zenon
by COPA-DATA

zenon in regulated industries

EU GMP Annex 11

www.copadata.com
pharmaceutical@copadata.com

Content

Revision History

Rev.	Date	Author	Description
1.0	Nov-2016	Robert Harrison	First issue
2.0	Mar-2020	Giuseppe Menin	Review zenon Supervisor 8.20 & zenon Analyzer 3.40
3.0	Oct-2022	Giuseppe Menin	Review zenon Software Platform 11
4.0	June-2023	Bernhard Korten	Review zenon Software Platform 12

1. Executive summary

The EU GMP Annex 11 regulation concerns all computerized systems (i.e. a set of software and hardware components which together fulfill certain functionalities) used as part of GMP-regulated activities.

Compliance with the requirements of the EU GMP Annex 11 throughout the system lifecycle guarantees that there is no increase in overall risk in the controlled process and no decrease in product quality, process control or quality assurance compared to manual operations. COPA-DATA and its zenon Software Platform provide solutions that ensure compliance in GMP-regulated environments. A strict internal company-wide quality management system provides development procedures that ensure high quality and reliable products. We provide solutions which adhere to the EU GMP regulation while also providing the most efficient platform to develop regulated projects, enabling efficiently engineered solutions that reduce the validation effort needed.

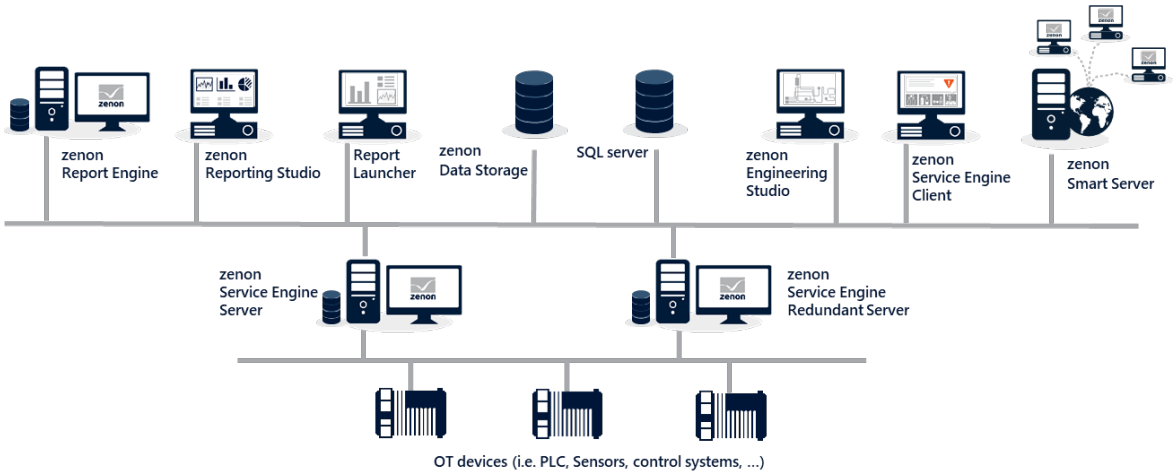
2. Introduction

This document details information on how zenon is in full accordance with the EU GMP Annex 11 regulation (Euralex - Volume 4, Good Manufacturing Practice, Medical Products for Human and Veterinary Use, Annex 11: Computerized Systems).

Each section states the Annex 11 text, followed by the zenon capabilities which provide the functionalities to fulfill the requirements set out in that section of Annex 11. Since each project design and implementation is specific, each project must be individually assessed and qualified using the full Annex 11 criteria. Ultimate responsibility for system compliance falls to the regulated company that uses the system.

2.1. Scope – System Architecture

This document applies to the zenon Software Platform consisting of the following modules:



- zenon Engineering Studio → This is an administration module used to configure projects, i.e. HMI screens, recipes, audit trail, user levels, etc.

- zenon Service Engine → This is a module used by end users to execute projects configured in zenon Engineering Studio.

- zenon Reporting Studio → This is an application used by administrators to configure reports and layouts using report templates.

- zenon Report Engine: This is the application generating reports based on predefined templates, using real time and historical data produced within zenon platform and linked external databases.

- Report Launcher → This is a web client where configured reports are made available to end users who can then launch, display, print and export the reports.

- zenon Data Storage -> This is a zenon service, based on MongoDB technology, where historical data produced in zenon software platform are stored (E.g. Time series process values, Alarm history, Audit Trail).

- zenon Smart Server -> This service offer access to zenon application via Web Clients.

3. Annex 11

3.1. [1] Risk Management

Risk management should be applied throughout the lifecycle of the computerized system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerized system.

Customers are responsible for implementing risk management in order to determine the extent of validation and data integrity controls.

zenon Service Engine, zenon Report Engine:
COPA-DATA software development operates according to *SEI CERT Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems* and the OWASP Top 10 standard awareness document for developers and web application security.
According to these standards, COPA-DATA operates precisely defined processes and procedures.

3.2. [2] Personnel

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

Customers are responsible for identifying the Process Owner, System Owner, Qualified Persons and IT and for guaranteeing that all personnel have appropriate qualifications, roles and defined responsibilities.

In terms of levels of access, the zenon Software Platform provides state-of-the-art technical measures as described below.

zenon Service Engine
Utilizing zenon's authorization levels, different layers of security can be applied to different users or user groups.

Each dynamic element accessible to a user can have an authorization level attributed to it. Therefore, the logged-in user must hold the specific authorization level in order to execute each dynamic element.

zenon Report Engine
Access to zenon Report Engine is limited only to authorized users, i.e. users who have been enabled by the Administrator to access the Report Launcher.

3.3. [3] Suppliers and Service Providers

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

zenon Service Engine, zenon Report Engine
COPA-DATA offers a range of support services for its products.
In addition to the basic services, a customer can opt for a Premium Service Level Agreement (SLA).
For more information about the services offered, please visit:
https://www.copadata.com/en/support-services/service-level-agreement/.

3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.

zenon Service Engine, zenon Report Engine
Supplier evaluation is in responsibility of the regulated company.

COPA-DATA is available to assist with both postal and on-site audits to provide evidence that the zenon Software Platform operates in compliance with the applicable regulatory rules and with the reference guidelines for the life-science industries.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

zenon Service Engine, zenon Report Engine
Not applicable.
The products of the zenon Software Platform are configurable, i.e. they are SW category 4 according to GAMP5 guidelines.

3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

zenon Service Engine, zenon Report Engine
Not applicable.
Supplier evaluation is the responsibility of the regulated company.

3.4. [4] Validation

4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

zenon Service Engine, zenon Report Engine
COPA-DATA is available to assist with both postal and on-site audits to provide evidence of the testing activities carried out during system development and testing.

The customer is ultimately responsible for the system validation.

4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

zenon Service Engine, zenon Report Engine
Not applicable.
System validation is the responsibility of the regulated company.

4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

zenon Service Engine, zenon Report Engine
Inventory of critical systems is the responsibility of the regulated company.

In terms of the system description, system manuals are provided with the zenon Software Platform. In addition, zenon offers a documentation tool that provides a hardcopy of the project content and a comparison wizard that can identify differences in projects, highlighting changes and any situations that need verification.
The ultimate responsibility for writing an up-to-date description of the system falls to the system engineer (system integrator and/or regulated company) that configures the zenon project(s).

4.4 User Requirements Specifications should describe the required functions of the computerized system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.

zenon Service Engine, zenon Report Engine
Not applicable
The regulated users are responsible for writing the user requirements of the system and for tracing them throughout the system lifecycle against both the specification documents and the validation tests.

4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

zenon Service Engine, zenon Report Engine
Supplier evaluation is the responsibility of the regulated company.

COPA-DATA software development works according to *SEI CERT Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems* and the OWASP Top 10 standard awareness document for developers and web application security.
According these standards, COPA-DATA operates precisely defined processes and procedures.
COPA-DATA is certified according to IEC 62443-4-1:2018 (Secure Product Development Lifecycle).

COPA-DATA is available to assist with both postal and on-site audits to provide evidence that the zenon Software Platform operates in compliance with the applicable regulatory rules and with the reference guidelines for the life-science industries.

4.6 For the validation of bespoke or customized computerized systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.

zenon Service Engine, zenon Report Engine
Custom software add-ins (GAMP5 SW CAT.5) can be integrated with the zenon Software Platform by the project engineer using a dedicated API (Application Program Interface). The project engineer and the regulated company are responsible for satisfying the compliance requirements relating to this integration.

4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.

zenon Service Engine, zenon Report Engine
The regulated company is responsible for demonstrating the appropriateness of test methods, scenarios and system environments.

4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.

zenon Service Engine, zenon Report Engine
Validation of any data migration is the responsibility of the regulated company with the support, if necessary, of the system integrator.
The zenon Software Platform provides several import and export functions to support data migration.

3.5. [5] Data

Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

zenon Service Engine
The system can be interfaced with third-party industrial systems and networks using a native communication tool. Native communication means that connection to systems and networks is achieved without the need to involve another system, because any possible interface is an integral to the zenon Software Platform.

When evacuating historical data to an external database, there are internal mechanisms that check during the transfer that the data has been correctly and completely transferred. If, for whatever reason, the data hasn't been transferred, the data will be saved in the internal buffer and evacuated as soon as the communication has been re-established.
When using communication drivers to connect with PLCs, each variable has a readable status which shows, for example, whether the value has timed out.

zenon Report Engine
zenon Report Engine can be interfaced with third-party databases in order to read dynamic data that is used to populate reports.

3.6. [6] Accuracy Checks

For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

zenon Service Engine
It is possible to set a predefined range for imputable parameters. If the operator enters data that is outside the defined range, the system won't accept the value and prompts an error message.
Both the graphical aspect of the input window and the system behavior in case of invalid data/operation can be configured using the zenon Editor.
If a second signature (e.g. QA's signature) is required to make a change effective, this can be configured in zenon eSignature function. In the zenon Engineering Studio it's possible to configure a signature workflow requiring 1, 2 or 3 different users. (i.e. User1 performs the change, User2 verifies the change, User3 approves the change). Each user can add an individual comment to his signature manifestation. The users of each step must not be in the same user group.

zenon Report Engine
Not applicable since it is not possible to enter data in zenon Report Engine.

3.7. [7] Data Storage

7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

zenon Service Engine
Data is stored in zenon-specific binary files, which can be secured by the security system of the Windows file system, or in a SQL database or in a MongoDB Data Storage. In all cases, customers should establish policies and procedures to ensure that records are retained for an appropriate retention period.
The location of the data can be specified by the user. Therefore, data can be placed on a secure server with its own protection and security measures.

zenon Report Engine
zenon Report Engine is provided with its own SQL database where report (RDL files) and configuration data are saved. This database contains the procedures used by the system to populate and optimize report generation.
The zenon Report Engine database is protected by means of access control measures.
Dynamic data that is used to populate the reports is not saved in the tool database but is read from the interfaced databases on request.

Exported or saved reports fall under the responsibility of the regulated company since their protection depends on where they are archived.
The location of the data can be specified by the user. Therefore, data can be placed on a secure server with its own protection and security measures.

7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

zenon Service Engine
There are different options for Data Backup. When data is stored locally in binary databases, data can be backed up using a copy functionality that creates a second copy of the data on a predefined shared folder. This function can be scheduled so that it is automatically executed at a predefined time interval, according to the customer's backup SOPs. Data can be restored using the same copy functionality.
Another option is provided, to evacuate Process, Alarm and Event Data instantly to any central database (based on SQL or MongoDB). This data is available to zenon also for backup/restore.

Furthermore backup/restore operations can be performed using standard Hard disk Backup tools for MS Windows or classical functions available on Virtual Machines.
When historical Data are stored on SQL Server or on MongoDB Data Storage, customers should use dedicated backup/restore functions.

zenon Report Engine
zenon Report Engine databases (metadata database, reporting services database and other related databases) can be backed up by a specific function in Reporting Studio. The user can define the scheduling and the shared destination folder. Databases can also be restored using a specific function in Reporting Studio.

3.8. [8] Printouts

8.1 It should be possible to obtain clear printed copies of electronically stored data.

zenon Service Engine
Data in zenon is saved in its own proprietary file formats or in an SQL database. The individual data can be accessed in many ways:

- zenon has reporting capabilities that can provide combined or individual documents for audit trail, alarm lists, historical and online values. The data is provided as a screen report, hardcopy, or in electronic .PDF format, enabling the reading and archiving of the data.
- zenon integrated tools include: audit trail, alarm management and archive revision screens for reading, listing and commenting. Data can be stored in the proprietary formats and accessed via the zenon tools afterwards.
- Data can be exported into different formats (dBase, ASCII/CSV, XML, SQL) and then displayed and archived in external systems.
- Historical data and Alarm & Event data can be stored in a relational SQL database or MongoDB Data Storage. External programs can access data there via authorized access.

Specific reports can be configured using the Report Viewer, which generates reports when manually requested by a user; automatically on process events such as "batch complete"; on a timed basis; or when instructed by an external system, such as the ERP or MES.

zenon Report Engine
zenon Report Engine is used to design and generate reports to visualize, print and export data acquired by zenon Service Engine. It can access data from any linked database, even third-party databases. Reports can be exported in .PDF, .XML, .CSV, Word, Excel, PowerPoint, .MHTML formats. Reports can be sent by email or stored in a central file share.

8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.

If a report is used to support batch releasing, it is the responsibility of the report designer to properly configure the report in order to indicate whether any of the data has been changed since the original entry. All data and events are registered by the audit trail which shows the evolution of all data.

3.9. [9] Audit Trails

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

zenon Service Engine

All events managed through the user interface (i.e. in the Service Engine) can be included in the audit trail. The fields that are recorded in the audit trail can be configured at project level (i.e. in the zenon Engineering Studio).

The audit trail records: time-stamp (date & time of the event), variable name, user name, inserted and modified values (in this case, the audit trail should register both the old value and the new one).

In addition, it is possible to configure the audit trail to display further information, such as: variable identification, full user name, computer or system name, project/application name, variable status, alarm text, alarm area and alarm class, etc. Users can add comments about all the information captured. Furthermore, automated events and system events can be recorded in the audit trail.

zenon has a built-in clock synchronization with the (server) operating system date and time to ensure that all date and time stamps are accurately recorded in the audit trail. It is the responsibility of the Customer to synchronize the operating system date and time with a reference one and to inhibit the change of date, time and time zone.

The audit trail is automatically recorded and maintained as a binary file in a specific folder or in SQL Server or MongoDB data storage. This data can be accessed, filtered and queried by users through the user interface; both the audit trail of the entire project and a view of the audit trail for any relevant field can be displayed.

The audit trail can be exported in several formats (i.e. CSV, XML, SQL, etc.) and printed in .PDF and paper format. The customer is responsible for activating the audit trail and configuring backup for it.

zenon Report Engine

The audit trail is not applicable to zenon Report Engine since, while end users can launch a report, they cannot modify any data contained within it. If the audit trail recorded by zenon Service Engine is included in a report created with zenon Report Engine, it is responsibility of the report designer to properly configure the report in order to include all the required audit trail information (i.e. user name of the operator, date and time of the operation, value before and after the change).

3.10. [10] Change and Configuration Management

Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

The regulated company owns the ultimate responsibility for managing change in a controlled manner. However, zenon provides several tools to assist with change control and configuration management processes.

zenon Service Engine
zenon offers a documentation tool able to provide a hardcopy of the project content as well as a comparison wizard able to identify differences in projects, highlighting the changes and the situations that require verification.

zenon Service Engine includes a "history of changes" functionality that tracks all modifications to the configuration of zenon projects. This information is available to support the configuration management process.

zenon Report Engine
In order to support the configuration management process, it is suggested users manage report template versioning manually, adding a version number and an explanatory comment (e.g. in the Report Launcher comments and in the Reporting Studio comment fields) when there is a change to the report template.

3.11. [11] Periodic Evaluation

Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

The regulated company is ultimately responsible for carrying out periodic evaluation of the computerized systems. zenon Service Engine can support periodic review by providing information by means of system variables about system performances, e.g. free disk space, RAM utilization, system temperature, network communication errors, etc. This information can be displayed, archived or exported. zenon Service Engine can also act as an SNMP agent to provide information to an IT monitoring system.

3.12. [12] Security

12.1 Physical and/or logical controls should be in place to restrict access to computerized system to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

zenon Service Engine

Access to both, zenon Engineering Studio and zenon Service Engine is limited only to authorized users who have active credentials (username and password).

zenon has local internal User Administration features and supports the use of Active Directory accounts. Both systems can be used concurrently.

Biometric and external security identification devices that bear or generate identification codes or password information can be accommodated. They can be activated upon request.

The system detects failed login attempts using incorrect passwords or ID and locks out the user after a certain (configurable) number of attempts. All successful and unsuccessful login attempts are recorded.

zenon also offers password aging, length, complexity and history functionalities.

Each zenon project should utilize the automatic user logout function which logs out a user after a defined period of time.

In order to prevent concurrent access to the same record in client-server architectures, it is possible to set an option that allows only one person to access the record at a time.
When accessing the system remotely, specific functionality is available to allow only one person to access the system at a time, and protocols are in place to request access and log out other users.

The customer must have procedures in place to define who is authorized to access the system and at which access level. Moreover, the customer's procedures should be in place at the operating system level to restrict user access across the PC operating system.

zenon Report Engine

Access to zenon Report Engine is limited only to authorized users, i.e. users that have been enabled by the Administrator to access the Report Launcher.
Users/user groups can be given access right to one or more folders that contain report(s).
In addition, different user roles with different privileges can be configured, e.g. an administrator can delete/rename report templates while standard users can only run reports.
zenon Report Engine can use both Windows local accounts and Active Directory accounts.

Only administrators can access the SQL database using the standard login functionality of the database itself.

12.2 The extent of security controls depends on the criticality of the computerized system.

The evaluation of system criticality is the responsibility of the regulated company. As a consequence, the customer is responsible for defining which users have access to the system and with what privileges.

12.3 Creation, change, and cancellation of access authorizations should be recorded.

Management of the user accounts is the responsibility of the customer according to its SOPs.
However, the system supports this process since all user information that is changed in the Runtime is recorded in the audit trail and permanently saved in zenon.
When the "History of changes" option is enabled in the Editor project design environment, user additions or changes will also be recorded.

12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

zenon Service Engine
All events managed through the user interface (i.e. in the Service Engine) can be included in the audit trail. The fields that are recorded in the audit trail can be configured at project level (i.e. in the zenon Engineering Studio).

The audit trail records: timestamp (date and time of the event), variable name, user name, inserted and modified values (in this case, the audit trail should register both the old value

and the new one). In addition, it is possible to configure the audit trail to display further information, such as: variable identification, full user name, computer or system name, project/application name, variable status, alarm text, alarm area and alarm class, etc.

zenon Report Engine

The audit trail is not applicable to zenon Report Engine since, while end users can launch a report, they cannot modify the data contained within it.

3.13. [13] Incident Management

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

Management of incidents and related CAPA is the responsibility of the customer.

zenon Service Engine

The system supports this process since all system, user and process events are recorded in the audit trail. Details about the event include timestamp, variable name, value and unit, description text, computer name, user identification, full username, and a comment on the event. This provides a detailed view of the incident and the progression of events on the Runtime system.

The zenon Process Recorder module can be used to collect critical process parameters and all relevant process data. The process history can be further replayed in a normal zenon client operating in replay mode. From this client it is possible to observe the process screens from a specific time in the past and move backward and forward step by step.
The zenon Process Recorder is a useful tool to support incident analysis.

zenon Service Engine can also provide information about system performances, e.g. free disk space, RAM utilization, system temperature, network communication errors, etc. by means of system variables. This information can be displayed, archived or exported.
zenon Service Engine can act also as an SNMP agent to provide information to an IT monitoring system.

zenon Report Engine

All the information collected by zenon Service Engine can be used by zenon Report Engine to generate specific diagnostic reports. These reports can be generated manually or automatically on specific events and sent to a specific user by email.

3.14. [14] Electronic Signature

Electronic records may be signed electronically. Electronic signatures are expected to:

a. have the same impact as hand-written signatures within the boundaries of the company,

b. be permanently linked to their respective record,

c. include the time and date that they were applied.

zenon Service Engine
Electronic signatures can be enabled for each project field and button, for example for modifying a GxP critical recipe parameter, for the steps of the recipe approval workflow or for executing a lot.

Each signature record consists of the full name of the user, of the date and time of the signature and of the meaning of signature (e.g. value change, verification of value change, recipe approval, etc.). All this information can be visualized when the signed record is visualized on the HMI and on the generated paper or .PDF report.

Electronic signatures are linked to the signed records and it is not possible to alter or falsify an executed signature.

Electronic signatures are stored in the same binary database of the audit trail records, hence they are subject to the same controls described above, i.e. they are in proprietary binary format therefore individual modifications are not possible external to the zenon system. Furthermore, audit trail records can be also stored in an SQL Database or MongoDB Data Storage.
Customers should also establish policies and procedures to prevent unauthorized access to signature records (AML, CEL), which can be done with the security system of the Windows file system in the case of binary databases or by controlling access to SQL Database or MongoDB Data Storage when selecting an external storage location. Furthermore, customers should ensure the necessary backups are in place and active.

zenon Report Engine
zenon Report Engine is not provided with electronic signature functionality.

In case it is necessary to satisfy the signature manifestation requirements for a record signed in zenon Service Engine or in any other interfaced system, it is the responsibility of the report designer to properly configure the report in order to include all the required signature information (i.e. the printed name of the signer; the date and time when the signature was executed; the meaning associated with the signature).

3.15. [15] Batch Release

When a computerized system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

zenon Service Engine, zenon Report Engine
Not applicable

3.16. [16] Business Continuity

For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

Business continuity and disaster recovery measures are the responsibility of the regulated company.

zenon Service Engine
zenon Service Engine can be configured as a redundant system, utilizing two servers to provide high availability of the system and to protect against data loss.

zenon Report Engine
zenon Report Engine does not support redundant configuration as it does not store process data.

zenon Report Engine can be recovered via backup files generated using specific functions in Reporting Studio.

3.17. [17] Archiving

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

zenon Service Engine
Using integral zenon functionality, it is possible to use an external database as the historian storage (SQL Server or MongoDB Data Storage). Historical Data includes Time series, Alarm history and Audit Trail records. Historical data from the zenon historian can be copied and exported to a database with ODBC connection (e.g. SQL or Oracle), a comma delimited text file, and .XML. In the first option, the database can be read using zenon tools; for the latter options, the exported data can be read by third-party solutions. After the successful completion of the copy/export process, the online data can be deleted.

zenon Report Engine
Not applicable because it does not store data.