International Organization
Standardization
Web: www.iso.org

for International
Accreditation Forum
Web : www.iaf.nu

Edition 2
Date: 2021-06-07

ISO 9001 Auditing Practices Group

Guidance on:

Auditing Statutory and Regulatory Requirements

Table of Contents

INTRODUCTION

An organization adopting ISO 9001 needs to demonstrate its ability to conform to the statutory, regulatory, and customer requirements, which are applicable to its products and services within the scope of its quality management system (QMS). Throughout the standard, ISO 9001 defines requirements for an organization to identify the statutory and regulatory (S&R) requirements applicable to its products and services. Organizations should, determine their applicability, define the processes needed to address them and the means to demonstrate consistent ability to meet these requirements.

S&R requirements applicable to the products and services provided may range from extreme simplicity to a degree of complexity. Some products and services are heavily regulated, while others have very few, if any, requirements.

When auditing ISO 9001 QMS requirements, the auditor needs to consider the S&R requirements applicable to the organization's products and services. Auditors must be aware of the differences and implications between auditing conformity to QMS requirements and verifying compliance to legal requirements.

1. UNDERSTANDING STATUTORY AND REGULATORY REQUIREMENTS

S&R requirements are obligatory. The statutory are specified by a legislative body and the regulatory by an Authority mandated by a legislative body, see definitions 3.6.6 and 3.6.7 in ISO 9000:2015.

- Examples of Statutory requirement are those issued by any kind of Government, such as Regional, National, Federal, State or Local Governments.
- Examples of Regulatory Requirements are requirements issued by Agencies like Food agencies, Medicine authorizations bureaus, Communications regulators, aerospace regulators, etc.

S&R requirements can be related to product and service characteristics, to their life cycle processes, to production and servicing processes, respective test methods or monitoring and measuring activities, to information labelling, packaging, trading authorizations to put in the market, consumer rights, warranty, infrastructure requirements, qualification of personnel, service level, capacity, and more. While some products or services are required to have product certification or approval (e.g. CE marking, FDA approval, etc.) others, like in the service sector, may also include Local Licensing Regulations.

Government agencies and organizations may adopt by reference voluntary industry standards such as those from the IEC (International Electrotechnical Commission), API (American Petroleum Institute), DIN (German Institute for Standardization), ISSN (International Standard Serial Number centre), NACE (National Association of Corrosion Engineers), CEN (European Committee for Standardization) and other institutions that generate standards that are used nationally or internationally. These industry standards may be voluntary, but they may become mandatory when the government authority requires conformance to such standard's requirements. This way standardization supports legal requirements.

The table in Annex A gives the relationship between the clauses in ISO 9001, which refer to S&R requirements and the context in which these S&R requirements may be audited.

Audit teams must be competent to audit the quality management system of an organization. A relevant aspect of the audit team's competence is their knowledge and understanding of S&R requirements relevant to the organization, as defined in ISO/IEC 17021-3 Conformity assessment —Requirements for bodies providing audit and certification of management systems — Part 3: Competence requirements for auditing and certification of quality management systems.

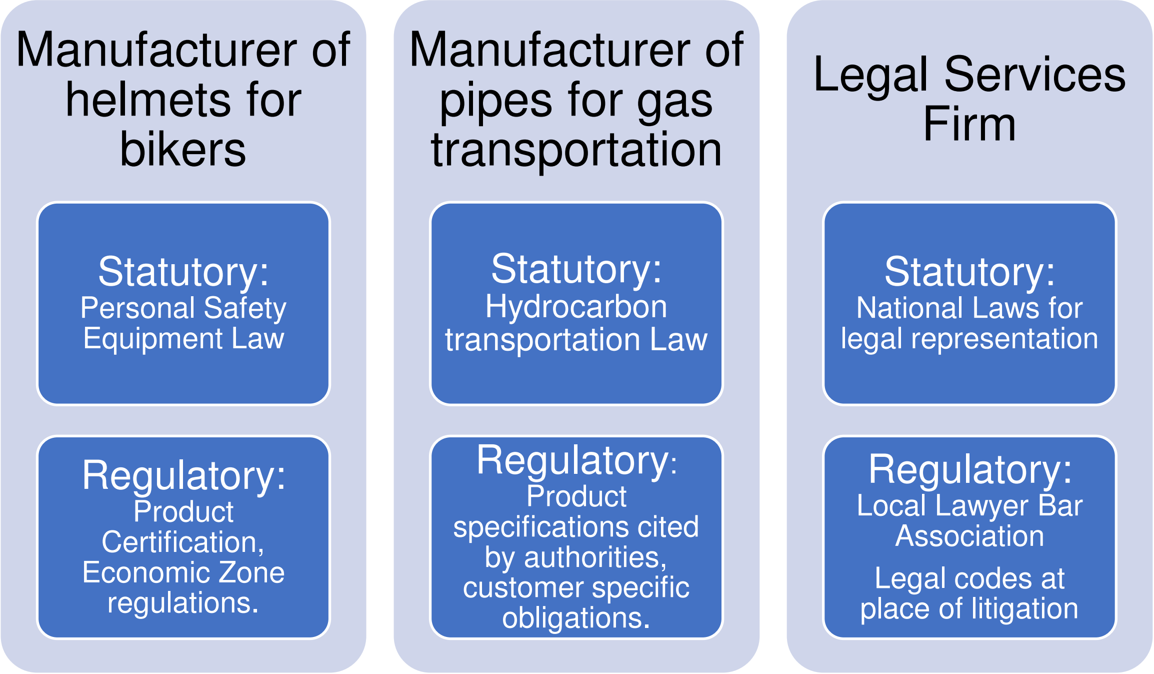
Manufacturer of helmets for bikers
Statutory: Personal Safety Equipment Law
Regulatory: Product Certification, Economic Zone regulations.
Manufacturer of pipes for gas transportation
Statutory: Hydrocarbon transportation Law
Regulatory: Product specifications cited by authorities, customer specific obligations.
Legal Services Firm
Statutory: National Laws for legal representation
Regulatory: Local Lawyer Bar Association
Legal codes at place of litigation

Figure 1 - Examples of general sources of S&R requirements

2. AUDITING STATUTORY AND REGULATORY REQUIREMENTS IN THE CONTEXT OF AN ISO 9001 AUDIT

During the audit preparation phase and audit execution phase, auditors should obtain relevant information from internal or external sources with respect to S&R requirements that may be applicable, and the respective interested parties involved. When sampling for S&R requirements, auditors should consider not only Statutory requirements such as laws for Product Liability Act, Act on Electrical Engineering, food law, sector specific law, etc. but also include regulatory requirements set out in Directives such as those for Machinery Regulation, CE marking, Construction Products Directive, material regulations, trade licences, contracts, liability insurance, codes of federal regulations, and others, where applicable.

Sampling S&R requirements should take a risk based approach and ensure a balance between different requirements, while at the same time giving proper attention to those that can be more harmful for the organization, its customers or end users of products and services.

ISO 17021-1 requires that one of the objectives of a third-party management system audit is the “determination of the ability of the management system to ensure the client meets applicable statutory, regulatory and contractual requirements”. It includes a note, which states that “a management system certification audit is not a legal compliance audit.” The audit team must keep in mind that S&R requirements are not audited for compliance. Rather, the organization’s processes are audited to evaluate their ability to address those S&R requirements.

A management system audit is not a verification of compliance to all applicable requirements to the products and services provided, nor does certification imply a statement of full compliance by the organization. An evidence-based approach utilizing sampling is an important principle when auditing management systems. While evaluating the organizations conformity to the ISO 9001 standard, auditors collect evidence regarding the organization’s processes and its ability to effectively determine, manage and consistently ensure conformity with S&R requirements applicable to products and services. Please refer to ISO 19011 cl 4.f. and cl A.7

3. AUDITING STATUTORY AND REGULATORY REQUIREMENTS AND POTENTIAL LIABILITIES

The responsibility to demonstrate legal compliance resides in the organization. To avoid liability to the audit team, auditors should not make statements regarding compliance to S&R requirements or make any prescriptive comments related to specific statutory or regulatory requirements.

When an organization’s process for statutory or regulatory requirement is found non-compliant, the auditor may write a finding in reference to the applicable QMS requirement. For example, there may be an S&R requirement, related to the delivery of a non-conforming product or service. The finding may be cited against ISO 9001 cl 8.6 relating to release of a product, or (ISO 9001 cl 8.7) relating to controlling of non-conforming product. Similarly, the failure to handle a consumer complaint according to legal requirements (where legal requirements exist related to handling of complaints) may be related to ISO 9001 cl. 8.2.1 Customer Communication. QMS nonconformities should be issued only in situations where there is evidence that quality management system deficiencies have been identified.

Auditors should be careful and avoid becoming legally liable for acts or omissions when auditing and reporting on compliance against legal requirements outside the agreed audit criteria and beyond auditor’s competence. If environmental, health and safety, or other non-QMS related compliance obligations are found non-compliant, the QMS auditor may bring it to the attention of the audited organization, clarifying that it is not a QMS finding. If a serious breach of a S&R requirement (e.g., a health and safety regulation) is identified, the audit team should refer this immediately to the certification body, in order to decide if it should be reported to the regulatory body.

The QMS auditor should be aware that liabilities may exist, and confidentiality agreements may be an important consideration when reporting a finding related to compliance obligations, or requirements outside of the agreed audit criteria.

4. STATUTORY AND REGULATORY REQUIREMENTS AND THEIR BOUNDARIES IN THE QMS

S&R requirements are to be audited under the boundaries of what is applicable to the products and services within the QMS scope. Figure 2 (below) shows these boundaries.

QMS auditors should focus on evaluating the way the QMS processes are addressing the applicable S&R requirements.

ISO 37301:2021 *Compliance management systems — Requirements with guidance for use* specifies requirements and provides guidelines for establishing, developing, implementing, evaluating, maintaining and improving an effective compliance management system within an organization, however, its scope goes beyond the boundaries for a QMS. For ISO 9001 audits, the QMS determines the scope of the S&R requirements to be considered. Both ISO 37301 and ISO 9001 are management system standards audited for conformity with their requirements. Even for certification to ISO 37301 there is not a presumption nor a declaration of compliance.

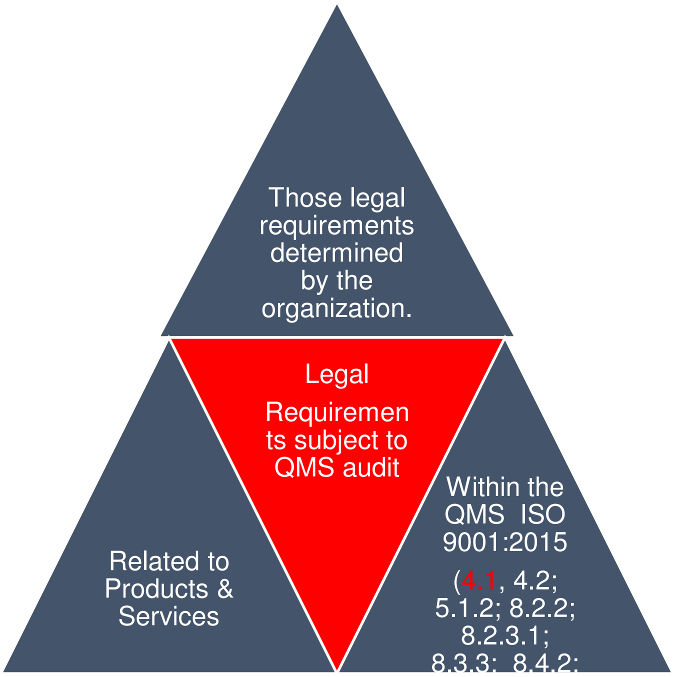
Those legal requirements determined by the organization.
Legal
Requirements subject to QMS audit
Related to Products & Services
Within the QMS ISO 9001:2015
(4.1, 4.2; 5.1.2; 8.2.2; 8.2.3.1; 8.3.3; 8.4.2;

Figure 2 - S&R requirements are to be audited under the boundaries of what is applicable to the products and services within the QMS scope

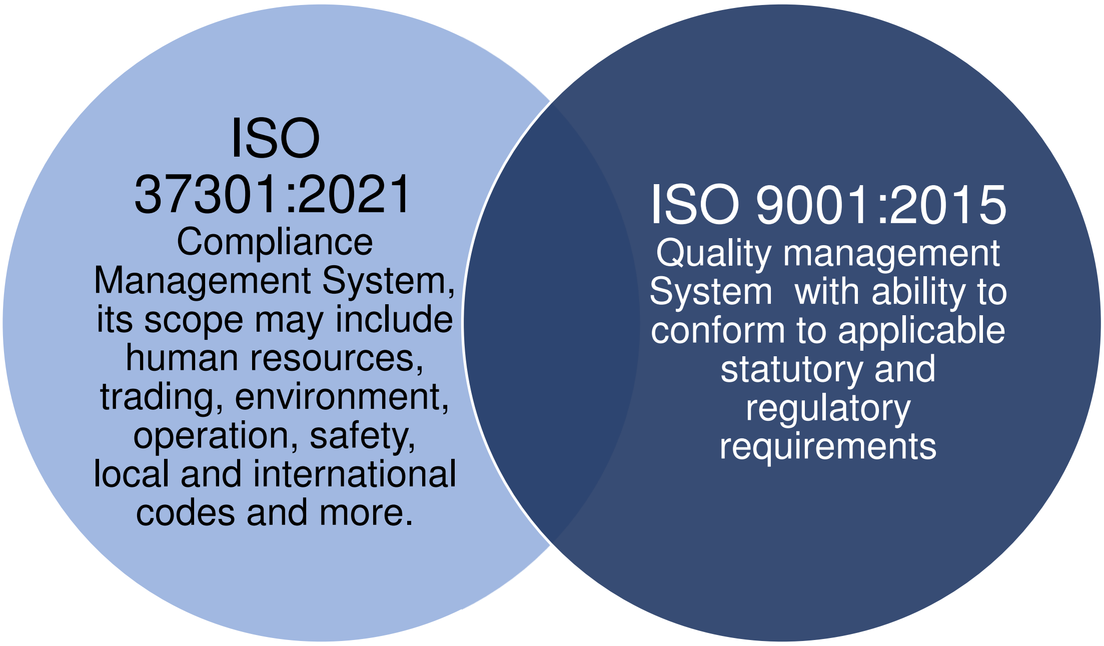
ISO 37301:2021
Compliance Management System, its scope may include human resources, trading, environment, operation, safety, local and international codes and more.
ISO 9001:2015
Quality management System with ability to conform to applicable statutory and regulatory requirements

Figure 3 – Overlap between ISO 9001 and ISO 37301

5. STATUTORY AND REGULATORY REQUIREMENTS AND AUDIT CONCLUSIONS

Finally, when reviewing audit findings, verifying the fulfilment of audit objectives and determining the audit conclusions, a conclusion on the extent of QMS conformity with the audit criteria should be stated as referred in ISO 19011 cl 9.4.9.2, including the effectiveness of the management system in meeting its intended outcomes, which includes a conclusion on the organization's demonstration of its ability to consistently provide products and services that meet customer and applicable S&R requirements.

Annex A provides a non-limiting set of examples of context(s) that the auditor may find when considering S&R requirements while auditing ISO 9001.

ANNEX A

CONTEXT OF AUDITING STATUTORY AND REGULATORY REQUIREMENTS WITHIN ISO 9001:2015

Clause	ISO 9001 clause	Context for the auditors
4.1	Understanding the Organization and its Context	The organization is required to evaluate external context that would include S&R requirements and have controls in place to monitor changes to these requirements.
4.2	Understanding the needs and expectation of interested parties	S&R requirements may be different among interested parties, which may have legal requirements coming from their own governments, or regulations from their customers. Auditors should assess that interested parties such as regulatory agencies were appropriately identified, and their interests determined by the organization. During the audit the interactions between the organization and its interested parties for the markets where they operate, should be assessed. Some S&R may take the form of mandatory product or service certification.
4.4.	Processes	Many types of products and services will also have their production processes, or service delivery processes regulated. For example, service companies such as utilities are usually regulated by service level agreements that may take the form of objectives for their processes. The production of medicines and medical devices often includes regulation of their production processes.
5.1.2	Customer Focus	Auditors should assess the leadership initiatives that top management is exercising to ensure effective management of S&R requirements on product and services.
7.1	Support	Requirements for infrastructure, equipment, competence and qualification of personnel are common in public services such health and social services, education, etc.

		Facilities open to the public are subject to licensing permits that define requirements for the infrastructure Communication with the client and authorities can also be the subject of S&R requirements
8.2.2	Determining the requirements for products and services	When auditing customer related processes, the determination of S&R requirements may be included in documentation such as request for proposals/quotations, purchase orders, sales meetings, or other relevant communications with the customers. These may have been previously determined by the organization (see 4.2).
8.2.3	Review of the requirements for products and services	Auditors should collect evidence of the organization's commitment to provide its product and services and establish if S&R requirements were considered. Auditors may find evidence in activities and documentation such as contracts, accepted purchase orders, audit plans, emails, agreed designs, product catalogs, product technical datasheets, websites, digital marketing and other forms of agreements with customers.
8.3.3	Design and development inputs	Auditors may review S&R requirements mentioned in the communication with customers, previous designs and the auditor's expertise, as well as other sources of information and assess how they have been integrated into the design of the product or service.
8.4.2	Type and extent of control	Externally provided processes, products and services may impact the organization ability to manage their applicable S&R requirements. Auditors should collect evidence within the agreements with suppliers, purchase orders, designs, audit plans, service quality plans, receiving inspection, monitoring plans and other control activities and documentation that the organization ensures that applicable S&R requirements are determined, acknowledged, and managed by the supplier, and that the organization has adequate control over them.
8.5.5	Post Delivery activities	Auditors should evaluate how post-delivery commitments include S&R requirements. Auditors may audit warranties, maintenance services, management of data exchange with customers, contracts, website offerings, and previous processes related to sales, design, and suppliers.

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

https://committee.iso.org/home/tc176/iso-9001-auditing-practices-group.html

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.