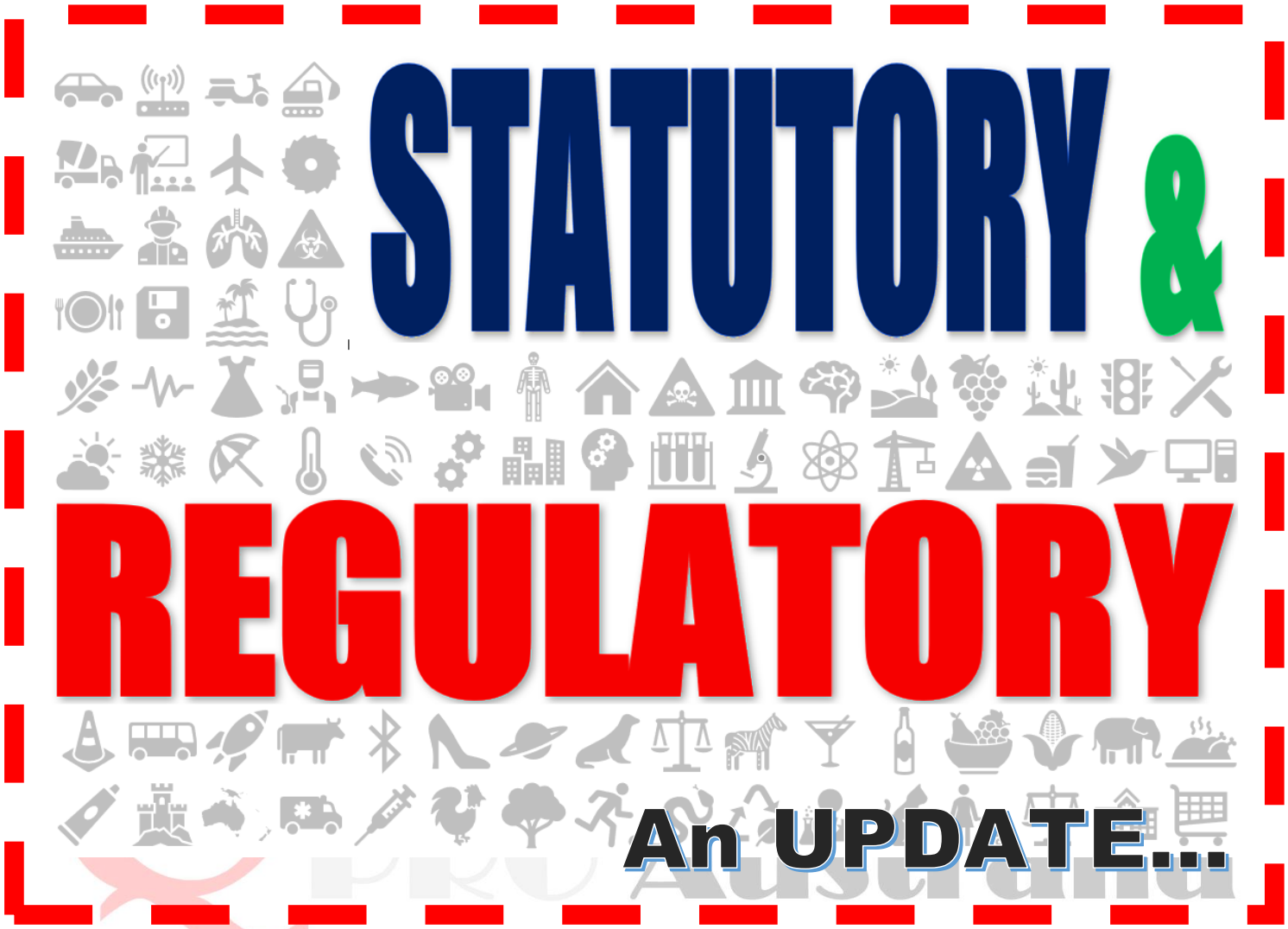


Statutory and Regulatory (S&R) Requirements – An Auditing Insight

1 S&R Requirements – A link to the Previous Article (An insight and clarity posted on 30-Sep-19)

2 S&R Overview

In this article the author has given latest update with a clarity, details and aspects included and applicable to organisation adopting or implemented or certified to the **ISO 9001:2015 (QMS)** | **ISO 14OO1:2015 (EMS)** | **ISO 45001:2018 (WHS-MS)** standards or other management systems.

3 Statutory and Regulatory Requirements - INTRODUCTION

Any organisation adopting and/or certified to ISO 9001:2015 (QMS) | ISO 14OO1:2015 (EMS) | ISO 45001:2018 (WHS-MS) or other management systems standards would require to demonstrate their ability to conform to the statutory, regulatory, and customer requirements, applicable to their products and services within the scope of the appropriate management systems.

However, for the purpose of easiness, I have focussed on the **ISO 9001:2015 as the standard in context to the S&R Requirements.**

The standard, ISO 9001:2015 requires an organisation to identify the applicable statutory and regulatory (S&R) requirements for the products and services they provide/deliver to their customers. This means that organisations should,

1. Determine the S&R applicability;
2. Define the processes needed to address them; and
3. The means to demonstrate consistent ability to meet the S&R requirements.

Refer Annex B – S&R Assurance Process

4 S&R Scope Debunked

In this article, S&R is focused to give an organisation the details on the following including the role of an external assessor from CAB.

1. Understanding Statutory and Regulatory requirements
2. Auditing Statutory and Regulatory Requirements in the context of an ISO 9001:2015 audit
3. Auditing Statutory and Regulatory Requirements and potential liabilities
4. Statutory and Regulatory Requirements and their boundaries in the QMS
5. Statutory and Regulatory Requirements and audit Conclusions

4.1 Understanding Statutory and Regulatory requirements

S&R requirements are mandatory. The statutory are specified by a legislative body (*3.6.6 in ISO 9000:2015*) and the regulatory by an authority mandated by a legislative body (*3.6.7 in ISO 9000:2015*). Below are examples to demonstrate the differences of S&R

- **Statutory** requirements are issued by specified by a legislative body like the local, regional, state, federal government.
- **Regulatory** requirements are issued by an authority mandated by a legislative body like road transport regulators, aerospace regulators, food regulators/agencies, medicine bureaus etc.

In general, applicable S&R requirements related to products and services may typically be specific to these processes e.g.,

- Lifecycle of a product
- Product manufacturing
- Equipment and devices
- Product warranty
- Inspection and test methods or monitoring and measuring activities
- Labelling and packaging
- Storage, handling and transport
- Product introduction to local, national and international market
- Consumer rights
- Infrastructure requirements
- ICT communication
- Safety & security
- Travel & transport
- Personnel qualification (including schools, university, RTO's)
- Commercial and technical (products and services) and more

Note:

1. Some products require product certification or approval e.g., CE marking, FDA/ TGA approval etc. and others, like in the service sector, may require to comply with Licensing Regulations etc.

2. Annex A – The table gives the relationship between the clauses in ISO 9001:2015, and references to the S&R requirements. These S&R form a part of the auditing process including customer specific requirements (CSR).
3. Auditing Statutory and Regulatory Requirements in the context of an ISO 9001:2015 audit

4.2 Auditing S&R requirements in the context of an ISO 9001:2015 audit

You will notice that your certification body will be now more focussed on S&R requirements to verify how well you meet and comply to the S&R requirements applicable to the products and services you provide to your customers. During such audits, it now requires that auditors performing first, second-, and third-party audits have a process to assess the S&R process.

It means that the CAB assessors have the task to prepare, perform risk assessments based on the activities that will be executed. So, the external assessors would require to ensure that the process is tested and ensure that all applicable S&R requirements from sources are reviewed, understood and audits performed. The S&R auditing process may be sampled as appropriate.

CAB assessors/audit team would perform an ISO 9001:2015 audit but they are looking for effectivity of the S&R process and not compliance. It means that the organisation's S&R processes are evaluated and verified if the organisation have addressed their ability to those applicable S&R requirements.

This is a requirement of the ISO 17021-1 and 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.*"

However, the auditors require to demonstrate competency in S&R process. It purely means that auditors must have a thorough knowledge and understanding of S&R requirements relevant to the organisation products and services. For the CAB Assessor, they have to ensure their competence meet the requirements 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.

In summary, organisation's conformity to e.g., ISO 9001:2015 standard is evaluated. An external assessor may just gather evidence regarding the S&R processes and how effective the process is.

So, it is organisation's responsibility to ensure that there is a robust system in place to assure process conformity and compliance to applicable S&R requirements (*Reference: ISO 19011:2018 cl 4.f. and cl A.7*). Refer section 4.3 in this article.

4.3 Auditing Statutory and Regulatory Requirements and potential liabilities

Even if an organisation has a certified or non-certified management system, all S&R requirements are the responsibility of the organisation. They are accountable for and they must demonstrate that legal compliance is met and sustained.

Internal auditors may require to ensure that they take proactive evaluation to verify compliance to the applicable S&R requirements. Note: An external assessor from a CAB may avoid liability. It means that the CAB auditors would not make statements regarding compliance to S&R requirements or make any prescriptive comments related to specific statutory or regulatory requirements.

The CAB assessors would be careful and avoid becoming legally liable* for acts or omissions when auditing and reporting on compliance against legal requirements outside the agreed audit scope and criteria and/or is beyond assessor's competence. It is a shame that an organisation would expect an independent assessor's input in regards to the S&R compliance. Unfortunately, it is the liability of the organisation to assure that they meet the applicable S&R requirements for the products and services they deliver to their customers.

During a routine QMS audit (ISO 9001:2015), if an environmental and/or health and safety, or other non-QMS related compliance obligations are found to be non-compliant, the CAB assessor may bring it to the attention of the audited organisation, clarifying that it is not a QMS finding.

However, if there is an evidence of a serious breach of a S&R requirement (e.g., an environmental and/or health and safety regulation and/or serious security breach etc.), the CAB Assessor have the right to immediately inform to the certification body, in order to decide if it should be reported to the regulatory body.

So, it's clear that it is organisations' liability to assure that confidence of the S&R requirement conforms and that applicable S&R requirement comply for the products and services they provide to their customer or the end users.

*NOTE: *An external CAB Assessor may not report a finding related to compliance as certain obligations, or requirements outside of the agreed audit criteria as some liabilities may exist, and confidentiality agreements per contract or similar agreements may be an important factor.*

4.4 Statutory and Regulatory Requirements and their boundaries in the QMS

ISO 9001:2015 requires that organisation meet S&R and customer/contractual requirements. Therefore, applicable S&R requirements of products and services are audited within the boundaries of the QMS scope.

However, if the products and services provided by the organisation mandates or require compliance requirements to the new standard ISO 37301:2021 (*previously ISO 19600:2014 Compliance management systems — Guidelines*), then the CAB assessors would perform the audit per the CMS criteria. Both ISO 9001:2015 AND iso 37301:2021 are Type A management systems.

NOTE:

1. **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 organisation. The CMS scope goes beyond the boundaries for a QMS. For ISO 9001:2015 audit, the QMS determines the scope of the S&R requirements to be considered. Both ISO 37301:2021 and ISO 9001:2015 are management system standards audited for conformity with their requirements. Even for certification to ISO 37301:2021 there is not a presumption nor a declaration of compliance.
2. A certified CMS can be an indicator of an organisation's due diligence and commitment to **compliance** which may be useful in limiting legal liability and lowering penalties for contraventions of relevant laws. Hence, organisation develops a positive culture of compliance, build strong and valuable relationships with regulators, build customer trust and loyalty etc.

4.5 Statutory and Regulatory Requirements and audit Conclusions

In finalising the assessment of an organisation processes per ISO 9001:2015, the assessor has to review the audit findings, verify the fulfilment of audit objectives and then determine the audit conclusions. A conclusion on the extent of QMS conformity with the audit criteria should be stated as referred in ISO 19011:2018 cl 9.4.9.2, including the effectiveness of the management system in meeting its intended outcomes, which includes a conclusion on the organisation'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 9001:2015.

5 Terms and Definitions:

The key terms and definitions from the management system standards are used for clarification purposes and is an extract from the appropriate standards.

Terms and definitions (extract from the standards)

ISO 9000:2015 Quality management systems — Fundamentals and vocabulary

3.6.4
requirement
need or expectation that is stated, generally implied or obligatory

3.6.6
statutory requirement
obligatory *requirement* (3.6.4) specified **by a legislative body**

3.6.7
regulatory requirement
obligatory requirement (3.6.4) specified by an **authority mandated by a legislative body**

NOTE 2 Statutory and regulatory requirements can be expressed as legal requirements.

ISO 14001:2015 Environmental management systems —Requirements with guidance for use

3.2.8**
Requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.1.4) and *interested parties* (3.1.6) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (3.3.2).

Note 3 to entry: Requirements other than legal requirements become obligatory when the organization decides to comply with them.

3.2.9
Compliance obligations (preferred term)
Legal requirements and other requirements (admitted term)
Legal *requirements* (3.2.8) that an *organization* (3.1.4) has to comply with and other requirements that an organization has to or chooses to comply with

Note 1 to entry: Compliance obligations are related to the *environmental management system* (3.1.2).

Note 2 to entry: Compliance obligations can rise from mandatory requirements, such as applicable laws and regulations or voluntary commitments, such as organisational and industry standards, contractual relationships, codes of practice and agreements with community groups and non-governmental organizations.

NOTE:
The term **"compliance obligations"** in ISO 14001:2015 replaces the ISO 14001:2004 phrase **"Legal requirements and other requirements at to which the organization subscribes"**. The intent of this new term does not differ from that of the 2004 edition.

ISO 45001:2018 Occupational health and safety management systems — Requirements with guidance for use

3.8
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (3.24),

Note 3 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1.

3.9
legal requirements and other requirements
legal requirements that an organization (3.1) has to comply with and other requirements (3.8) that an organization has to or chooses to comply with

Note 1 to entry: For the purposes of this document, legal requirements and other requirements are those relevant to the *OH&S management system* (3.11).

Note 2 to entry: "Legal requirements and other requirements" include the provisions in collective agreements.

Note 3 to entry: Legal requirements and other requirements include those that determine the persons who are w*orkers'* (3.3) representatives in accordance with laws, regulations, collective agreements and practices.

CAB - Conformity Assessment Bodies
CMS – Compliance Management System
QMS – Quality Management System
S&R – Statutory & Regulatory Requirements

Guidance on selected words used in the ISO 9000 family of standards

6 Source References:

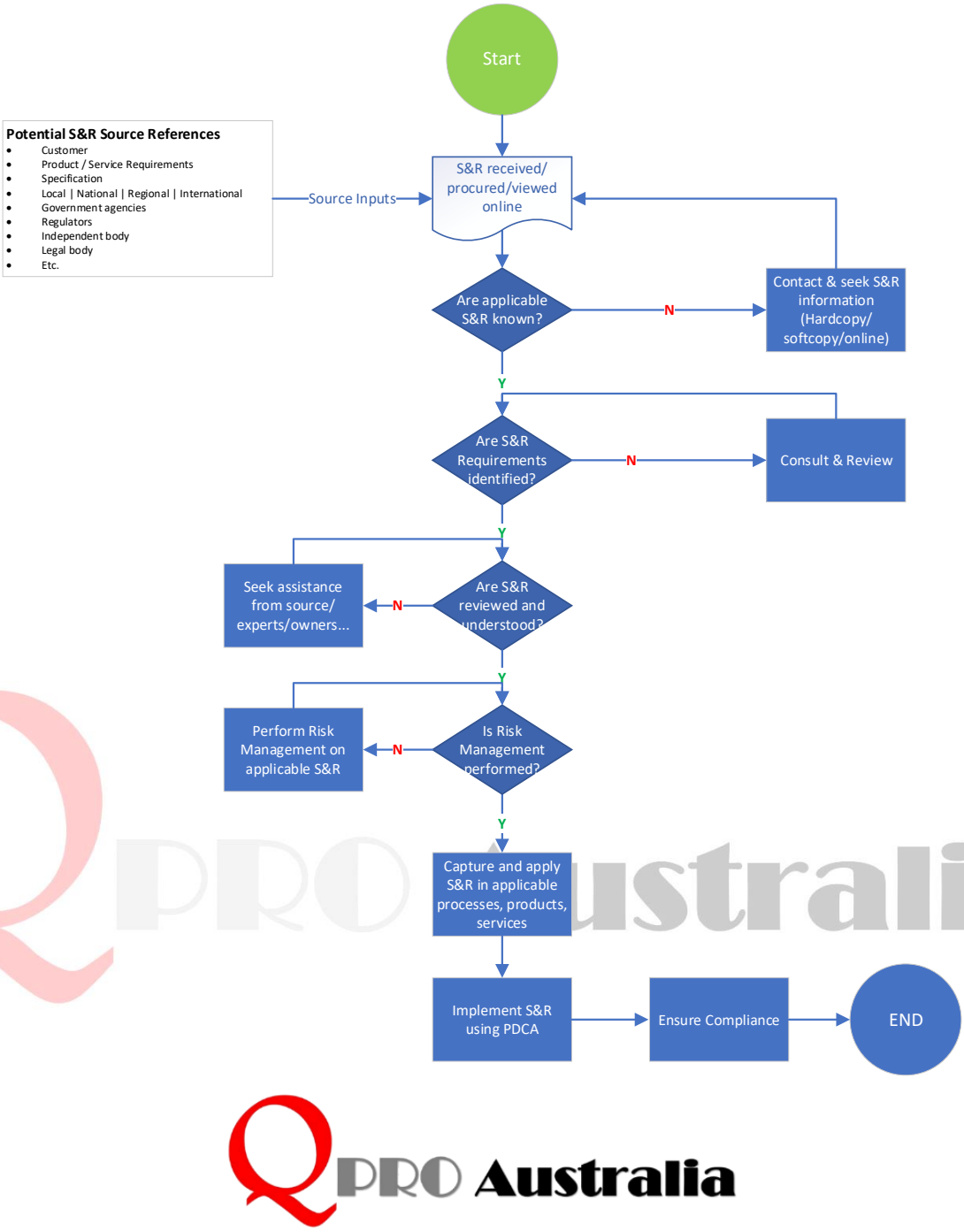
- ISO 9000:2015 Quality management systems — Fundamentals and vocabulary
- ISO 9001:2015 Quality management systems — Requirements
- ISO 14001:2015 Environmental management systems —Requirements with guidance for use
- ISO 45001:2018 Occupational health and safety management systems — Requirements with guidance for use
- ISO 19011:2018 Guidelines for auditing management systems
- ISO 37301:2021 Compliance management systems — Requirements with guidance for use
- 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
- Glossary – Guidance on selected words used in the ISO 9000 family of standards

ANNEX A - Context of auditing statutory and regulatory requirements within ISO 9001:2015

ISO 9001 Clause	Clause Title	Context for the auditors
4.1	Understanding the Organisation and its Context	The organisation 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 organisation. During the audit the interactions between the organisation 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/customer 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 organisation (see 4.2 – Annex A).
8.2.3	Review of the requirements for products and services	Auditors should collect evidence of the organisation'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 catalogues, 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 organisation 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 organisation ensures that applicable S&R requirements are determined, acknowledged, and managed by the supplier, and that the organisation 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.

ANNEX B – S&R Assurance Process example (Demo)



This information is intended to provide the reader and the organisation a brief awareness about the AUDITING ASPECTS of applicable Statutory & Regulatory (S&R) requirements to ensure compliance depending on the type of business the organisation operates. The article is a guidance to assure that organisation with or without a management system certification, still have to proactively support and comply to applicable S&R requirements. The S&R requirements information and references in this article are current at the time of publication. The contents of this document should not constitute legal advice and legal advice should be sought as required.