TECHNICAL SPECIFICATION

ISO/IEC TS 30105-6

First edition
2021-10

Information technology — IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes —

Part 6: Guidelines on risk management

Reference number
ISO/IEC TS 30105-6:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Risk principles **2**
4.1 Outcomes 2
4.1.1 General 2
4.1.2 Value creation and protection 2
4.2 Principles 2
4.2.1 Integrated risk management 2
4.2.2 Structured and comprehensive 3
4.2.3 Customized 3
4.2.4 Inclusive 3
4.2.5 Dynamic 3
4.2.6 Best available information 3
4.2.7 Human and cultural factors 4
4.2.8 Continual improvement 4

5 Risk management framework **4**
5.1 General 4
5.2 Risk management framework design 5
5.2.1 General 5
5.2.2 Context 5
5.3 Risk culture 6
5.4 Risk management framework implementation 6

6 Risk management process **6**
6.1 General 6
6.2 Scope, context and criteria 7
6.2.1 General 7
6.2.2 Scope 7
6.2.3 External and internal context 7
6.2.4 Criteria 8
6.3 Risk assessment 8
6.3.1 General 8
6.3.2 Risk identification 9
6.3.3 Risk analysis 9
6.3.4 Risk evaluation 10
6.4 Risk treatment 10
6.4.1 General 10
6.4.2 Risk mitigation 10
6.4.3 Risk avoidance 10
6.4.4 Risk transfer 11
6.4.5 Risk retention 11

7 Communication and reporting **11**

8 Monitoring and review **12**
8.1 General 12
8.2 Monitoring and management review 12
8.2.1 Monitoring 12
8.2.2 Management review 13
8.3 Key risk indicators (KRIs) 13

Annex A (informative) **Case study** **15**

Annex B (informative) **Indicative governance structure for risk management** **17**
Bibliography **18**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 40, *IT Service Management and IT Governance*.

A list of all parts in the ISO/IEC 30105 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

ITES-BPO services encompass the provision of one of more IT-enabled business processes by a service provider. Such a service provider manages the outsourced business processes in accordance with agreed contractual arrangements. This covers diverse business process areas such as finance, human resource management, administration, healthcare, banking and financial services, supply chain management, travel and hospitality, media, market research, analytics, telecommunication, manufacturing, etc. These services provide business solutions to customers across the globe and form part of the core service delivery chain for customers.

In an ITES-BPO service provider organization, risks are prevalent due to the nature of the services that are outsourced to service providers. Risks can be financial, regulatory, reputational, technological, etc. These risks can impact the ITES-BPO organization, customers and other interested parties. Thus, it is necessary for an ITES-BPO organization to incorporate the management of these risks within their risk management framework. A process should be in place to assess, treat, communicate, monitor and report risks, with the goal of creating and protecting value for the organization, customers and end-users.

The changing environment in the ITES-BPO service sector is leading to many challenges, including:

— heightened oversight by global regulators of outsourcing engagements;

— changes to regulations;

— non-sequential process automations, leading to additional risk imposed on customers;

— non-conformance resulting in fines/sanctions in certain business segments or processes.

Therefore, managing risk effectively helps ITES-BPO organizations to perform well in an environment of uncertainty.

These guidelines are intended to help an ITES-BPO organization improve their risk management practices by providing sound principles for effective risk management.

In addition, these guidelines are intended to support the effective implementation of the risk management process within the ISO/IEC 30105 series through:

— risk assessment, including identification, analysis and evaluation at an early stage, and at regular intervals, to determine risk levels and required controls to provide assurance for ITES-BPO organizations;

— appropriate risk treatments;

— awareness of the required controls and adherence;

— risk governance for monitoring, effective treatment and communication;

— recording and reporting;

— scanning environments for emerging risks.

Throughout this document, the term "ITES-BPO organizations" refers to ITES-BPO service provider organizations.

Information technology — IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes —

Part 6: Guidelines on risk management

1 Scope

This document provides guidance on risk management practices for the IT enabled services-business process outsourcing (ITES-BPO) service provider for the outsourced business processes. It provides guidance for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and improving the risk management framework for the ITES-BPO services.

This document:

— covers IT enabled business processes that are outsourced;

— is applicable to the service provider;

— is applicable to all lifecycle processes of ITES-BPO;

— is not intended to cover IT services.

The guidelines in this document align to ISO 31000, elaborating the risk principles, risk management framework and risk management process from an ITES-BPO perspective.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO Guide 73, *Risk management — Vocabulary*

ISO 31000:2018, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO Guide 73 and ISO 31000 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Risk principles

4.1 Outcomes

4.1.1 General

The risk principles described in ISO 31000 can be applied in the context of ITES-BPO to ensure a consistent, effective, efficient and economical approach to risk management. The risk management principles facilitate the effective planning, managing and treating of risks. They provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. These principles should enable an organization to manage the effects of uncertainty on its objectives.

A risk management framework should exist to contribute to the achievement of objectives for both the service provider and the customer. The purpose of the risk management framework is to increase the awareness of both existing and emerging risks. Knowledge of these risks, combined with risk management processes, should enable both organizations to take appropriate and timely mitigation/ reduction measures.

4.1.2 Value creation and protection

There are certain risks inherent in the ITES-BPO industry due to the nature of the services and the engagement model.

It is important that the risk management framework is designed to manage the risks for all parties to the outsourcing arrangement in an open, transparent and mutually beneficial way.

A key input into strategic decision-making in ITES-BPO services is comprehensive risk assessment, based on external intelligence and internal processes, enabling risks to be addressed and treated.

For example, creating market differentiation for the customer by enhancing the business process with systemic controls beyond managing the business process.

4.2 Principles

4.2.1 Integrated risk management

The ITES-BPO organization has an inherent need to recognize the integrated nature of its relevance with its customers. Integration from an ITES-BPO organization's perspective has to consider both the internal organization risk management framework as well as customers' risk management requirements and how these interfaces and interact. The risks arising from an ITES-BPO organization will influence the risk profile of the customer.

An ITES-BPO organization's risk management programme has to ensure all strategic, tactical and operational risks are identified and managed for the IT-enabled business processes delivered. In addition, it is necessary for risk management to be integrated to cover the entire outsourcing lifecycle of each customer contract.

For example, the ITES-BPO organization governance model for risk and controls proactively aims to identify and evaluate all strategic and tactical risks during pre-contract stage, in order to support decision- making. In addition, at the business process level, all operational risk controls should be part of the detailed business process operating manuals to mitigate risks. The management of risks, and the implementation and monitoring of controls, should not be done in isolation but integrated into the operational delivery controls.

4.2.2 Structured and comprehensive

A risk management approach should be systematic and structured and should operate on a regular basis for the ITES-BPO organization in order to provide consistent and comparable results to the customer and other interested parties.

The risk profile of an ITES-BPO organization is affected by multiple customers and interested parties. This increases the need for the risk management programme implementing critical controls and governance measures to achieve the business objectives of both the service provider and the customers. Additionally, the enhanced risk management processes can be a market differentiator with competitors.

4.2.3 Customized

An ITES-BPO organization should create and maintain a common risk management framework, with the application of the framework customized, for each customer, based on their contractual requirements, geographic needs and product/service-specific requirements. This enables a common risk management approach to be easily and cost effectively integrated.

For example, the data privacy risk treatment practices for a business process should be tailored based on the applicable data privacy requirements of the respective country and/or product for which services are being rendered.

4.2.4 Inclusive

Involving interested parties in risk assessment or risk treatment will ensure that risk management remains current and contextual. ITES-BPO organizations should ensure that customers and other interested parties are regularly appraised of risk treatment status and open or active risks.

For example, the risk management framework formation team should encompass representation from leadership, service delivery, enabling functions, customers and other key interested parties.

In a changing world and business environment, ITES-BPO organizations should create policies that are inclusive and transparent to all interested parties.

4.2.5 Dynamic

The risk management procedures should be dynamic in order to adapt to change (taking into consideration the continuous changes occurring in the industry) and to regulations, technology transformation and contractual requirements. It is therefore important that an ITES-BPO organization regularly monitors risks, along with their controls, and maintains procedures to detect risks arising from change.

For example, for any changes occurring in the regulations, business processes, contractual requirements or technology used, an ITES-BPO organization should assess the risk and undertake appropriate treatment.

4.2.6 Best available information

An ITES-BPO organization will be less effective in decision-making if the data is incomplete. Hence, they should obtain all possible information to understand the risks as conclusively as possible and from a number of perspectives.

For example, identification of all possible process design risks at the time of process migration cannot be fully accurate based only on available data. Historical data and the right expertise, such as inputs from the customer or experts, should be considered. It is also important to determine, and agree with the customer, the methods for collecting or generating data early in the lifecycle of the process.

4.2.7 Human and cultural factors

An ITES-BPO organization's success revolves around human and cultural factors. Therefore, it is important that all aspects of risk are evaluated and managed taking into consideration these human and cultural factors.

For example, the attrition rate or resources availability for recruitment should be considered as key risk factors when selecting a location for delivery of a new business process or existing business process. In addition, most ITES-BPO contracts demand background checks for on-boarding personnel, which should be considered as one of the risks related to human factors.

4.2.8 Continual improvement

Continual improvement is a basic expectation and should be demonstrated through a robust risk management framework and governance model (see Annex B). Risk assessment and governance provide direction for enhancements to the controls and processes. This facilitates improved processes, leading to enhancement of the ITES-BPO organization.

Treating an identified financial risk, relating to high-value fund transfer, by introducing an automated control to assign high-value fund transfer authorizations to a senior authorizer, is an example of how risk management can contribute to or even drive the continual improvement of the organization.

5 Risk management framework

5.1 General

When establishing a risk management framework, ITES-BPO organizations should consider strategic, tactical and operational policies, and contractual requirements and risk principles, as explained in Clause 4 of this document. A risk management framework should cover planning, in terms of setting the right risk environment, monitoring of controls on an ongoing basis and appropriate review. Additionally, ITES-BPO organizations should plan to establish the required culture and awareness: to cascade the importance of active engagement in risk management and adherence to process controls, including potential consequences of failure.

Figure 1 illustrates the different inputs to a risk management framework.

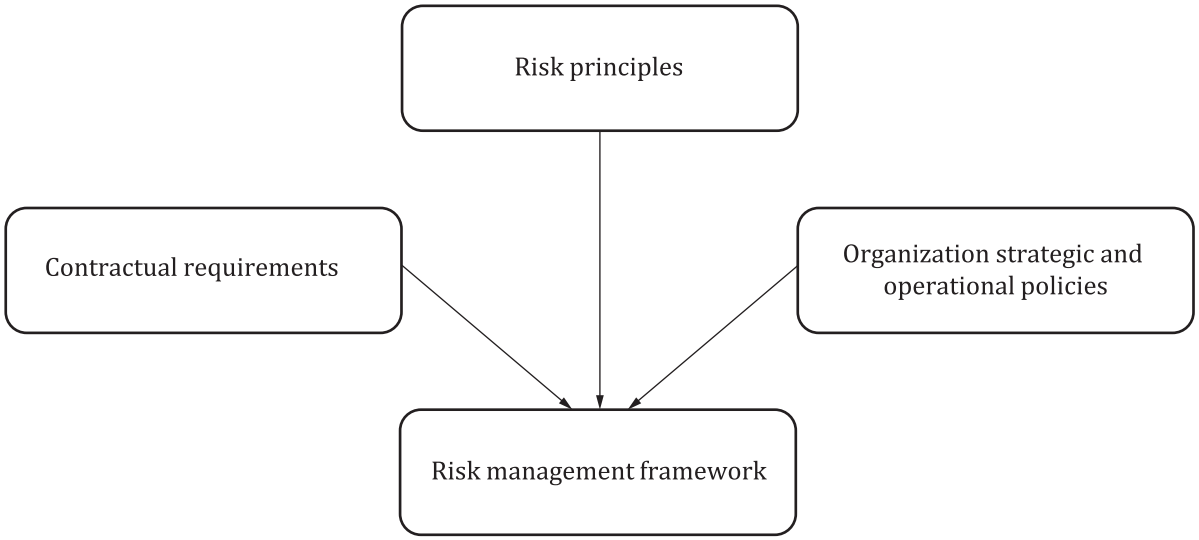

Figure 1 — Inputs to a risk management framework

This framework should ensure that it includes all components, in terms of design, implementation, monitoring, review and improvement of the framework.