation make it easier for manufacturers to decide on and validate cloud-based software or infrastructure? **From a medical device regulatory perspective, we think that the regulatory requirements are about right and that available tools for managing these requirements are sufficient.** Manufacturers should not hold off from using cloud-based solutions. They should make use of technical expertise and guidance which fills in the technical background to the technology, and examples and explanations of how to apply it and of associated regulatory processes.

The FDA's CSA approach signposts the direction that needs to be taken 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. Such an approach would need to meet any IT security requirements imposed by national legislation. Guidance in practical guides such as this whitepaper can be updated frequently, delivering state of the art approaches to dealing with novel technologies such as cloud systems.

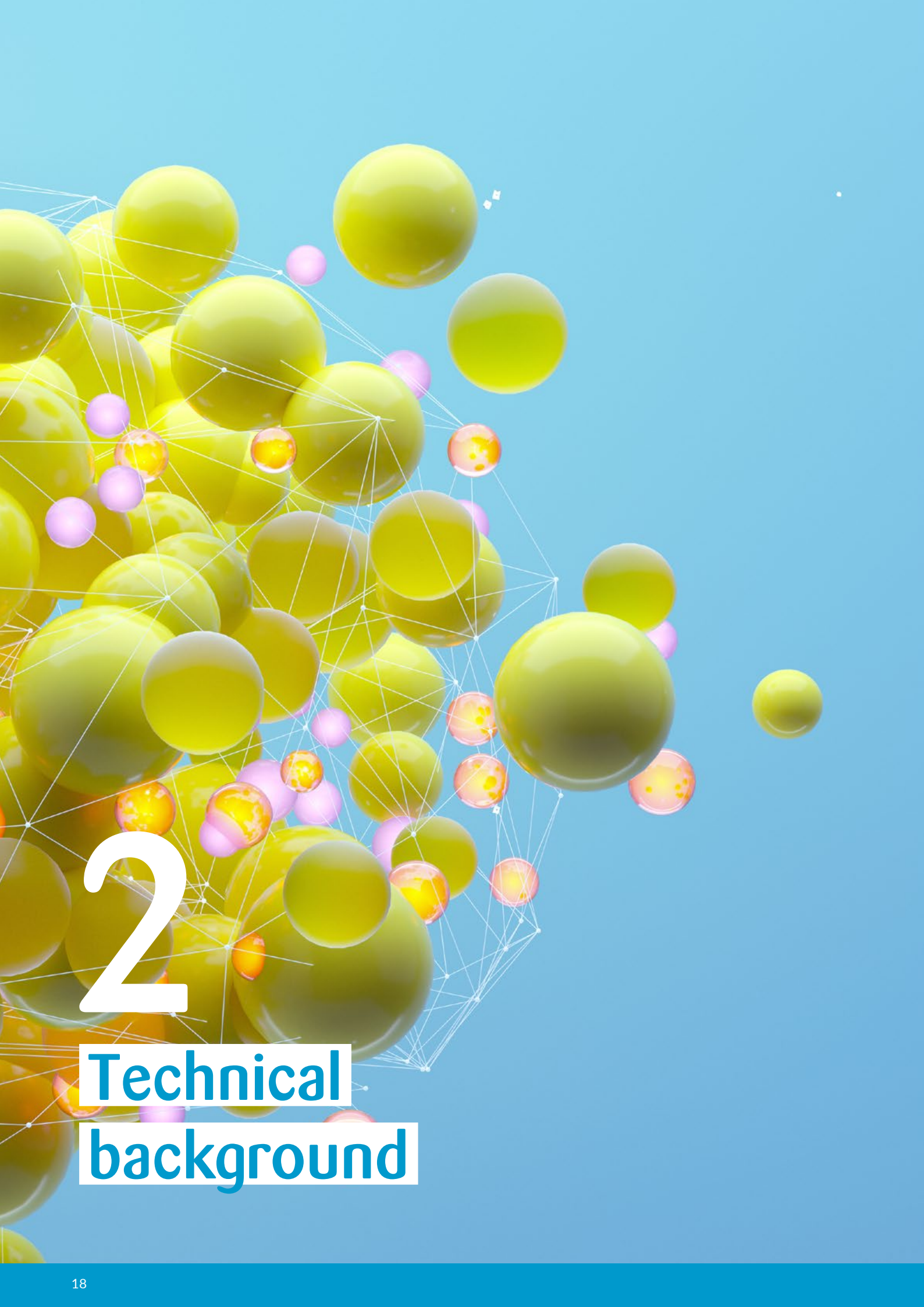
1.6 Our proposed approach to achieving regulatory compliance

Taking into account the technical nature of cloud applications and infrastructure (which will be explored in section 2), pursuing 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 and revalidation tailored to change impact and risk, cloud systems require constant monitoring and validation testing. This is because cloud solutions tend to be subject to frequent updates and frequent changes to the underlying infrastructure and services. To build test-automation solutions for all application layers for cloud applications would be too time-consuming and would generally 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 combining different activities as described in Computerized System Validation (CSV). Our approach has the following main elements:

- Use critical thinking and risk management to identify appropriate validation activities.
- Where feasible and applicable, continuously implement cloud test automation using standard tools provided by the cloud provider.
- Reuse established architectural patterns provided by the cloud service provider.
- Continuously monitor and evaluate changes to the system by conducting regular assessments of cloud systems based on criticality and risk.
- Make use of cloud service provider management artifacts, e.g. request any required certificates, establish service contracts and perform audits.

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



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. 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 point is that **the chosen solution should meet your 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 3 levels which differ in how responsibility is split between cloud service provider and 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.

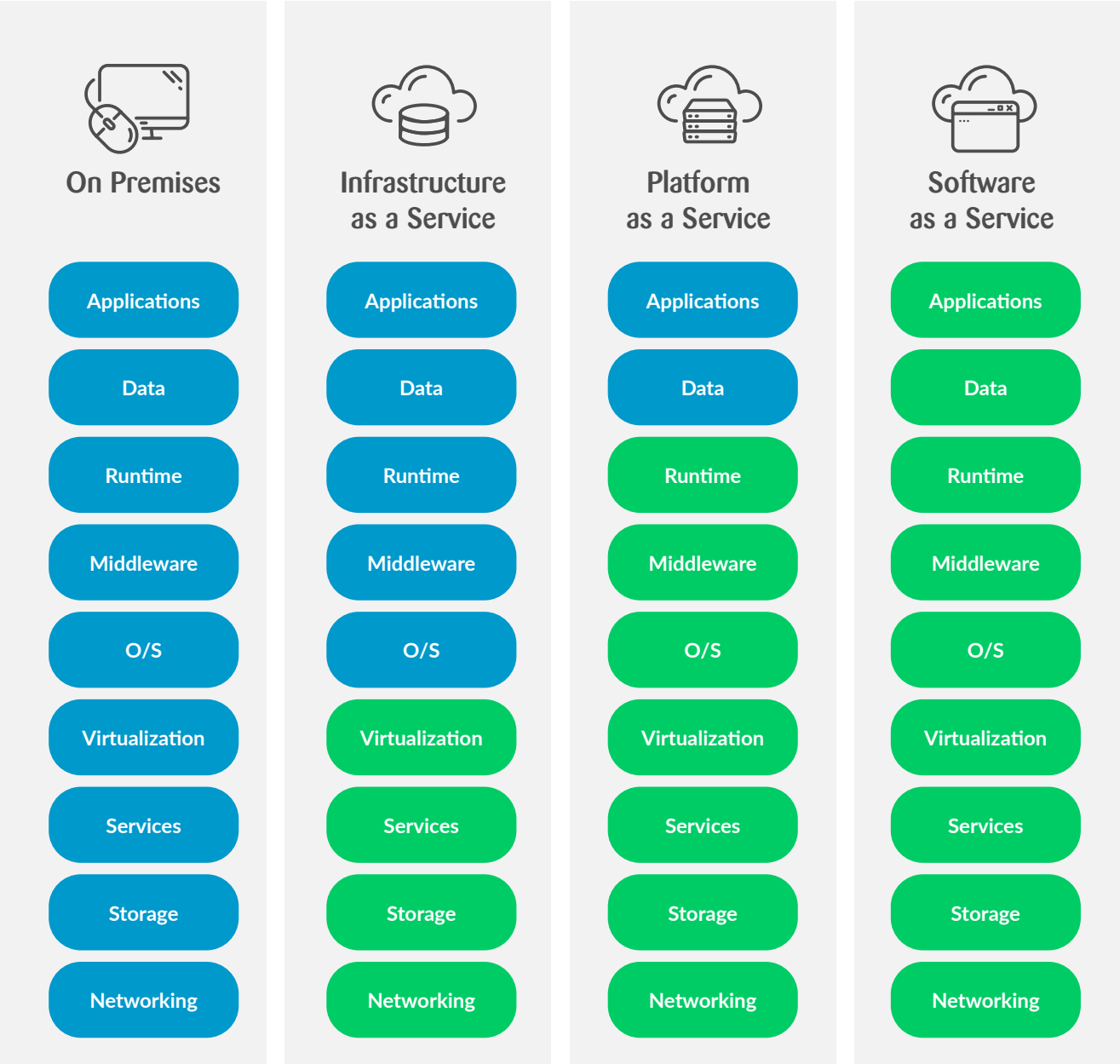
Software as a Service (SaaS)

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 utilising 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 leveraging the certification status of your cloud service provider or cloud vendor for your validation activities.**



Source: Zühlke

Figure 2: Differences between On Premises, IaaS, PaaS and SaaS. ● you manage ● others manage

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.

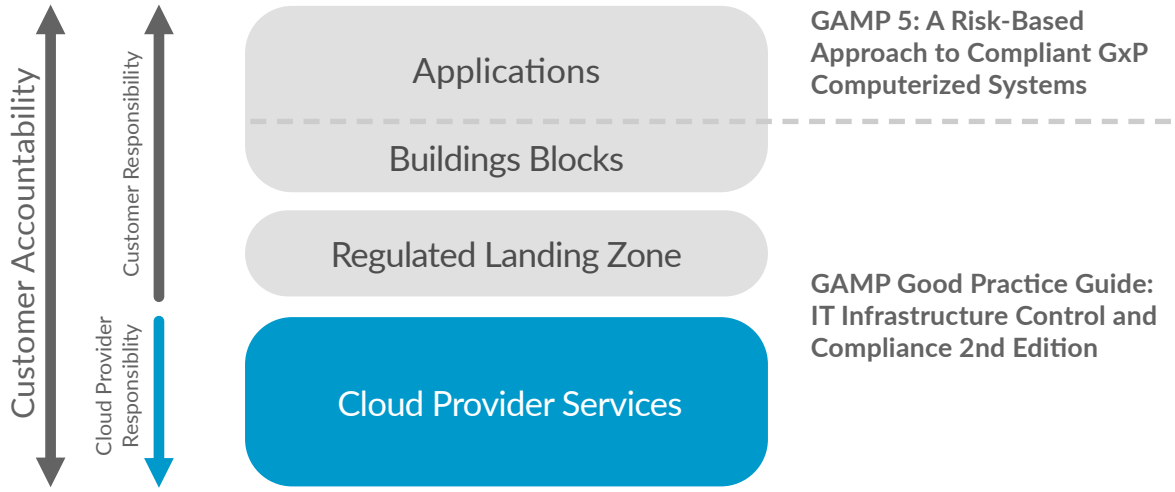


Figure 3: Requirements of compliant systems.

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. A comprehensive description of and guide to choosing the right digital health platform on which to build your products can be found in the white paper **Digital Health Platforms – For a future of more connected end-to-end patient experiences.**

2.6 Regulatory & Strategic Summary

The use of cloud solutions means adopting a very 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 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.**

Current regulations in Europe and the US do not prohibit the use of cloud systems as part of a medical device or as part of quality management software which is subject to validation. Newer guidance documents and standards are starting to be adapted for cloud systems, and to cover areas such as cyber security, 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 computerized systems validation, which elevates critical thinking (CSA) above extensive testing (CSV).

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 integrity. 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.

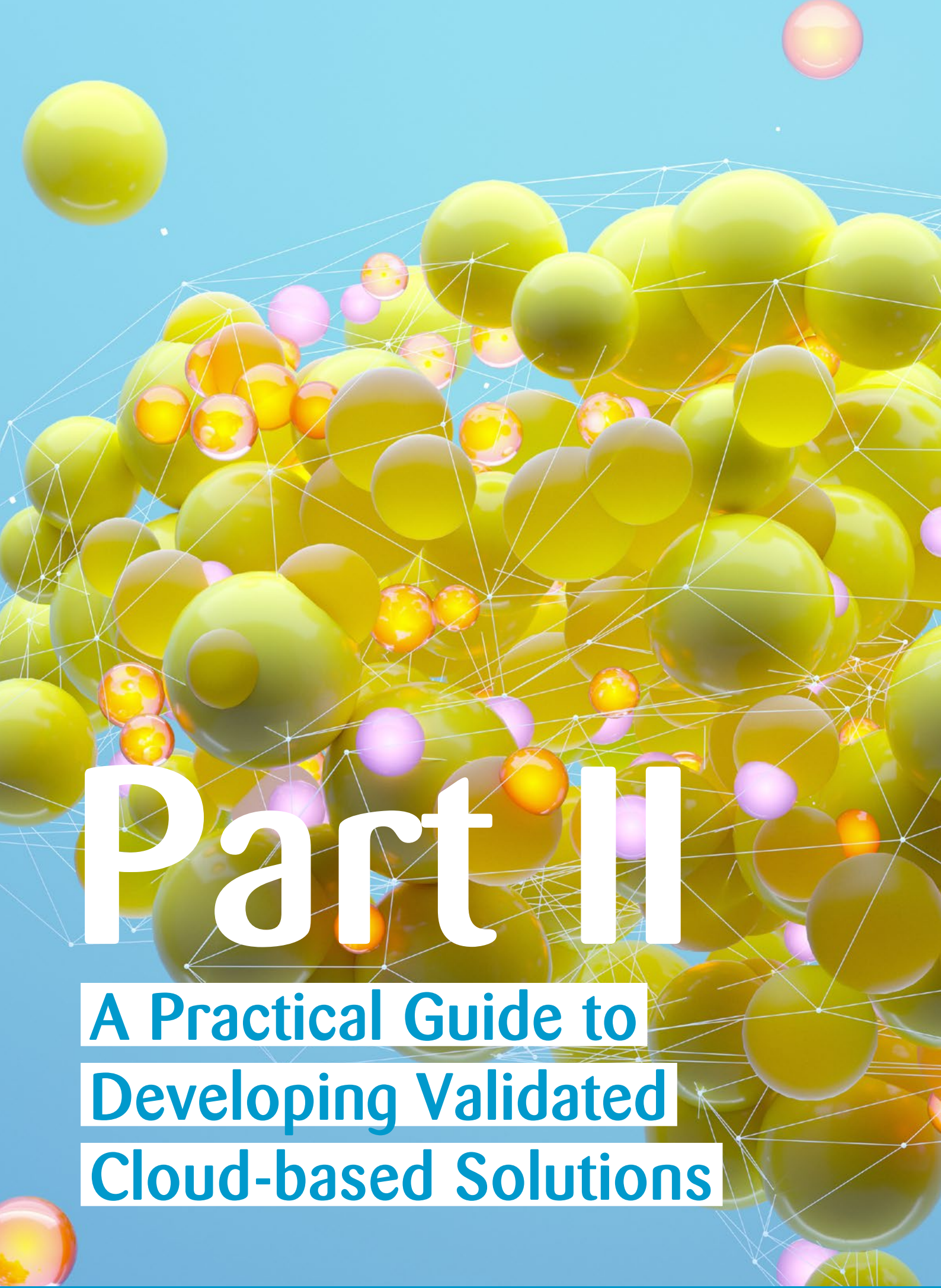
3

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.

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 and to software used as part of a quality management system. 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 computerized 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, cyber security and data integrity-related technologies and continuous validation based on periodic evaluations and test automation.



Part II

A Practical Guide to Developing Validated Cloud-based Solutions

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 technical blueprint, which is described in chapter 4.1 We also discuss technical approaches to and procedures for each project phase from concept through to retirement.

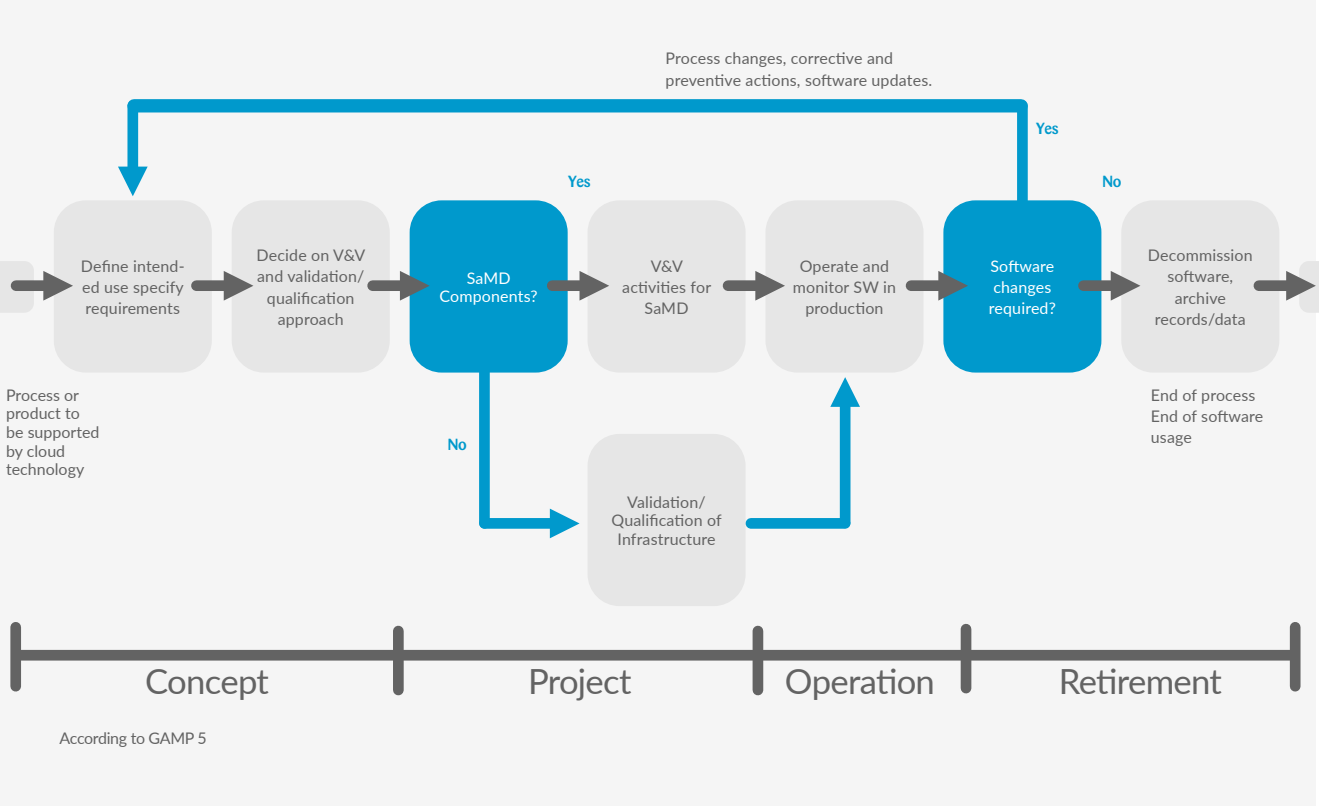


Figure 4: Verification and validation lifecycle activities for or SaMD, cloud based software as part of QM and corresponding cloud infrastructure.

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

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

QMS considerations

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.

Technical considerations

- 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

- 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.

QMS considerations

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 cyber security protocols for cloud systems or extend existing protocols.
- Incorporate an assessment of controls which are the responsibility of the cloud provider.

Technical considerations

- Involve the cloud service provider and/or other experts in requirements engineering and risk analysis.
- Cloud service providers often offer white papers, checklists and blueprints to support this process.
- Use a zero-trust[1] approach to security.

[1] https://en.wikipedia.org/wiki/Zero_trust_security_model

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

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.

QMS considerations

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 1–6 months, depending on how critical the system is.

Technical considerations

- Identify cloud services able to support continuous validation and define the validation chain architecture.

Understand the difference between infrastructure, runtime services and SOUP

In conventional systems or products, it's easy to differentiate between infrastructure, runtime elements and components that need to be treated as software of unknown provenance (SOUP). In cloud-based systems, this distinction is less clear, since services can fall into any of these three categories depending on how they are integrated into the architecture or solution.

Process 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.

QMS considerations

- 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.

Technical considerations

- Minimise the use of SOUP and base your architecture on cloud services which use the shared responsibility model.

Typical requirements include:

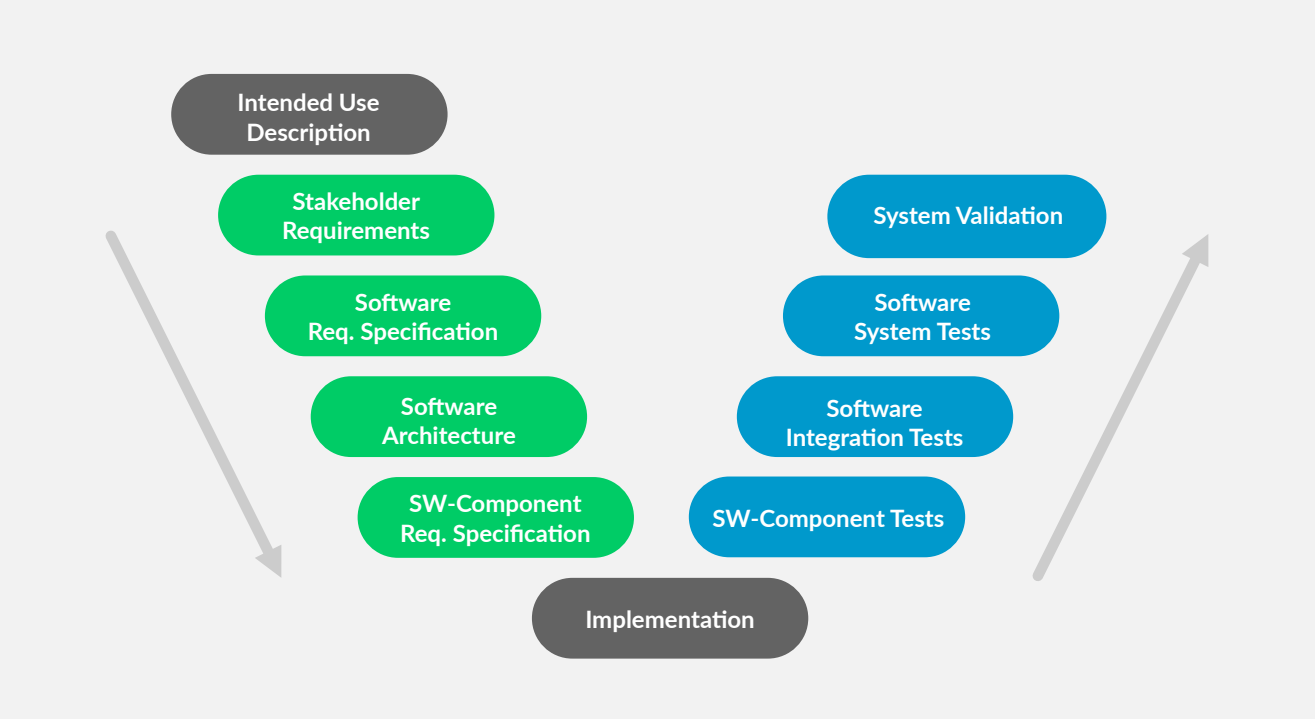
- provider location (data protection legislation)
- performance
- required features (e.g. database with audit trail)
- scalability (planned features need to be able to grow)
- cloud provider auditability
- any mitigations from the risk assessment

Typical points for consideration during risk assessment include:

- cloud system availability
- risk of data loss
- risk of data falsification
- cyber security 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 check-points.



Source: Zühlke

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 activites.

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

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

QMS considerations

- Establish SLA and quality agreements.
- Establish servicing, maintenance and monitoring procedures for the cloud service used.
- Incorporate cloud service considerations into PMS activities.

Technical considerations

- n/a

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

- 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.

QMS considerations

- Ensure that cybersecurity risks are properly covered by processes and guidelines.
- For software as a medical device, define SOPs for managing SOUP.

Technical considerations

- Set up automated vulnerability, network security and intrusion detection (Amazon Inspector & GuardDuty, Azure Defender, etc).
- Consider making use of architecture/security reviews provided by the cloud service provider.
- Check the architecture against available guidelines and blueprints.
- Consider early stage performance and penetration tests.

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

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.

QMS considerations

Define strategy, guidelines and processes for de-coupling 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.

Technical considerations

- Chose 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

- 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.

QMS considerations

- 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.

Technical considerations

- 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 (SonarCube, 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 Files, 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

- 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.

QMS considerations

- 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.

Technical considerations

- Chose and implement an appropriate CI/CD solution (AWS CodeBuild & CodePipeline, Azure Pipelines, 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.

Process 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 triggers on-demand tests.

QMS considerations

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 therefore 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).

Technical considerations

- 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, Azure Defender & 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

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.

QMS considerations

- Ensure that proper procedures for evaluating failed tests are in place and that immediate actions and communications are defined.

Technical considerations

- 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

- Identify a location for long-term storage of any data that needs to be retained for regulatory reasons.

QMS considerations

- 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.

Technical considerations

- 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

- 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.

QMS considerations

- 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.

Technical considerations

- 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

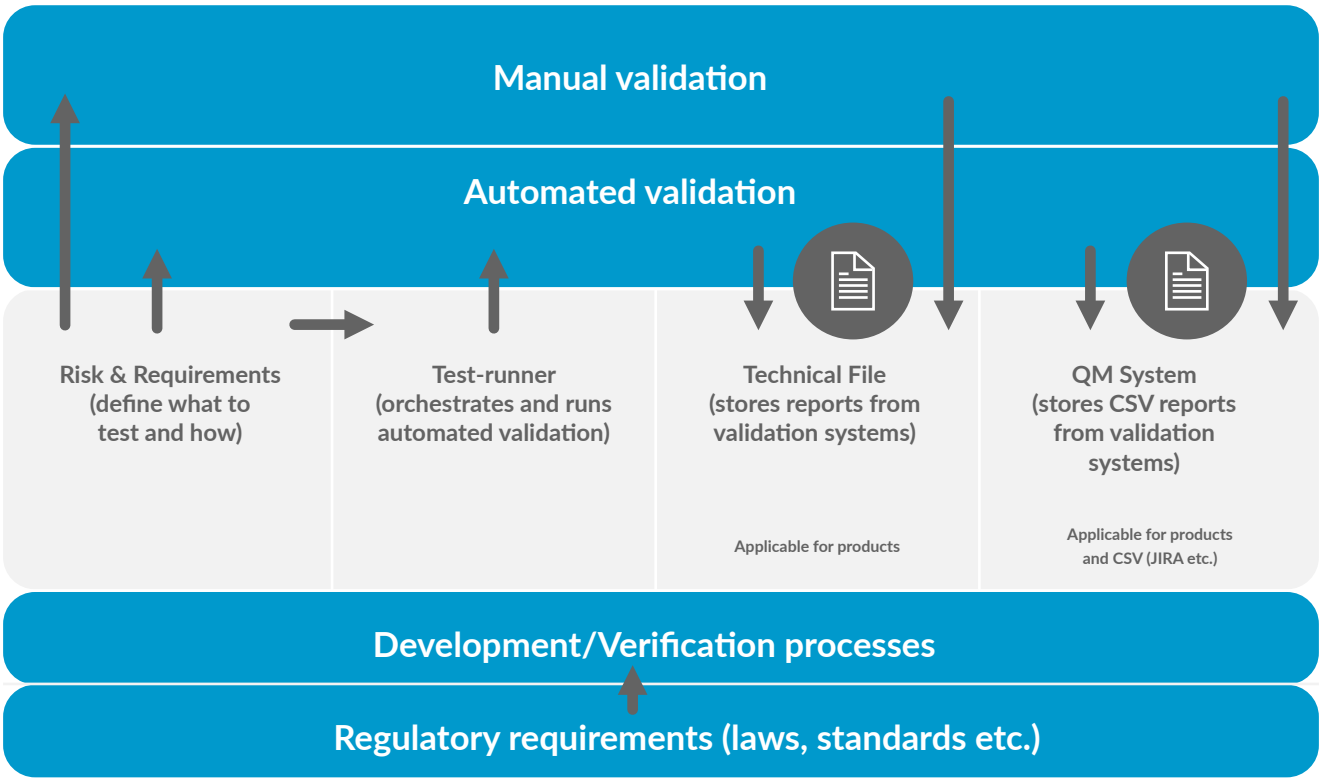


Figure 6

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 it in the QM system for auditing processes.

As discussed above, automated validation is a powerful tool for ensuring that your product or service is still working as 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.

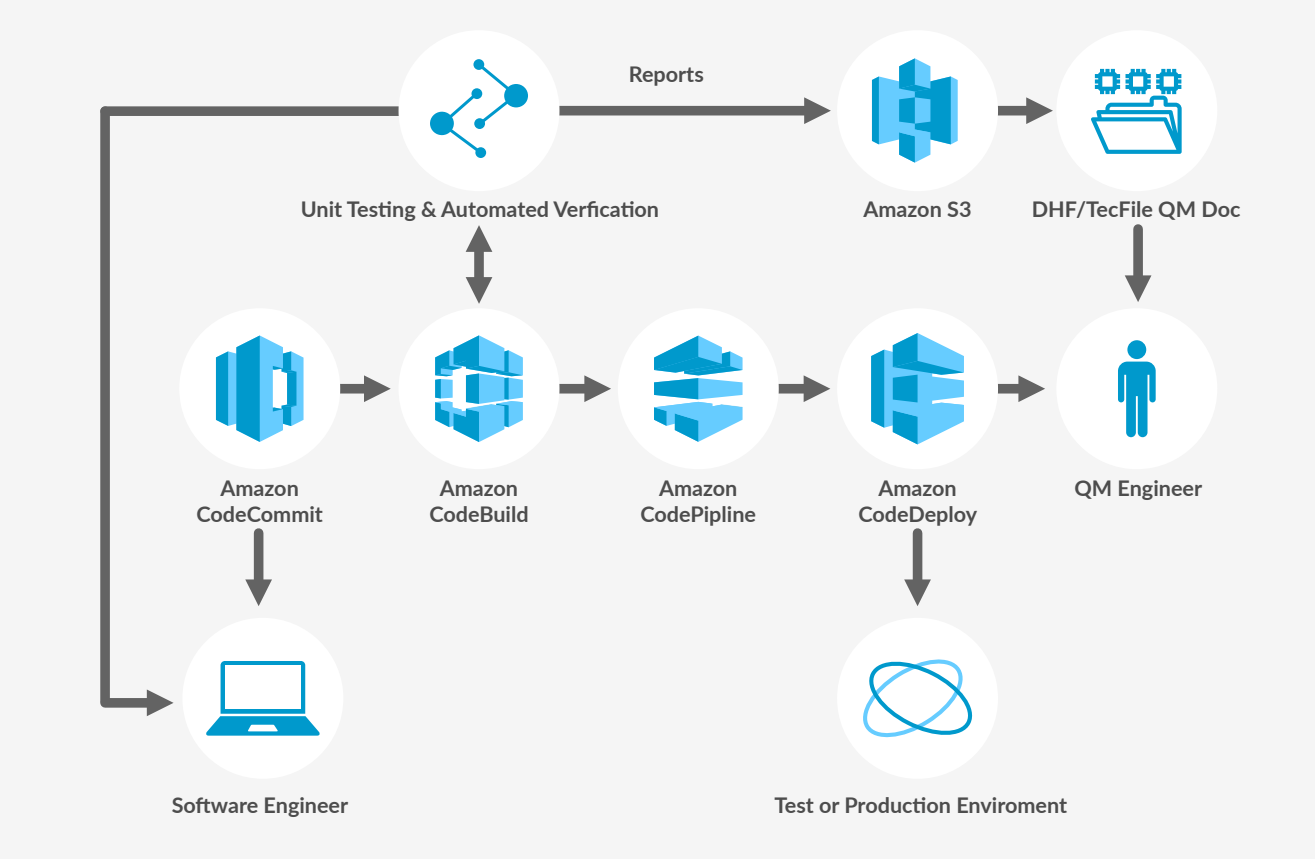


Figure 7: AWS CI/CD Example: On AWS you can set up CI/CD using cloud-native services such as Amazon CodeCommit (or Git or another version control system), CodeBuild, CodePipeline (CI) and CodeDeploy (CD).

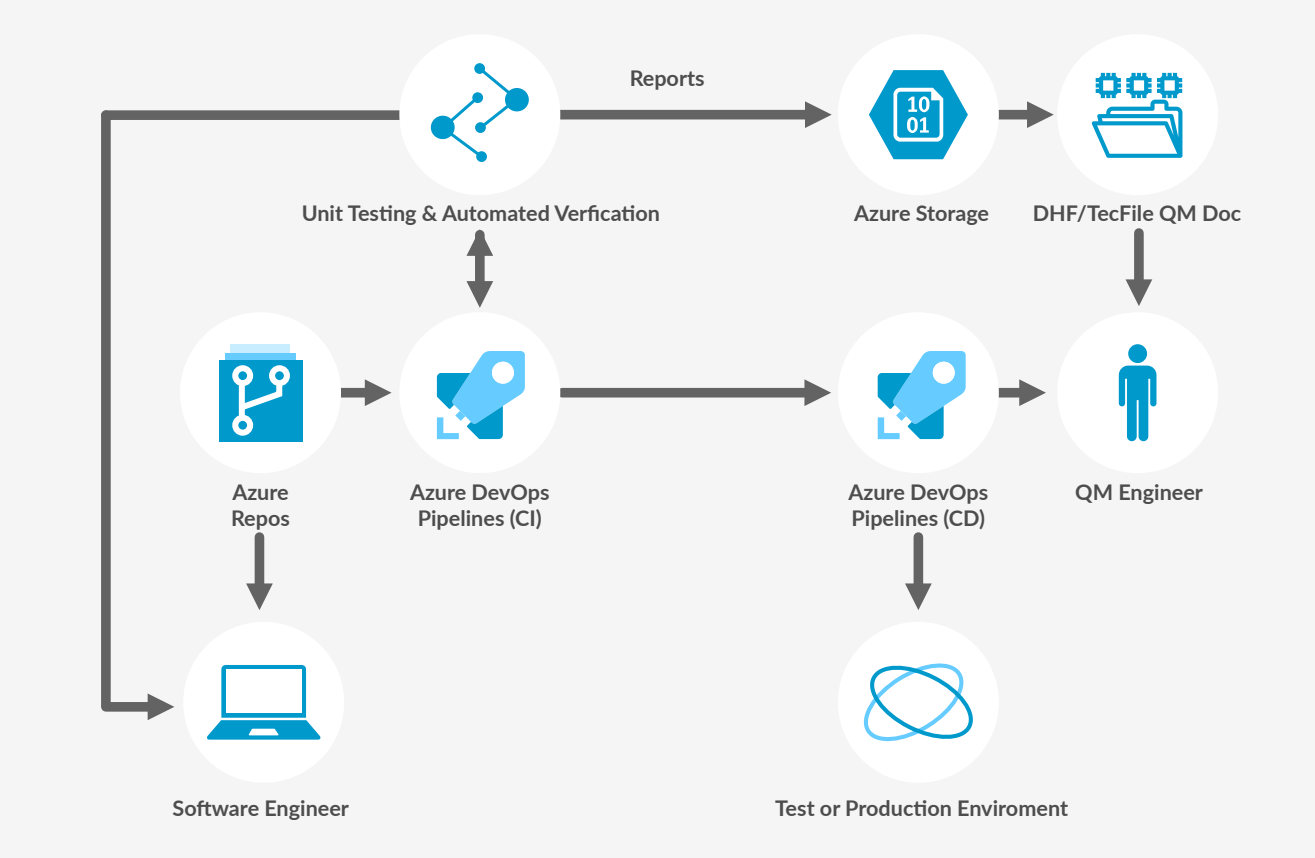


Figure 8: Azure CI/CD Example: Setup on Azure is somewhat simpler, as Azure DevOps Pipelines deals with both CI and CD.

Minimum blueprint for compliant cloud production deployment

There is no one-size-fits-all solution, but below we offer basic blueprints for AWS & 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 control over storage, analysis, and remediation actions.
- **Amazon CloudWatch** – collects monitoring and operational data in the form of logs, metrics, and events. Detects anomalous behaviour in your environments, sets alarms, visualises logs and metrics side by side, takes automated actions, troubleshoots issues.
- **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.

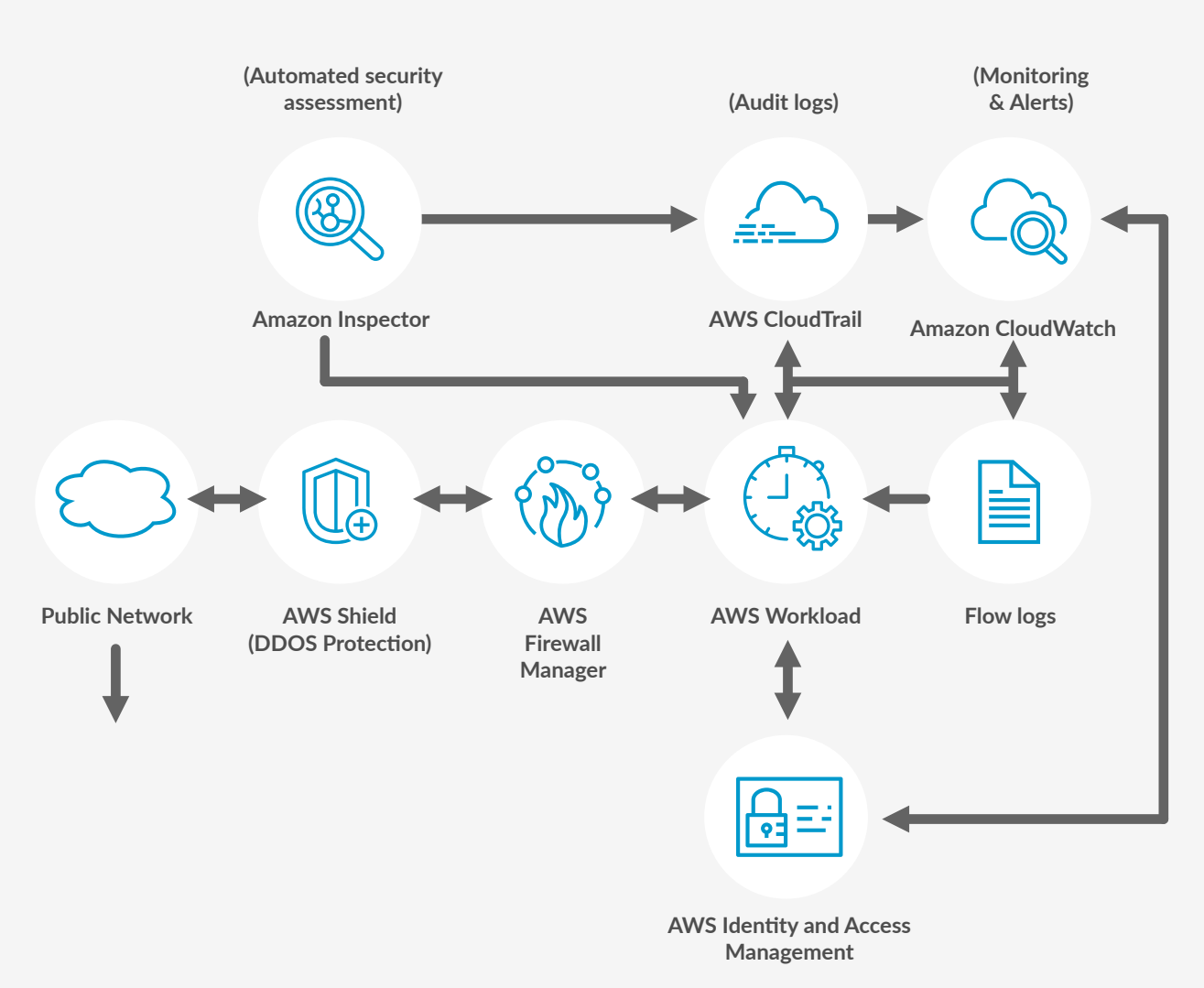


Figure 9: Sample AWS blueprint

On Azure, services that help to achieve compliance are:

- **Azure Defender** – is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, 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.
- **Azure Active Directory** – (Azure AD) enterprise identity service provides single sign-on, multifactor authentication, and conditional access to guard against 99.9 percent of cybersecurity attacks.

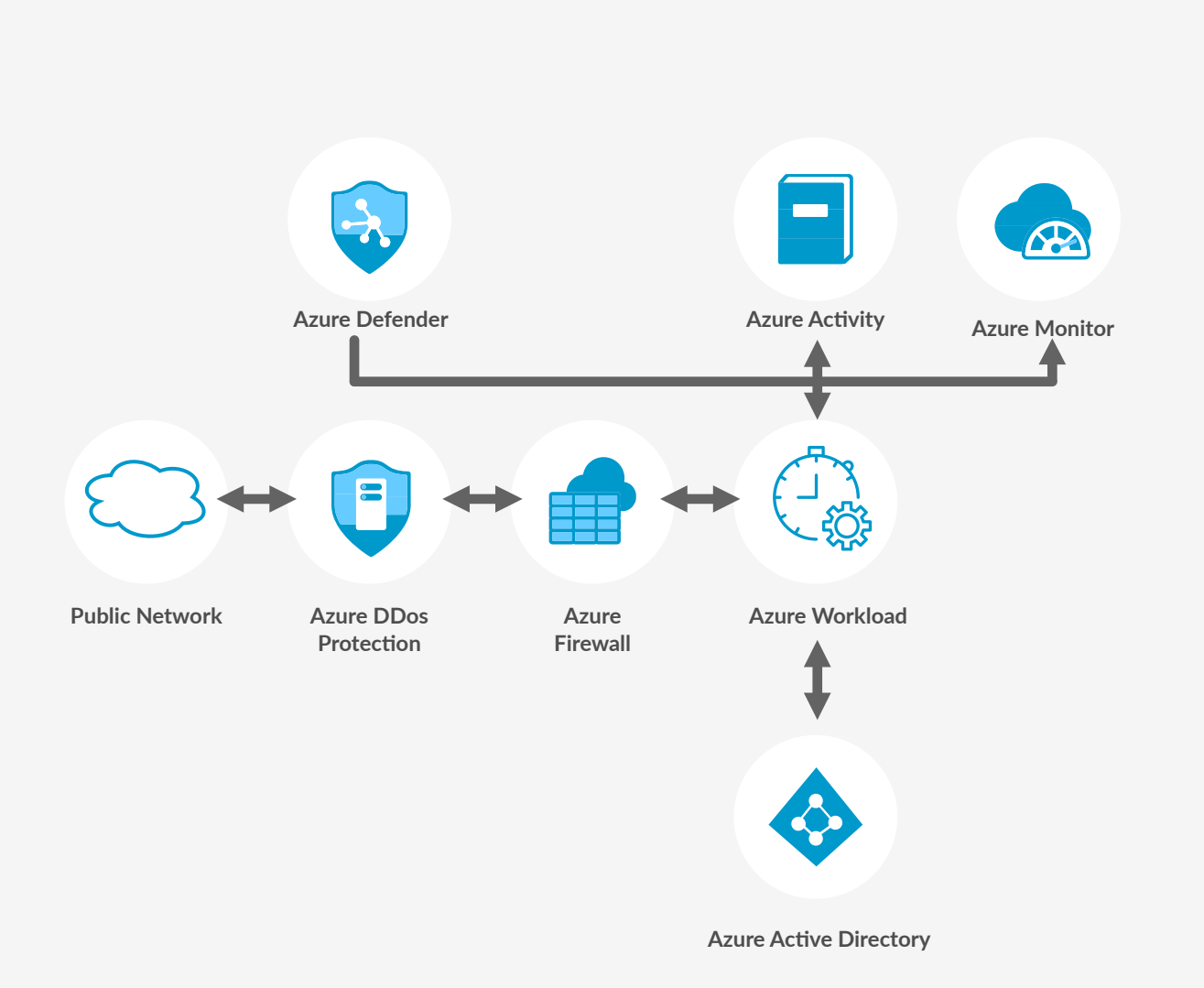


Figure 10: Sample Azure blueprint

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

- ISO 80002-2 “Validation of software for medical device quality systems” can be used to set up a risk-based framework for software validation for computerized systems. ISO 80002-2 is not a harmonized standard under the MDR. The risk-based approach and general process appear to represent an appropriate approach, which can also be used for validating cloud systems. It lacks examples or specific recommendations for dealing with cloud-based systems.

- AAMI TIR 36 “Validation for software for regulated processes” describes a risk-based approach that can be applied to quality management systems. The concepts and approaches underlying this standard are similar to those underpinning ISO 80002-2. As with ISO 80002-2, the examples section lacks examples relating to cloud systems and it also lacks specific recommendations for dealing with cloud systems.

- “GAMP 5 - a risk-based approach to compliant GxP computerized systems” is a large framework which includes suggestions for classification, documentation and most importantly how to apply risk management and critical thinking to software validation tasks. GAMP 5 does not include specific recommendations on validation of cloud systems. The risk–based approach, lifecycle concept and supplier management system appear to be appropriate for identifying controls for cloud systems used in a production environment. The latest edition of the ISPE guidance document “IT Infrastructure control and compliance” outlines a similar approach.

- GAMP 5 represents a sound guide to setting up a risk-based validation framework, but publisher ISPE also publishes additional good practice guides, addressing in more detail subjects complementary to the GAMP framework. The most recent guidance document is “IT Infrastructure control and compliance”, published in 2018 dealing with cloud validation aspects, which includes recommendations on assessment and validation of cloud systems.

- PIC/S and ICH published several guidance documents on GxP and data integrity. In recent years, the pharmaceutical industry in particular has started to focus more closely on software and validation-related data integrity issues. PIC/S published a guidance document on data integrity in July 2021. Of note is that it is their first guidance document to include the word “cloud”. The FDA published a guidance document on data integrity in 2018. None of these guidance documents provide specific guidance on cloud systems, so drug manufacturers really need to understand the technology they are using and its effect on products and data. Data integrity recommendations contained in these documents should nonetheless be taken into account when using cloud systems in a production environment.

- There are specific data protection regulations in force in Europe and almost every other country. Companies need to check that the cloud functionality and cloud storage they are planning to deploy are compatible with local data protection legislation. Regulatory authorities may also set out additional requirements or recommendations. The German Federal Office for Information Security has published guidance documents on cyber security which also cover cloud systems and cloud providers.

4.3 Glossary

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 method of hybrid deployment is between the cloud and existing on-premises infrastructure to extend and grow an organization'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 is serving its members by leading scientific, technical, and regulatory advancement throughout the entire 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 organizations 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).
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 life cycle 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 Computerized Systems, ISPE, 2006
[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 Offthe-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)

Authors

Peter Bäck
Zühlke Engineering AG

Peter Bäck has been Principal Business Consultant at Zühlke since 2018. He has over 22 years experience in software engineering, software architecture, and building and leading teams. His main focus is cloud technologies and he is currently working on several cloud-based machine learning-enabled SaMD projects He has an MSc in Computer Science.

Christian Berger
Zühlke Engineering AG

Christian Berger is a Lead Project Manager and has been with Zühlke since October 2008. His main area of expertise is the regulated environment. He primarily works on medical & laboratory equipment and machinery & manufacturing. His passion is working on large, complex, strongly interdisciplinary IVD device projects.

Urs Müller
Johner Institut

Urs Müller works as a consultant in the Johner Institute's Swiss office. He supports customers and projects in the areas of product development and development of medical technology production equipment, with a focus on verification, validation (CSV) and software development. Since completing his computer science degree, Urs has been working in the service environment of software development, first as a software test automation engineer/software tester, then as a team leader at an engineering company focused on medical product development.

Patrick Steiner
RetinAI Medical AG

Patrick Steiner worked at Zühlke from 2016 to October 2021 before joining RetinAI Medical AG as a Senior Project Manager. He is actively engaged in enabling cloud-based SaMD solutions for enhancing the efficiency of ophthalmological drug development and patient care. His focus is on pragmatic, lean implementation of digital regulated medical products. Patrick Steiner has an MSc ETH in Biomedical Engineering and a PhD in Biomedical Imaging.

Published by

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

E-mail: info@zuehlke.com
CEO: Nicolas Durville

Pictures: Getty Images Deutschland GmbH

www.zuehlke.com

Version 1, May 2022