International Organization for Standardization
Web: www.iso.org

International Accreditation Forum
Web : www.iaf.nu

Edition 1
2020-09-21

ISO 9001 Auditing Practices Group Guidance on:

Auditing Digital Processes

Contents

1. Introduction

An audit is defined as a "systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled" (see ISO 9000:2015).

Audit criteria are "the set of policies, procedures or *requirements* used as a reference against which *objective evidence* is compared" (ISO 9000:2015).

When thinking about the process of collecting objective and verifiable evidence in the audit process, what often comes to mind are the interviews, the observations of persons acting within facilities, infrastructure, equipment, activities, the analysis of records and documents, the comparison of different sources of information and visit to the facilities to observe the processes.

In the case of ISO 9001:2015 we usually conduct the audit along processes, looking at inputs and outputs, sequences and interactions, methods, criteria, monitoring, resources, responsibilities and authorities, risks and opportunities, evaluation and improvement.

What happens when the processes are intrinsic to the equipment, embedded in the software or hidden behind automated processes? A typical audit approach may give us a limited view and capability to assess conformity to requirements. Actually most items, such as inputs and outputs, sequences and interactions, methods, criteria, monitoring, resources, responsibilities and authorities are pre-determined. Our classical approach is to interact with people and objects. In a digital environment we need to deal more with software and hardware.

When processes are automated, embedded in software and hardware, executed without apparent human intervention, then our auditing process is presented with a challenge. The first challenge is to understand the virtual environment where digital and traditional processes interact. In a digital world an increasing amount of processes, especially quality relevant processes, are carried out in automated or even autonomous systems.

Large energy generation plants, massive distribution companies involving numerous sites and assets, and extensive networks of pipelines are all examples of operations that are huge in size and amazingly small in manpower. Behind that scenario, you find that most of the processes run under the scrutiny and monitoring of digital devices, which are the equipment in which the programs are running, and data are being processed and analyzed, utilizing formulas and algorithms. You, as an auditor, are presented with a virtual environment where a digital asset is processing data, making decisions and perform actions based on a program.

Our audit activities should recognize the challenges that such virtual environments and processes pose to the audit process. Automated re-stocking process involve warehouse and purchasing, a control room in a production process makes operational decisions on its own based on inputs and programming of sensors and equipment. These and many other processes were once run with pencil, paper, remission notes, phone calls, expertise, and data extracted from material reception or shipping records. Now, these processes are run without that amount of human intervention and it is a program based on assumptions, rules, data, and decisions within those processes.

Take, for example, documented information, a core concept of a quality management system. It is essential to understand that the documented information formerly contained within the constructs of text documents and handwritten reports is now increasingly digitized. This is not limited to the transition of paper files to PDF format or the inputting of data into electronic spreadsheets.

Documented information is now incorporated into software programs, ERP systems and workflows, e-commerce portals, entities of artificial intelligence and a myriad of other formats. The requirements and inputs are integral to the software programs. Hence, "…documented information to support the operation of its processes … and the retain[ed] documented information to have confidence that the processes are being carried out as planned" (ISO 9001:2015, clause 4.4.2) are often intrinsically woven into the electronic infrastructure.

A simple example (see also Section 4) of the interaction of virtual and analog processes is a hamburger shop providing hamburgers as a product, and a fast meal as a service.

A hamburger shop can have:

- Employee conversations with customers for order taking
- Digital order-taking process via software
- Software assuming ingredients, unless otherwise indicated. Feeding order data to cookers, and inventory info to purchasing
- Sequencing of cooking activities based on the software registering orders
- Electronic cooking processes for fries, not connected to software but automated in a battery of several fryers.
- Cook selecting ingredients and adding them to assemble hamburger
- Employee coordinating order completion based on visual aids and alarms from software display
- Assembly of order (Fries, sodas, hamburger, dessert)
- Employee conversation for order delivery

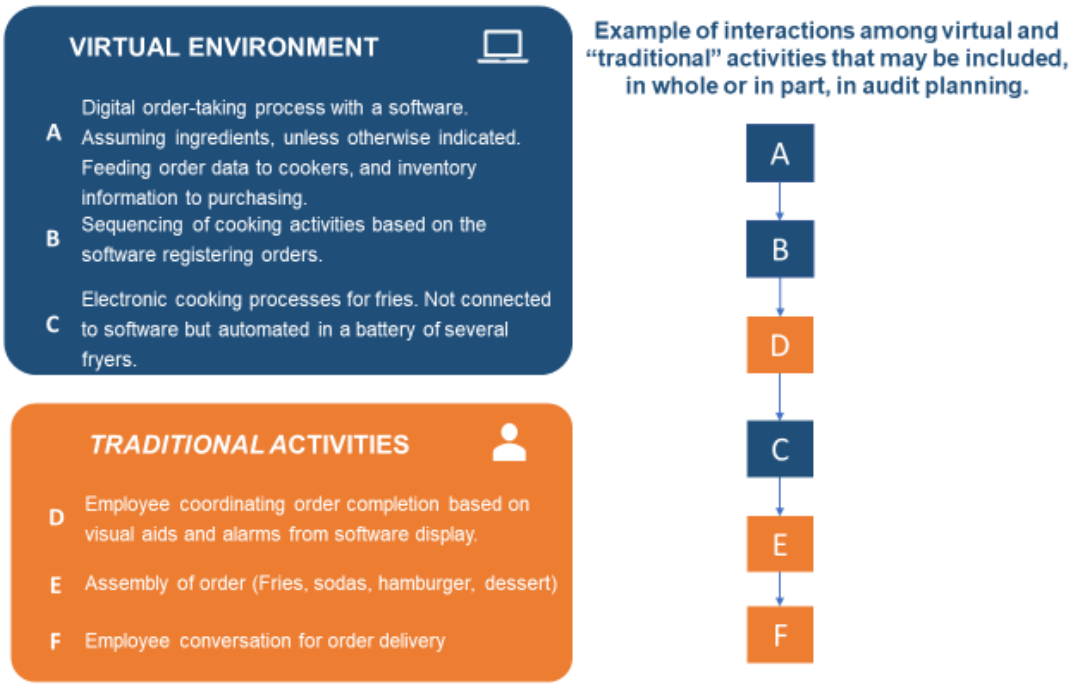


Figure 1: Hamburger shop

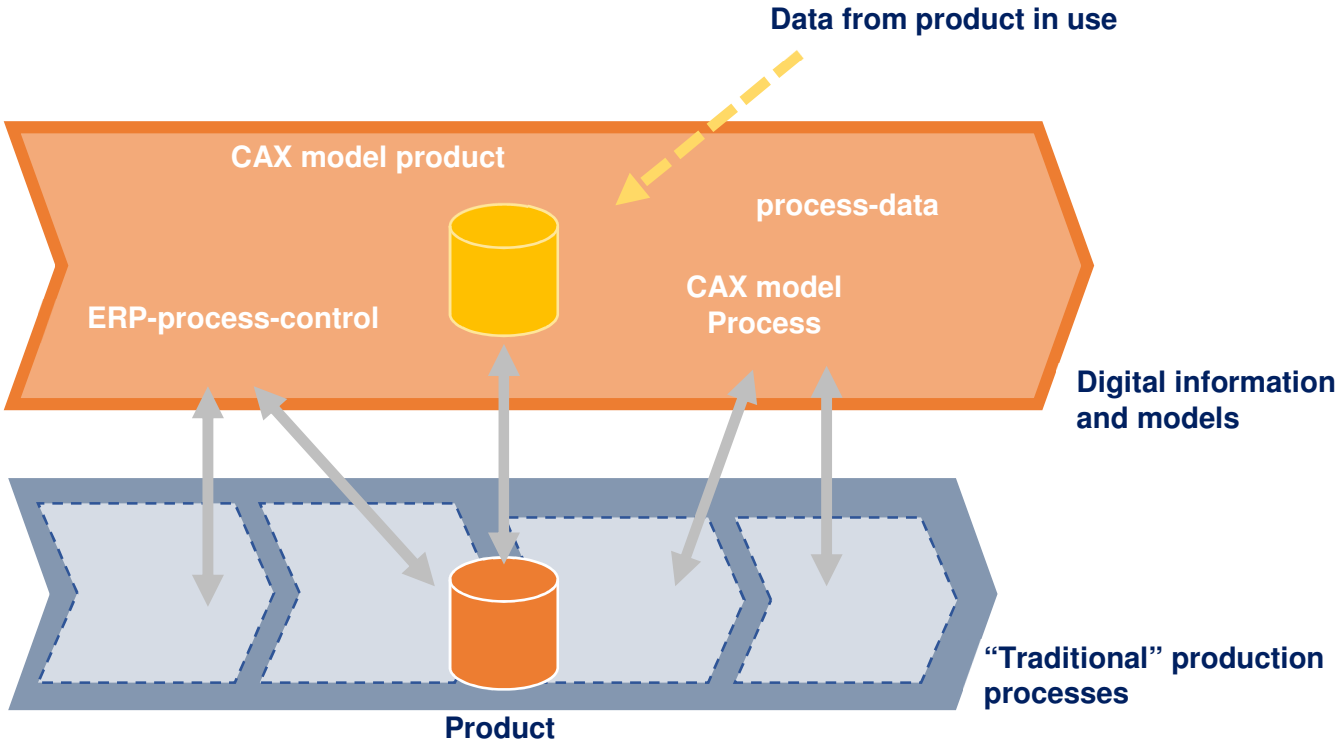
Digital and analog activities interact in organizations all the time in different ways and composition. Therefore, understanding the context in which these activities occur and constitute processes is key for effective audit planning.

This paper focus on these virtual processes, processes that are carried out mainly in an automated way with little human intervention and no direct human decision making at operational level, but where product and process characteristics are determined in a development or planning phase. Embedded in the software programs is the digitized documented information that defines and controls the process.

For consistency throughout this paper the following terms are used:
"Virtual processes" are those that are automated, embedded in software and hardware, executed without apparent human intervention.
"Traditional processes" are those that are tangible, concrete and executed with direct human intervention. They maybe also referred as «brick and mortar », « analog », «face to face » or « physical ».

2. Considering virtual processes in audit planning

The auditor, when possible, should have adequate knowledge of what digital activities are taking place and where, so that the audit plan can include enough time for understanding the digital program applications and, consequently, the virtual environment. This could be achieved during stage 1 audits or review of previous reports.



Note: CAX – Computer Aid Technology; ERP, Enterprise Resource Planning

Figure 2 – Interactions of digital and traditional activities within processes

If there is no preparatory information on virtual environments, and the auditor is facing an unexpected significant virtual process, the auditor must adjust the current audit plan and allocate time to understand and audit the processes.

When planning, the interactions between the virtual environment and traditional activities should be understood in a process approach perspective. See Figure 2 above which shows the interaction of digital and traditional activities within processes.

A digital representation may reflect the interaction of more than one process. In order to understand the decisions and controls inherent in the virtual model, a mapping may be useful for planning the audit.

Process interfaces between different program applications or virtual models are often prone to errors. Since they must be defined and controlled, the following questions in an audit may allow the auditor to determine if virtual processes are adequately controlled:

- Is there a clear understanding of which digital program applications are in use in the organization?
- Is there a clear understanding of the scope of each program, and its tasks?
- Which objects (kind of data used in the software, such as client data, product data, financial data, etc.) are represented in these models?
- How are different programs interacting?
- How coherent are the models: can data be transferred automatically (in comparison to manually) or with additional formats?
- Are data structures consistent?

When an overall view of the processes and its interfaces is available, the effectiveness of each program should be audited. This is a critical point. Some topics to consider in order to understand if the program is doing its job:

- What is the scope of its model?
- What are the intended results?
- What are the inputs and outputs and how they are realised and communicated /transmitted?
- How was the model developed? Which assumptions and simplifications have been made? What is the scope of the resulting program application?
- Who has developed the model? Who has the authority and responsibility to change it?
- How was the model verified against requirements and tested for consistency?
- How was the model validated and what were the results?
- Where have deviations to the reality/ limitations to applicability been detected?
- How are the results of the model used?
- What data from usage of the product or service are brought back over the life cycle for the improvement of products, services and processes?
- How is the model changed?
- Does the organization have a contingency scenario in case the model has incorrectly executed its task.

The auditor should ensure that the individual being interviewed is the one with responsibility for these aspects of the process; in general it is not the operator of the machine, or the person working on an operative level.

It is important during audit planning to allocate adequate time for interviews with developers of algorithms, persons fixing decision criteria and persons involved in validating applications.

3. Audit realization

When observing a virtual environment, auditors may be biased to consider that the personnel in the control room are actually taking all decisions in the process. Auditors may also focus on the equipment, sensors and digital interfaces and consider them controls. However, the equipment and the personnel running the equipment should be only part of the audit process. The auditor should understand the intended results of the virtual process and how actual decisions are made. See examples in table 1.

Virtual process intended results Intent is the expected outcome of the process.	Decisions made virtually Tasks and actions taken by the digital program
"filtering of similar items within a website"	"what is the algorithm or equation behind that filtering?"
"activating material-feeding equipment when parameters are reached"	"How is the equipment activated? Which parameters exist?
"show visual alerts in all sensors during operations".	"how do dozens of sensors interact and where does the alert activation occurs? Under what criteria?"

Table 1 – Examples of process intended results and program's decision criteria.

A suitable audit model of a virtual environment comprises the understanding of the process intended results.

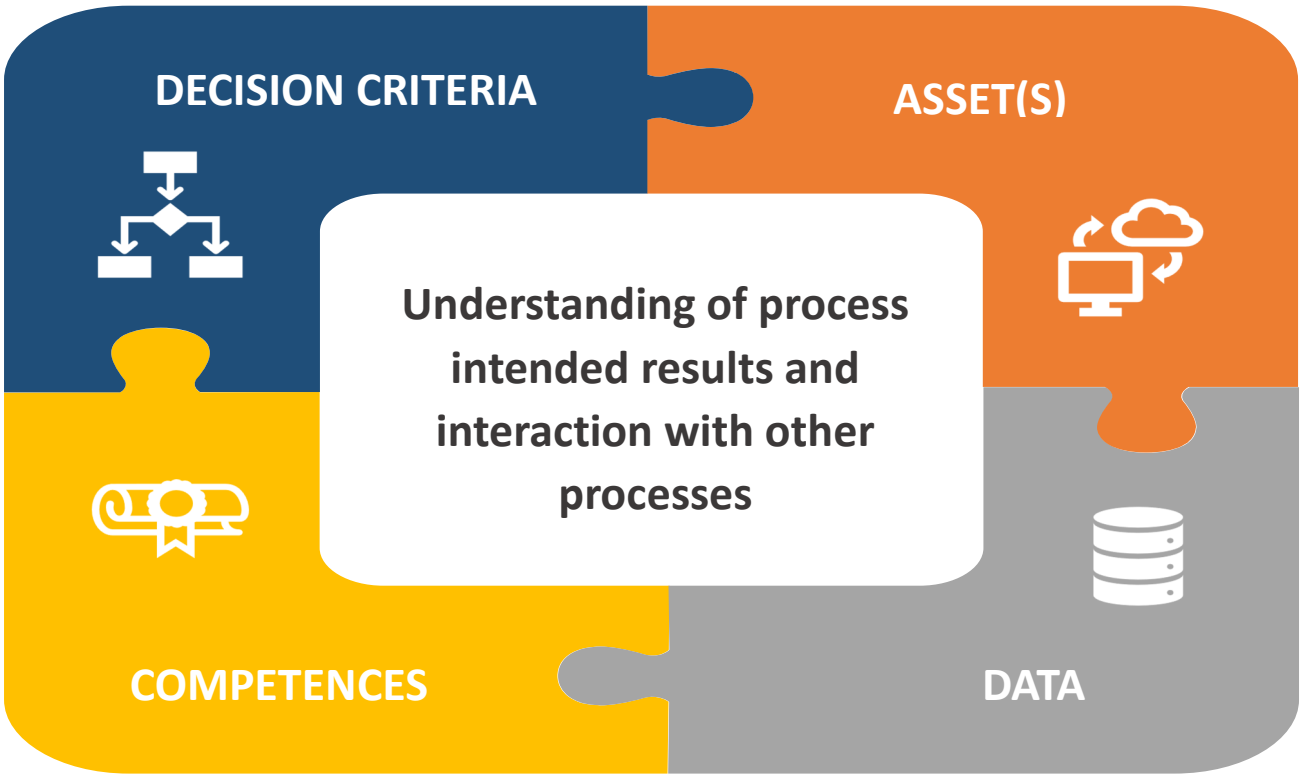


Figure 3 - Audit model for understanding the virtual environment.

The model can be used to achieve understanding and establish the basis to verify conformity to requirements by understanding the interaction among the program(s), the technological assets, their decision criteria and competences.

4. Practical case studies

Case 1: Hamburger shop

Using the model in figure 2 and the hamburger shop example in the Introduction, here is a practical example of the audit model implementation.

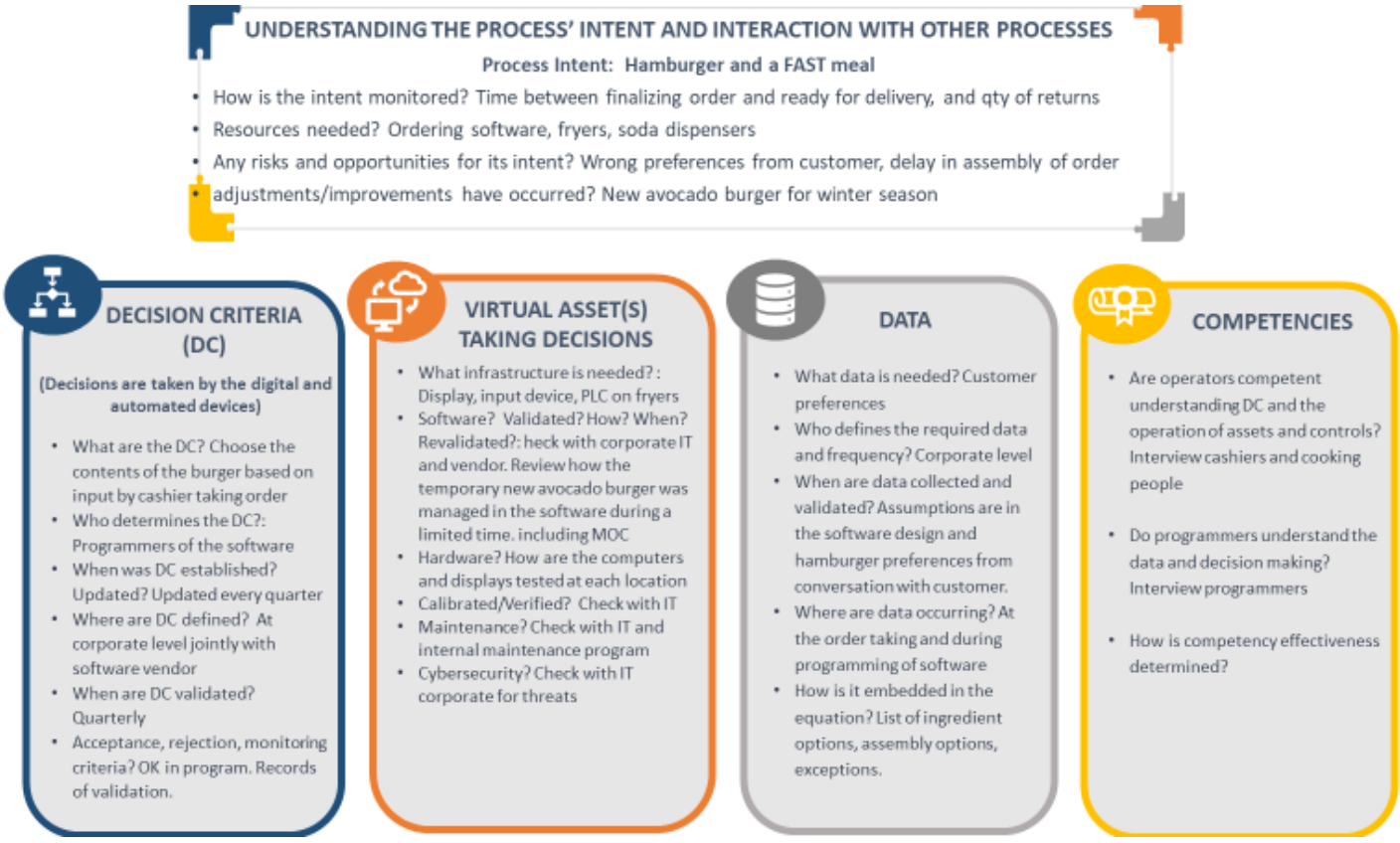


Figure 3 – Application of the audit model for understanding the virtual environment to a burger shop

Case 2: Auditing the purchasing function

The control of the purchasing function may be driven by complex algorithms that calculate inventory value, inventory turns, supplier lead times, seasonal peaks in sales, obsolescence, new product releases, product shelf-life and market trends. The output of the calculations could be so highly automated that when an item falls below a pre-determined stock level, a purchase requisition is transmitted through EDI (Electronic Data Interchange) to the supplier – with no human intervention. The product is received on the dock. It is then barcode scanned using handheld scanners that are networked to the ERP database. An acceptance label with warehousing barcode is printed and the material is routed into stock. There is no inspection due to the fact that the system has been programmed to flag any incoming goods with zero defects over a predetermined number of previous shipments as “dock-to-stock”. This signifies,

based on objective data, that the risk has been assessed and the product has been determined as not requiring incoming inspection or verification. The process is completely automated – with the exception of the individual receiving the goods. That step could be further automated by having robots move product from dock to designated shelf location. How does an auditor assess these interrelated processes to determine conformance to the requirements of *8.4 Control of externally provided processes, products and services*?

The auditor might request samples of the inspection reports that have been uploaded to the ERP, which drives the dock-to-stock program. To determine effectiveness of the inventory level program, questions might be asked to see if any customer orders were delayed due to out-of-stock conditions. An interview with both the purchasing agent and the individual who sets up the min/max parameters in the ERP system would demonstrate that the purchasing process is achieving the goal of maintaining levels that are aligned with financial objectives. An engineer might be interviewed to explain how part numbers with complete and correct description are loaded into the ERP system, complete with designated suppliers.

The same question may be asked in relation to a variety of other clauses of the ISO 9001 standard (see 5. Appendix, below, for clause based examples).

Case 3: Machine learning audit

During conformity assessment, an auditor may encounter the usage of methods such as machine learning by the organization being audited. Also, in connection with machine learning, a number of concepts are used, such as artificial intelligence, data mining, etc. These concepts are related and the application of a particular term, and its interpretation are directly dependent on the organization.
As machine learning is improvement through experience, the auditor should achieve understanding of how the audited process used computer algorithms. Each scenario may offer a different perspective, thus the importance of planning for understanding that process running within machine learning applications.
Machine Learning methods can be used in such programs as:
- Voice assistants;
- Chat bots;
- A variety of data analysis and forecasting programs;
- Control of various mechanisms without human participation or with limited human participation, etc.

In any case, the auditor should collect objective evidences on the following issues:
- What machine learning method / model is used (e.g. Neural Network, Random Forest, K-Neighbours etc.)?
- How was it adapted to the particular application?
- How was the method / model trained (if applicable)?
- How was its performance verified/validated?
- In what circumstances (if applicable) should a method / model transfer control to a human operator? How is this transfer established and how reliable is the transfer?

5. Appendix – Clause based examples

Examples of applications of various levels of electronic data, digitized processes and supporting resources are presented here in relation to clauses of ISO 9001:2015

These examples are not exhaustive and can be elaborated. Although presented in relation to the clauses of the standard to which they relate closer, it is important to remind that audit is done by processes

Clause/ sub- clause		Process (or activity)
4.4	Quality management system and its processes	• Defining the interrelation of virtual processes • Audit the process approach planning implementation and changes within the virtual processes
5.3	Organizational Roles, responsibilities and authorities	• Defining accesses and authorization levels • Responsibility of programmers • Responsibility of program operators
6.1	Actions to address risks and opportunities	• Use of algorithms to quantify risk
7.1.3	Infrastructure	• Production equipment programs for maintenance integral to machinery • Preventive maintenance software programs (stand-alone) or integrated into ERP production schedule • Program updates • Software and hardware compatibility
7.1.5	Monitoring and measuring resources	• Selecting monitoring and measuring resources • Ensuring integrity of algorithms and other electronically controlled monitoring, such as real-time SPC adjustments. • Calibration programs managed through software – including determining/monitoring frequencies and recall • Access of calibration of records through portal of third party provider of calibration services.
7.2	Competence	• Competence as relates to agility to understand and use digitized media effectively • Availability of self-directed on-line training • Competence of programmers • Competence of program operators
7.4	Communication	• Communication reliant on programmed alerts, etc. • Communication to other locations for organizations with multi-site schemes • Communication with customers, suppliers and other interested parties through portals.
7.5	Documented information	• Control of the electronic infrastructure, including security and other risks • Control and maintenance of website

		• Ensuring appropriate processes in place for: identification, description, format, review, approval, access retrieval and storage • Change control
8.1	Operational planning and control	• Production planning (including determination of resource constraints) • Service provision planning • How requirements for products and services, respective acceptance criteria and criteria for the processes are integrated on the application ? • How is control implemented in SW?
8.2	Requirements for products and services	• Customer requirements for both products and QMS related requirements accessed through portals • Transmission of orders through EDI or through customer portals. • E-commerce • Communication with customers including, complaints, corrective action portals, regular report cards
8.3	Design and development of products and services	• Any and all software for design including CAD/CAM, Solid Works, Gerber files, etc. • Inputs for the program design • Control of program design changes
8.4	Control of externally provided processes, products and services	• ERP system • EDI order transmission • Monitoring of product shelf life, etc.
8.5	Production and service provision	• Monitoring and control of automated processes – speed, time, temperature, weight, viscosity, etc. • Remote monitoring and control of processes as a joint responsibility between supplier and customer.
8.5.6	Control of changes	• Automatic record of change with dates and authorization
9.1	Monitoring, measurement, analysis and evaluation	• Performance evaluation – monitoring of processes through electronic media and the ability to analyze the data for effective decision making • Validation of data, input as well as output
10.2	Nonconformity and corrective action	• Ability to link nonconforming outcomes to corrective actions • Capability to link multiple other processes such as engineering change notices and design changes

---

For further information on the ISO 9001 Auditing Practices Group, please refer to the paper: Introduction to the ISO 9001 Auditing Practices Group
Feedback from users will be used by the ISO 9001 Auditing Practices Group to determine whether additional guidance documents should be developed, or if these current ones should be revised.

Comments on the papers or presentations can be sent to the following email address: charles.corrie@bsigoup.com.

The other ISO 9001 Auditing Practices Group papers and presentations may be downloaded from the web sites:

www.iaf.nu
www.iso.org/tc176/ISO9001AuditingPracticesGroup

Disclaimer

This paper has not been subject to an endorsement process by the International Organization for Standardization (ISO), ISO Technical Committee 176, or the International Accreditation Forum (IAF). The information contained within it is available for educational and communication purposes. The ISO 9001 Auditing Practices Group does not take responsibility for any errors, omissions or other liabilities that may arise from the provision or subsequent use of such information.