Annex C
(informative)

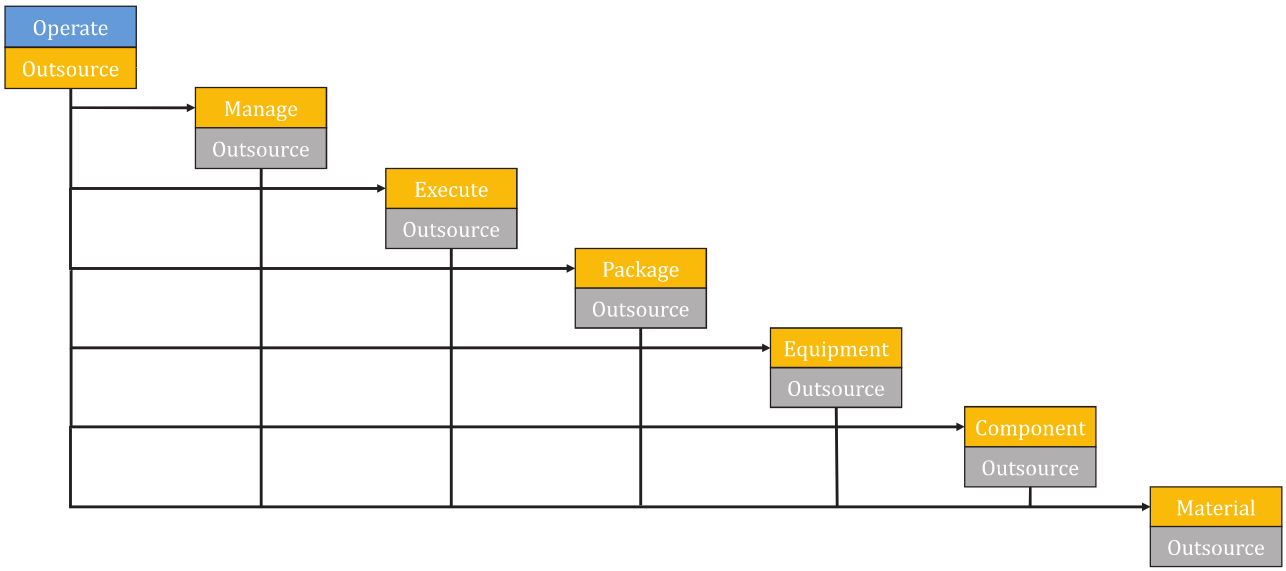
Risk and opportunity management and conformity assessment processes

C.1 General

When an organization wishes to obtain a product or service to be delivered internally or externally, the organization specifies the requirements to be met. It can also specify conformity assessment requirements.

This annex provides methods for assessing risk to the achievement of specified requirements and to the realization of improvement opportunities, and for planning the controls to be put in place by providers to assure conformance with specified requirements, including externally provided products and services in accordance with 8.1 and 8.4.

At any level in the supply chain, the organization can elect to provide products and services using their own processes or to place contracts via a management or execution contractor or directly to package, equipment, component or material providers. Figure C.1 illustrates this cascading contracting model.

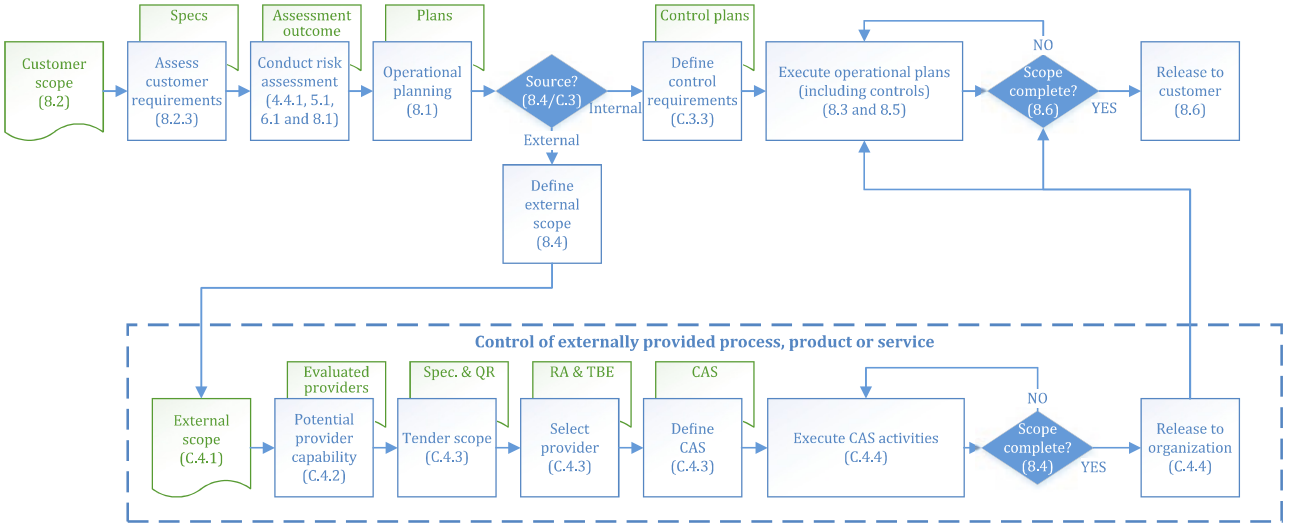


NOTE An operator (blue box) can decide to contract an external provider at any level in the supply chain. Similarly, any other organization in the supply chain (orange boxes) can provide the contracted process, product or service themselves or decide to (partly) outsource these activities.

Figure C.1 — Cascading contracting model

Recognizing that providers of externally provided processes, products and services use their quality management systems to ensure requirements are met and their delivery is assured, the organization should assess and manage the associated risks consistent to the role/scope played by their selected providers of product and/or service in accordance with 8.4.2.

The methodology is designed to be deployed and cascaded down through the supply chain as illustrated in Figure C.2.



NOTE QR is quality requirement, RA is risk assessment, TBE is technical bid evaluation, and CAS is conformity assessment system.

Figure C.2 — Representation of risk management and conformity assessment process

C.2 Risk classification principles

For the purposes of this document, the following risk classification principles apply.

a) Risk classification should be determined taking account of the total life of the product or service, starting with the specified requirements and ending with its product decommissioning and/or service completion.

b) Risk classification should take account of the health, safety and environmental requirements valid for the country or countries in which the product or service is created, used and/or decommissioned/completed.

c) Risk classification should be determined using defined parameters.

d) Risk management should be undertaken by personnel experienced and knowledgeable in the scope of the product or service, including:

— identification and management of failure consequences;

— where relevant, engineering, manufacturing, execution and maturity/complexity;

— previous failures and lessons learnt.

NOTE See 7.1.6 regarding sources of organization knowledge.

C.3 Risk management and conformity assessment process

C.3.1 Customer's scope and context

The customer's specified requirements for the product and/or service (see 8.2) provide the input for operational planning and control. In planning the delivery and control, the organization should consider:

— the product or service to be evaluated;

— the application in which it will be used;

— the design, production and service delivery processes to be employed;

— those activities to be provided externally;

— any customer or obligatory requirements.

C.3.2 Undertaking risk assessment

The organization should undertake risk assessments in accordance with 6.1 to determine the risks associated with the proposed product or service delivery processes. Risk assessments should consider, as applicable, the following categories of risks to the achievement of specified requirements and to the realization of improvement opportunities:

— obligatory requirements;

— health and personal safety;

— process safety;

— environment;

— capital expenditure (CAPEX);

— operational expenditure (OPEX);

— operations with non-productive time or deferred production;

— competence during use;

— competence during design, manufacturing or execution;

— externally provided processes, products or services.

For special services and for materials and equipment, risk assessments should also consider the following risk categories:

— intended use and reasonably foreseeable misuse;

— field-proven design or configuration;

— reliability and maintainability requirements;

— design/service maturity and complexity;

— past use of the same product, process or service;

— certification and traceability requirements.

The organization should develop a risk assessment process that defines the factors to be considered in evaluating risks and for documenting the assessment outcomes.

Risk assessment should be led by a competent facilitator supported by technical, quality, safety and operational specialists and relevant internal and external stakeholders. Risk assessment may be achieved through facilitated workshops, interviews, studies.

NOTE See IEC 31010 for risk assessment techniques that can be employed.

The output of risk assessment can be a ranking of risk based on:

— consequences of the event;

— likelihood of occurrence;

— failure mode detectability.

Further guidance/tools on risk assessment processes are available in electronic format via https://standards.iso.org/iso/29001/ed-1/en to assist determining conformity levels.

NOTE ISO 31000, ISO 31004 and IEC 31010 also provide guidance/tools for determining conformity levels.

C.3.3 Determination of control and conformity assessment requirements

The organization should review planned product and service delivery processes and the outcomes of risk assessments as the basis for defining control and conformity assessment requirements, to provide the basis for ensuring conformance with requirements.

The control and conformity assessment requirements should address:

a) internal operations as per 8.3, 8.5 and 8.6;

b) externally provided processes, products and services as per 8.4 and C.4;

c) the context under which control and assessment activities are invoked, including:

- first-party conformity assessment activities undertaken by the organization;
- second-party conformity assessment activities undertaken by or on behalf of the customer;
- third-party conformity assessment activities undertaken by an independent body to meet customer or obligatory requirements.

Documented information established to define the control and conformity assessment requirements (see 8.1) should include provisions for customer and independent conformity assessment requirements and obligations.

NOTE The provider remains responsible for operational planning and control and demonstration of the conformity of products and/or services with requirements (see 8.1 and 8.2), regardless of conformity assessment requirements defined by the customer, either by reference to standard/specification requirements or in the scope.

C.4 Control of externally provided processes, products and services

C.4.1 Scope of externally provided activity

The organization should define and manage the delivery of the scope for each externally provided process, product or service in accordance with 8.4.

C.4.2 Potential provider capability evaluation

The organization should evaluate potential providers to determine their capability to meet the scope requirements and that they have the pre-requisite (quality) management system controls to ensure that requirements are met. Considerations may include product or service complexity and the need for the organization's involvement during design, manufacturing and supply chain for the products or services, taking into account:

- design novelty of the products or services (e.g. ranging from modification of proven/tested design to redesign to new design of complex item);
- manufacturing complexity of the products or services (e.g. ranging from mass produced to singular runs that require prototypes, complex assembly and test requirements);
- requisites for preserving goods intended for use in petroleum or natural gas specific activities (e.g. elastomeric components or chemicals);
- supply chain knowledge, risk ownership and accountability, number and type of supply avenues (e.g. multiple layers of subcontracting, complex or unclear sources of component supply);

— providers present resource and proposed facility capabilities.

Evaluation of potential provider capability may be based on prior performance, prequalification or audit.

C.4.3 Conformity assessment requirements for external providers

Conformity assessment requirements specified in information for external providers per 8.4.3 should reflect the outputs of the risk assessment in relation to the scope (see C.3) and include definition of:

— control activities defined by the contract and/or specifications and, where applicable, a defined quality specification level (QSL);

— intended level of assessment of provider's control activities by the customer and when applicable, independent bodies, through nomination of a conformity assessment system (CAS).

The technical bid evaluation (TBE) including evaluation of the providers' capability to conform to the specification and associated QSL should be used to confirm or amend the CAS to be applied to the selected provider and reflected in the contract per 8.4.3.

Examples of approaches to defining conformity assessment requirements are available in electronic format via http://standards.iso.org/iso/29001.

C.4.4 Control of external providers during execution of scope

The organization should undertake planned conformity assessment activities as a prerequisite to release of an externally provided process, product or service for incorporation in its operations as per agreed conformity assessment requirements.

In the context of this document, conformity assessment requirements are typically managed as:

— Hold (H): Point in the chain of activities, defined in agreed documented information, that requires the approval of the customer or designated authority before proceeding.

— Witness (W): Point in the chain of activities, in which the customer or designated authority can witness the operation or process within an agreed timeframe after notification and according to a method, which is defined in agreed documented information.

— Surveillance (S): Point for the periodic observation or monitoring by the customer or its representative or designated authority of an activity, operation, process or documented information at provider's or external provider's premises.

— Review (R): Point for determination of the suitability, adequacy or effectiveness of documented information to verify conformance to agreed requirements and obligations.

Provider performance in meeting the requirements should be routinely assessed during execution of the scope and, where appropriate, corrective action implemented and the level of conformity assessment adjusted consistent with risk.

C.5 Example of conformity assessment activities

Table C.1 provides a matrix for generic conformity assessment activities and their application across four conformity assessment systems or levels of customer intervention based on assessed risk and opportunity.

Table C.1 — Generic conformity assessment activities matrix (adapted from ISO/TR 13881:2000)

CUSTOMER ASSESSMENT ACTIVITIES	CONFORMITY ASSESSMENT SYSTEM (decreasing supply risk)[a] →			
	A	B	C	D
Operational planning and control activities (8.1)				
Post award clarification (8.2)	H	W		
Risk assessment	H	W	R	
Operational planning and processes	H	W	R	
Control planning	H	W		
Design and development activities (8.3)				
Design and development planning (8.3.2)				
Design reviews	H	R		
Design verification	H (3)	R (3)		
Design validation	H (3)	R (3)		
Control of external supply (8.4)				
External supply scope, risk assessment and controls (8.4, C.4)	H	W	R	
Execution of external assessment activities	W	S	S	
Release to organisation	H	W	S	
Production and service provision (8.5)				
Process qualification	H	R	S	
Product, process or service surveillance by:				
— Periodic inspection	H	S	S	S
— Inspection of samples	W	S	S	
— 100 % inspection	W	S		
Release of product or service (8.6)				
Final inspection	H	W		
Providers declaration of conformity	H	W	R	R
Independent certification	H (3)	H	R	

[a] H is hold point, R is review, S is surveillance, and W is witness point.

Suffix "3" indicates third party conformity assessment activities.