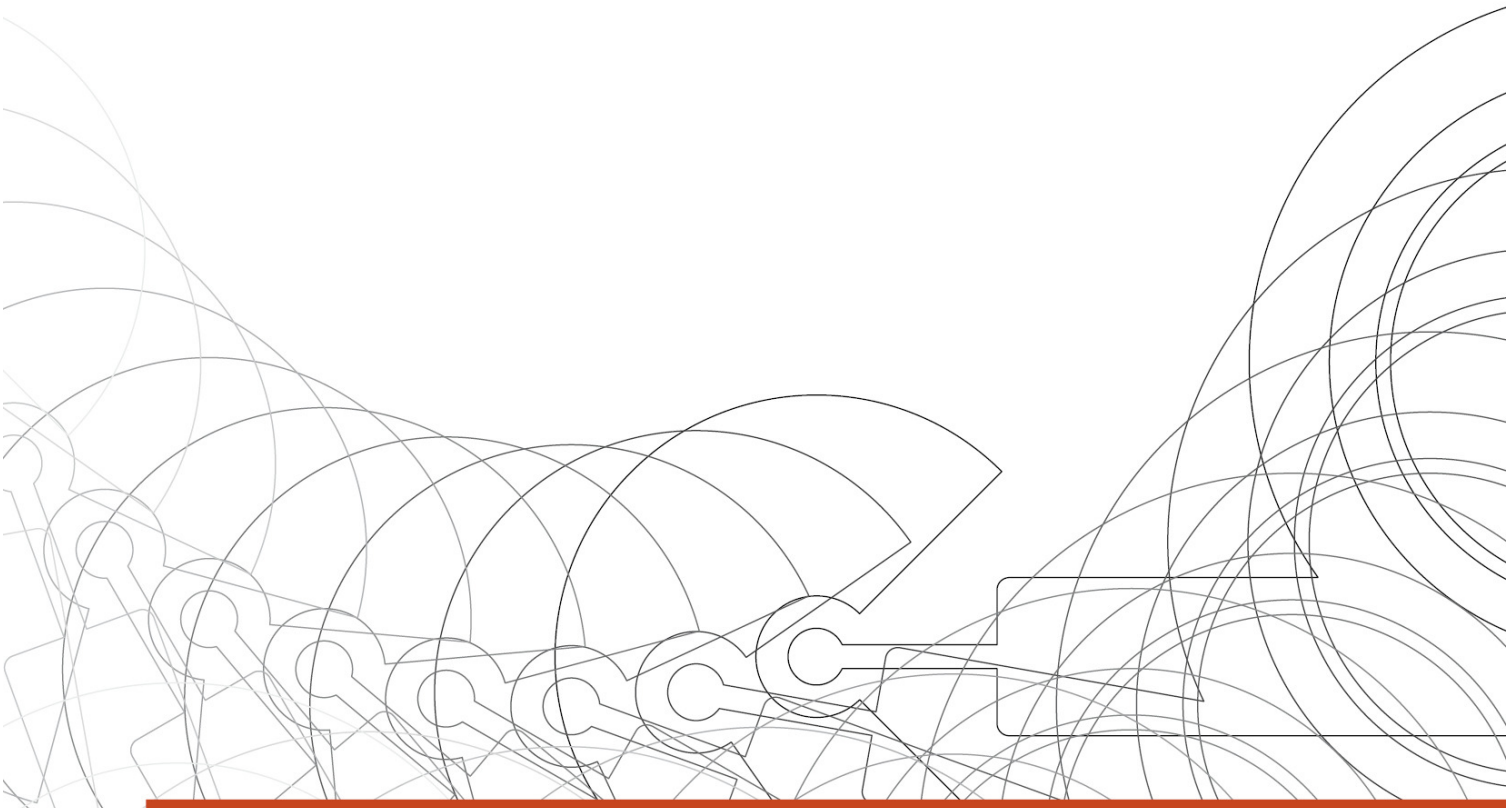
COPA-DATA
do it your way



COPA-DATA Know How: zenon & GAMP 5

Contents

Contents **2**
History **3**
Introduction **4**
When did the GAMP come in to force? 4
GAMP 4 to GAMP 5 Evolution 4
ISPE International Society for Pharmaceutical Engineering 5
GAMP applies to whom? 5
FDA & GAMP comparison 5
Supplier leverage and good practice **6**
Leverage supplier input 6
Supplier good practices 6
GAMP Appendices **8**
Backup & Restore - appendix O9 8
Security Management – appendix O11 8
Archiving & Retrieval – appendix O13 9
Electronic Production Records – appendix S2 9
Patch & Update management – appendix S4 9
Performance monitoring – appendix O3 10
Supplier quality and Project planning – appendix M6 10
Project change and Configuration management – appendix M8 11
Supplier Assessment – Appendix M2 12
GAMP 5 & zenon **14**

History

Date	Comment
22.09.2009	Robert Harrison, original author
23.08.2010	Robert Harrison, Review document

Introduction

The GAMP guidelines relate to the Regulated company and their good manufacturing practices, the responsibility for full compliance of relevant standards ultimately stops there. In GAMP 5 however greater importance has been placed on Supplier Leverage, that is the supplier of a product or service should be aware of the guidelines and adhere to them, this has the effect that Regulated companies can use the suppliers documentation, testing, verification, and quality plan, to prove compliance to regulation authorities. This puts more responsibility to the supplier, and reduces the amount of duplication the Regulated company needs to carry in order to have a compliant system to the required standards.

The key driver behind the evolution of the GAMP guidelines from GAMP 4 to GAMP 5 is to focus attention on patient safety, product quality and data integrity, through categorizing computer systems by risk, novelty & complexity. There is a need to avoid duplication by integrating engineering activities with computer system activities, and to leverage supplier activities whilst ensuring fitness for intended use. The aim is not to restrict but to aid innovation.

When did the GAMP come in to force?

Activity to gain more understanding of healthcare automated manufacturing started in the late 80's and early 90's, when greater validation of the pharmaceutical industries was becoming necessary as automated systems played a greater role in healthcare production.

The first GAMP guidelines were put into action in March 1994. January 2008 being the latest release of the GAMP 5 guidelines.

GAMP 4 to GAMP 5 Evolution

The GAMP guide has been updated to keep up with concepts and regulatory & industry developments.

- Avoid duplication of activities, fully integrate engineering and computer system activities so that they are only performed once.
- Leverage supplier activities to the maximum possible extent, while still ensuring fitness for intended use.
- Scale all life cycle activities and associated documentation according to risk, complexity, and novelty; e.g. If the system uses non-configured off the shelf software, complexity, novelty and risk is therefore low. If the system uses programmed software designed specifically for the application, the novelty, complexity and risk is high.

ISPE International Society for Pharmaceutical Engineering

Founded in 1980, the International Society for Pharmaceutical Engineering (ISPE) is a global not-for-profit industry trade group for pharmaceutical science and manufacturing professionals, and has 25,000 members in more than 90 countries.

ISPE aims to be the catalyst for pharmaceutical innovation by providing pharmaceutical industry professionals with opportunities to develop technical knowledge, exchange practical experience, and collaborate with global regulatory agencies and industry leaders. ISPE has worldwide headquarters in Tampa, Florida, USA; its European office in Brussels, Belgium; and its Asia Pacific office in Singapore.

ISPE offers access to industry-standard technical documents, peer-reviewed publications, industry and regulatory resources, relevant continuing education and training, and the first competency-based international certification for pharmaceutical professionals. And is the drive behind the GAMP guides.

GAMP applies to whom?

Healthcare industries who produce pharmaceutical, biotechnology & medical devices fall under the embrace of the GAMP guidelines.

The ISPE is an international organization, the GAMP documents are a guide to progress good manufacturing practices world wide. Because the GAMP guidelines are not a standard a company cannot be Certified, Compliant or Approved.

FDA & GAMP comparison

GAMP focuses on the whole system and the end product, where as the FDA focuses on each process and stage of production that contributes to the end product. FDA guidances are incorporated into the GAMP guidelines.

As the GAMP 5 guidelines have "Automated" built into the name and their philosophy—they envision process and system (computer) validation as integrated entities. An automated process is tested as an installation, operational, and performance qualification to be certain that the automated procedure has been properly installed, tested, and used. By contrast, the FDA's cGMP document assumes a manual process with reference to the reality of automated process systems through the separate document 21 *CFR* Part 11, which defines system validation and provides guidelines for it. The GAMP stresses bottom-line performance, while the FDA stresses the process itself (procedurally and with automation). Under GAMP 5, an investigator would validate the results of an automated analysis system as a functioning analytical unit. Under cGMP, an investigator would validate the analytical process of each step of the process.

Similarly, the GAMP focuses on quality assurance (QA). While still emphasizing QA, the FDA approach puts equal weight on the quality control (QC) process, including all aspects of production and operation as well as the final QA overview.

The result is, the FDA has a greater reliance on analysis at all phases, where GAMP has reliance on the final result rather than the interim steps that lead to that result. In short, process understanding (FDA) versus process outcome (GAMP).

Supplier leverage and good practice

Leverage supplier input

Supplier documentation and testing documentation may be used as a part of the supplier verification.

The regulated company assess the supplier for: acceptable quality system, technical capability, application of good practices, and that information from the supplier is accurate.

Supplier documentation is assessed for content & quality. The regulated company is flexible to accept supplier documentation & structure, i.e. the supplier doesn't have to use the regulated companies documents and structure. If inadequacies are found the regulated company can target additional verification, rather than repeating supplier activities.

Supplier good practices

Step	Practice	Description
1	Establish QMS	The supplier QMS should: 1. Provide a documented set of procedures and standards 2. Ensure activities are performed by suitably competent and trained staff 3. Provide evidence of compliance with the documented procedures and standards 4. Enable and promote continuous improvement
2	Establish Requirements	The supplier should ensure that clear requirements are defined or provided by the regulated company.
3	Quality Planning	The supplier should define how their QMS will be implemented for a particular product, application, or service.
4	Assessments of Sub-	Suppliers should formally assess their sub-suppliers as part of

	Suppliers	the process of selection and quality planning.
5	Produce Specifications	The supplier should specify the system to meet the define requirements.
6	Perform Design Review	The design of the system should be formally reviewed against requirements, standards, and identified risks to ensure that the system will meet its intended purpose and that adequate controls are established to manage the risks.
7	Software Production / Configuration	Software should be developed in accordance with defined standards, including the use of code review processes. Configuration should follow any pre-defined rules or recommendations and should be documented.
8	Perform Testing	The supplier should test the system in accordance with approved test plans and test specifications.
9	Commercial Release of the System	System release to customers should be performed in accordance with a formal process. (Note: this is not a release into GxP environment, which is a regulated company activity)
10	Provide User Documentation and Training	The supplier should provide adequate system management documentation, operational documentation, and training in accordance with agreed contracts.
11	Support and Maintain the System in Operation	The supplier should support and maintain the system in accordance with agreed contracts. The process for managing and documenting system changes should be fully described.
12	System Replacement and Retirement	The supplier should manage the replacement or withdrawal of products in accordance with a documented process and plan. The supplier also may support the regulated company with the retirement of computerized systems in accordance with regulated company procedures.

GAMP Appendices

The following paragraphs contain experts from the GAMP 5 Appendices, and summarizes their content. For further concise information please reference the GAMP 5 guidelines.

Backup & Restore - appendix O9

The backup and restore should be a well define company procedure. Procedures should exist for regular testing of Backup & Restore operations, which should be documented.

The backup and restore procedure must: ensure the backup operation is to a secure location, ensure integrity of the storage facility, ensure correct recovery to the on-line equipment, and ensure that all activities are logged. Full and incremental backup operations are possible.

The procedure should include: user authorization, full and incremental backup and restore operations, frequency of the backup, location of the stored data, test procedure, which software to backup or restore. Backup & Restore instructions should be securely stored with the backup data.

The latest operating system or software should be able to be restored. All software components required for operation should be included in the backup i.e. operating system, layered software, application software, configuration data; to ensure the full system can be restored.

Once the system is in operation is should be backed up after software modification, and at regular intervals. At least two generations should be kept.

A full backup operation should be performed before a restore operation is carried out. The restore operation must included a procedure to resynchronize with interdependent systems.

Security Management – appendix O11

The system must ensure against wilful or accidental loss, damage or unauthorized change; and maintain confidentiality, integrity, viability of regulated systems, records, and processes.

Ensure a list of authorized persons is established and maintained, and that appropriate levels of security are managed.

Persons should be made aware that their activities are monitored, and education is supplied to ensure security is maintained.

The security system policy ensures physical security of the system and stored data, access is by user ID & password, with all access activity being recorded.

Archiving & Retrieval – appendix O13

It must be possible to take records off-line and move them to a different location, to protect against further changes and deletion, and secure against wilful or accidental damage by physical or electronic means.

The application(s) that support the archived data should also be archived. Consider also the operating system and hardware needed to access the records.

Stored records should be checked initially after archiving, and periodically for accessibility, durability, accuracy and completeness. Human readable copies of data must be made available, and electronic signatures must be preserved.

All activity is logged and user authorization is required.

Electronic Production Records – appendix S2

Electronic records must provide a high level of assurance that the product has been produced according to its specification. Common type of record include, Electronic Device History Record (EDHR), Electronic Batch record (EBR).

Review by exception (RBE) records data to report on critical process exception, and filter production data for limit violations. Communication errors that prevent a critical process being reported must be included in the RBE. When no critical errors occur, the RBE indicates the operation completed without error.

Exception reports should include sufficient contextual information to allow for retrieval of associated data.

The GAMP approach is: processes are maintained within defined tolerances, data & events are recorded; process data is monitored at appropriate intervals, alerts and alarms are generated when tolerances are exceeded. Electronic records are trustworthy, accurate and secure.

Patch & Update management – appendix S4

Regulated companies should provide criteria for determining threat levels (security & critical process defects), and thus the urgency for applying patches.

First determine what effect applying or not applying the patch or upgrade will have on the compliant system. Configuration records must be kept that show the version and patch level for the system. With change records describing what level of testing was completed.

Performance monitoring – appendix O3

Performance monitoring is a part of overall preventive maintenance, and uses performance data in diagnosing problems. Trends that indicate performance problems are used as a part of corrective and preventive actions (CAPA) to reduce down time.

Example parameters include:

Servers / workstations / Control systems: CPU utilization, Cache utilization, response time, disk capacity, hardware status, alarms.

Network: Availability of components, network load, broadcasts.

Applications: Error messages, response times, availability to users.

Notification: Console message, Audible & Visual, Email to system operator, SMS or Pager alerts, logging of alerts.

This list is a broad example of the conditions that could be monitored. Please refer to the guidelines for further information.

Supplier quality and Project planning – appendix M6

The Quality and Project Plan defines how the supplier will fulfil the quality requirements of the project, and how the Quality Management System (QMS) will be applied.

Quality plan:
Introduction

- Who produced the document, under which authority, and for what purpose
- Contractual status of the document
- Relevant policies, procedures, standards & guidelines
- Relationship and reference to other documents, e.g. verification plan

Overview

- The project and technologies used should be described

Quality plan

- Quality related verification activities
- Responsibilities
- Procedures to be followed

User quality requirements

- Take precedent over supplier QMS
- Relevant company requirements

Supplier quality system

- How the regulated company quality requirements will be met

- Which quality activities will be handled under the supplier QMS, and which under the customer QMS
- The activities to be carried out, the procedures to be followed, and the responsibilities should be defined.

Project Plan
Project organization
- The supplier project team, showing personnel and job title
- Supplier contact for complaints etc.
- The interface between the supplier project team and the supplier quality assurance
- Nominated customer contacts

Deliverable items
- Definition of the deliverables and their identification

Activities
- Project milestones, identifiable project events
- Project activities, design reviews, verification
- Personnel allocated to activities
- Planned start and end date of each activity

Additional information
- Who produces, reviews, and approves the specification of the interfaces
- Who produces, reviews, and approves the test specification
- Is a simulator necessary for the interfaces, if so who designs it
- Who is responsible for testing the interface, FAT & SAT (Factory Acceptance Test, Site Acceptance Test)
- Who is responsible for designing and providing test data
- Who produces, reviews, and approves any test reports associated with the interface

Project change and Configuration management – appendix M8

Any controlled item that undergoes review, approval, or test should be governed by appropriate configuration and change management. Change management should be applied after the first formal approval, to avoid unintentional change.

All components of a computerized system and the changes to them should be controlled. The exact hardware and software configuration should be documented throughout the life of the system.

Responsibilities, procedure and schedules should be clearly defined; and all activities should be documented.

Key change management steps

Raising a change	Each change is uniquely identified
Change review	Decision to accept or reject clearly defined Scope of change Impact of change What verification is required The associated risk
Change completion	The change has been implemented, documented, verified, and approval by the project manager.

Supplier Assessment – Appendix M2

Regulated companies require a high level of confidence that computerized systems will meet their technical, commercial, and regulatory requirements. Knowledge, experience, and documentation must be leveraged from the supplier.

Regulated companies require documented evidence of quality and reliability that the computerized systems will consistently perform as intended.

Quality and integrity must be built into the software by the supplier as it cannot easily be added later. The supplier is best placed to document the required evidence during development.

The assessment process should provide a balanced view of the supplier, including positive observations and a list of concerns.

There are three main categories of assessment:

1) Basic assessment using available information. Appropriate for common desktop applications.
   A review of public domain documentation.
   Market reputation.
   Knowledge and experience of prior performance.
   Discussion with other regulated companies.

2) Postal audit, using a questionnaire. Appropriate for standard and configurable products.
   Provides a good understanding of the suppliers systems.
   Indicates how the management of quality is carried out.
   Problems can be solved by providing more information and supporting documentation.
   Use a preliminary audit to reduce time at the suppliers premises.

3) On-site audit, using a relevant expert, auditor, or audit team.

Postal audit questionnaire

- Company overview, locations
- Organization, roles, responsibilities, training, experience
- Key products and services
- QMS implementation at the company level
- Product/project management
- Software development life cycle
- Service delivery processes
- User training
- Product support & maintenance
- Security
- Sub-contractor usage

Supporting evidence will be requested, including real example and work performed.

Example audit requirements

- Test strategies at each stage of development
- Evidence of structural and functional testing
- Evidence that each key function of the product has been tested, and prove traceability
- Evidence of stress testing, and testing in abnormal conditions
- The use of testing tools
- Documentation standards employed, test results, raw test data, traceability on specification life cycle, review of test results, actions taken in the event of failure.
- Supplier quality assurance function in the testing process
- The independence and qualifications of testers and reviewers
- Verification that traceability from requirements through to testing is available and adequately documented

On-site auditing

1) Opening meeting.
   Formal introductions.
   Summarize the purpose and scope of the audit. The supplier may add suggestions and preferences.
2) Review and inspection.
3) Closing meeting.
   Supplier response to the findings.
   Agree on comments.
   A formal report is issue to the management of the regulated company.
   Required corrective actions determined & further audits.

All of the above will be documented in the audit report. A draft audit may be produced to allow the supplier to comment before submission to the regulated company management. The reports should not contain any significant issues not discussed during the audit or in the closing meeting.

GAMP 5 & zenon

Software must be produced in accordance with a system of quality assurance.	COPA-DATA has a system of quality assurance, where specifications, defects, tests, and test results are managed end to end for all software development. Customers must validate their applications, they may develop and/or execute the validation plans and protocols themselves or outsource these activities.
The system should include built-in checks of the correct entry and processing of data.	This is covered in many ways depending on the check necessary. User authorization, limits on a value can be placed, automatic reactions can be implemented, rechecking of data by a different person before processing can be designed in to a system. Data input can be restricted to defined stations, the station on which an action is executed can be protocolled. zenon client/server architecture restricts data storage to the server computer only, ensuring that the audit trail is generated from a single location. All audit trail records (AML and CEL) include date and time stamp, node of origination, and operator name.
Data should only be entered or amended by persons authorized to do so.	User authorization requires ID & Password, external systems can also be used to logon a user, from a biometric system for example. Account policies can be implemented in zenon with password aging, minimum password length, and account & system lockout after a reasonable number of unsuccessful login attempts. Internal zenon security should be used to limit user access to authorized security areas and applications. Data input can be restricted to defined stations. The station on which an action is executed can be protocolled. zenon client/server architecture restricts data storage to the server computer only, ensuring that the audit trail is generated

	from a single location.
The system should record the identity of operators entering or confirming critical data. Entering or amending critical data should be authorized and record the reason for the change.	The 'Audit trail' is achieved through the CEL, which records the identity of the person, the data being changed, and possibilities for entering the reason or comment is designed into the system. All zenon audit trail records (AML and CEL) include date and time stamp, node of origination, and operator name.
It should be possible to obtain clear printed copies of electronically stored data	All data in zenon are saved in their own proprietary file formats. There are four different ways to access to the data: Integrated tools of zenon such as: Report Generator, Report Server, Alarm and CEL administration. Data can be exported into different formats (dBase, ASCII/CSV, XML) and then be processed in external programs. Data can directly be stored in a SQL database, where external programs can then access data. Data can be printed in PDF format and then be archived.
Data should be secured by physical or electronic means against wilful or accidental damage.	Storage of the data (Archive or backup) can be local or anywhere on the connected network. The protection of data then falls under the site system/network administrator. Data are stored in zenon specific binary files, therefore modification by an external system is not possible. The data can be further secured by the security system of the Windows file system. Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time.
Data should be protected by backing-up at regular intervals.	The run time data of zenon is available to the system administrator, therefore external means of backing-up data can be put in place. Storage of the data (Archive or backup) can

	be anywhere on the connected network. The protection of data then falls under the site system/network administrator. Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time.
There should be adequate alternative arrangements for systems which need to be operated in the event of a breakdown, information required to effect recall must be available at short notice.	zenon & straton are both fully redundant systems, in both the client and server configuration.
A procedure should be established to record and analyze errors and to enable corrective action to be taken.	Reports can be generated to produce exception reports (RBE) through alarm & warnings. All data is available for later review, either by the use of zenon tools (IPA, IMM, Trending, SPC). Additionally data can be exported to external systems.
When the release of batches is carried out, the system should allow only a qualified person to release the batch.	Authorization levels can be placed on all manual actions. zenon can implement User Administration to set authorization levels and control, Windows Active Directory can be also utilized for central access control. All operations are subject to an audit trail recording. Account policies should implement password aging, minimum password length, and account & system lockout after a reasonable number of unsuccessful login attempts. Data input can be restricted to defined stations. The station on which an action is executed can be protocolled. zenon client/server architecture restricts data storage to the server computer only, ensuring that the audit trail is generated from a single location. It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task. The 'Audit trail' is achieved through the CEL, which records the identity of the person, the data being changed and possibilities for

	entering the reason or comment is designed into the system.
Understanding Critical Quality Attributes (CQA), and facilitate Quality By Design (QBD), ensure quality is built into a system. Identify opportunities for process & system improvements, continuous improvements, root cause analysis, corrective and preventive actions.	COPA-DATA has a well established quality assurance management system in place as a policy of continuous improvement. From concept of an idea or defect, the evolution through development and testing is fully documented.
Persons developing software have the required training, education & experience.	COPA-DATA employees have the required qualifications and experience for software development and project management. The specifications for development activities and projects are created by experienced persons. A system of quality assurance is in place to track a projects life cycle evolution. Customer training is advised to be carried when a new customer or user is established. Continuance training is available to refresh or advance the knowledge, via specific customer training or consultancy. It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task.
Evaluate effectiveness of training, maintain records, and ensure training is maintained.	Feedback on the training is requested from all students, continued connection with the customer is actively sought to maintain their needs. No training records are kept by COPA-DATA, this is the responsibility of the regulated company. It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task.
Persons should be made aware of the relevance and importance of their activities.	COPA-DATA has a dedicated manager responsible for communicating pharmaceutical related activities to its internal personnel.
Backups should be performed at regular intervals, to include: operating system,	The location of data created and used by our products is configurable by the end user, and

software, records & data. Each backup should be documented.	so provision can be made in the global system administration to perform backup operations and their documentation.
Restore	All zenon files are open, and can be accessed from the operating system. Customers are therefore responsible to establish policies and procedures to enable a system to restored and synchronized. The procedure of the regulated company should enforce a backup operation to be carried before a restore operation.
Testing	All zenon files are open, and can be accessed from the operating system. Customers can therefore restore a configuration to a test (offline) system. zenon has a simulation mode to enable test operations.
Protect against wilful or accidental loss, damage, or unauthorized change.	User authorization requires ID & Password, external systems can also be used to logon a user, from a biometric system for example. It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task. The 'Audit trail' is achieved through the CEL, which records the identity of the person, the data being changed, and possibilities for entering the reason or comment is designed into the system.
System access by User ID & Password	Zenon implements user administration with user ID & Password, external security system interfaces such as Biometric Identification can be utilized if they are designed so that they cannot be used by anyone other than the genuine owner. All access activities are recorded in the CEL. Account policies should implement password aging, minimum password length, and account & system lockout after a reasonable number of unsuccessful login attempts. Internal zenon security should be used to

	limit user access to authorized security areas and applications. Authorization levels are set on dynamic elements, and authorization levels are given under User administration. Windows Active Directory security and the zenon internal security do not permit the creation of duplicate user ID's. Customers using zenon applications in regulated environments must be responsible for ensuring that electronic signatures are unique to one individual and not reused by or reassigned to any other individual. Users must not be deleted from a system, even on leaving the organization. Customers using zenon applications in regulated environments must be responsible for verifying the identities of individuals using electronic signatures.
Archiving	The location of data created and used by our products is configurable by the end user, and so provision can be made in the global system administration to perform archiving operations. Zenon provides archiving capabilities for production data, where records can be taken off line and stored elsewhere. All content is preserved, and can be retrieved to its original form. Archive location can be located on a remote server.
Retrieval	Access can be made to the archived data and configuration. Reports can be generated from the archived data.
Production records	Zenon's local reporting tool allows for full reporting of a system, for both on-line (running) or off-line (backed up or archived) operation. Specific reports can be generated, to create batch records, critical process exceptions, review by exception, etc. All reports can be tailored to suit your means from the

	recorded data.
Patch & Update management	Supporting documentation is supplied with all new product releases or updates, which outlines what changes have been made or added. All software releases are tested on the supported operating systems.
Performance monitoring	Zenon has a SNMP client and server drivers to relay runtime information of the system, and so preventative actions can be taken before critical processes are affected.
Notification	Zenon has the possibility to send alerts and received acknowledgements via email, SMS, telephone voice messaging, together with traditional methods of console screen alerts & flags.
Testing	Out software is tested to ISO 9001: 2000 and using V-Model techniques. Testing is an integral part of our QMS, and is traceable to the original specification, or defect report. All software releases are tested on the supported operating systems.
Supplier quality & Project planning	COPA-DATA has a well established quality assurance management system in place as a policy of continuous improvement. From concept of an idea or defect, the evolution through development and testing is fully documented.
Project change and configuration management	COPA-DATA has a well established quality assurance management system in place, where all changes can be traced from conception to the finished product. Function specifications, quality review documents, test specifications & test results, and manuals/help are created for all modifications. All new revisions and service packs come with detailed descriptions of the changes and new additions that have been achieved in this installation. It is the responsibility of the customer to

	ensure that revision and change control procedures are in place to maintain an audit trail that documents time-sequenced development and modification of system documentation.
Supplier assessment	COPA-DATA has a history of successful assessment from a variety of customers. Basic assessments, Postal audits, and On-site audits can be completed at a customer's request . A quality management system is in placed at the COPA-DATA head quarters & its regional offices, to ensure that quality and integrity are integrated into our design from the outset of ideas