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/IEC 2021

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2021 – All rights reserved

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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/

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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.

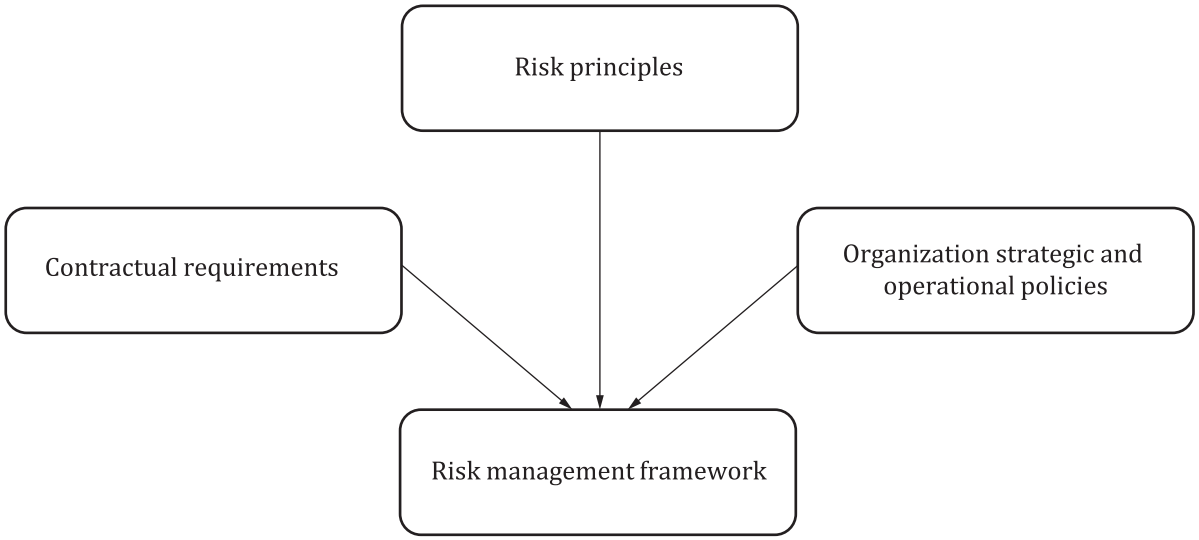

Figure 1 — Inputs to a risk management framework

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

© ISO/IEC 2021 – All rights reserved

Refer to Annex A for a case study on the risk management framework and deployment.

5.2 Risk management framework design

5.2.1 General

The risk management framework sets up the appropriate environment through design, implementation, monitoring and continually improving the risk management framework. It should include a plan, responsibilities and authorities, resources, processes and activities, and be aligned to the objectives of the customer and the ITES-BPO organization.

Top management for the ITES-BPO organization owns the risk management framework design. However, development of the risk management framework should be undertaken collaboratively with interested parties.

The risk management framework should be customized to the objectives and context of the ITES-BPO organization.

5.2.2 Context

The ITES-BPO organization should examine and understand the environment in which it operates, and the internal and external factors that can affect risks or the organizational arrangement needed to manage them.

For example, this can include financial, technical and regulatory factors, relationships with interested parties, and the organization's existing governance organizational structure, roles, responsibilities and authorities.

An ITES-BPO organization should define the risk management framework appropriate for the risks and threats.

Examples of internal threats and issues include:

— any process design or implementation issues identified through internal audits;

— any changes to standard operating procedures or policies, by the customer or the ITES-BPO organization that could impact the service;

— contract-related risks and amendments;

— capacity and scheduling-related challenges and threats to providing timely business services;

— any incidents and threats that could impact the customer or the ITES-BPO organization;

— changes due to adoption of newer or changed technologies and processes by the ITES-BPO organization or the customer.

Examples of external threats and issues include:

— new or changed regulations;

— customer feedback;

— disasters that threaten the continuity of the ITES-BPO service;

— other political, economic or social changes that are relevant.

© ISO/IEC 2021 – All rights reserved

5.3 Risk culture

Risk culture is the system of shared assumptions, values and beliefs that govern risk decisions in the ITES-BPO organization. The culture determines how employees understand and describe the context of their work, and how they recognize, describe and respond to risks.

The risk culture of the ITES-BPO organization should be enhanced to increase staff awareness of customer needs, as well as understanding risk and treatments, as appropriate.

ITES-BPO organizations are people-centric. Therefore, the right risk culture should be developed and maintained.

Risk awareness should be embedded from the day an employee is on-boarded and should continue throughout the term of employment. Employees of the ITES-BPO organization should be aware of the risks associated with their domains and the risk management process followed by the ITES-BPO organization.

Awareness can be driven through training, assessments, campaigns, simulations, continuous communications, etc. This should be an ongoing process.

Leadership should invest and continuously reiterate the importance of risk management to their employees. Risk management is the responsibility of all employees, starting at entry level.

5.4 Risk management framework implementation

An ITES-BPO organization should define a detailed plan for implementing the risk management framework, including plans for design, implementation, monitoring and review.

The required resources for assessing and implementing the risk management framework should be determined, including the required competencies. Resource provisioning and retention improves implementation effectiveness for the risk management framework.

A risk assessment should be performed in line with the plan, and the results should be shared with interested parties for action and review.

Reviews should be scheduled and implemented at a defined interval to evaluate the implementation status. Implementation should be integrated into the change management process to assess the implementation impact, plan the deployment and gain approval from required approvers.

Once the risk management framework is implemented, it should be monitored for effectiveness.

6 Risk management process

6.1 General

The risk management framework should define the risk management process. The subsequent subclauses consider each component of the risk management process in the context of ITES-BPO.

The risk management process is illustrated, at a high level, in Figure 2.

An ITES-BPO organization should define the roles, responsibilities and authorities to ensure effective implementation of the risk management framework.

Refer to Annex B for an illustrated structure with three lines of defence for effective risk management.

© ISO/IEC 2021 – All rights reserved

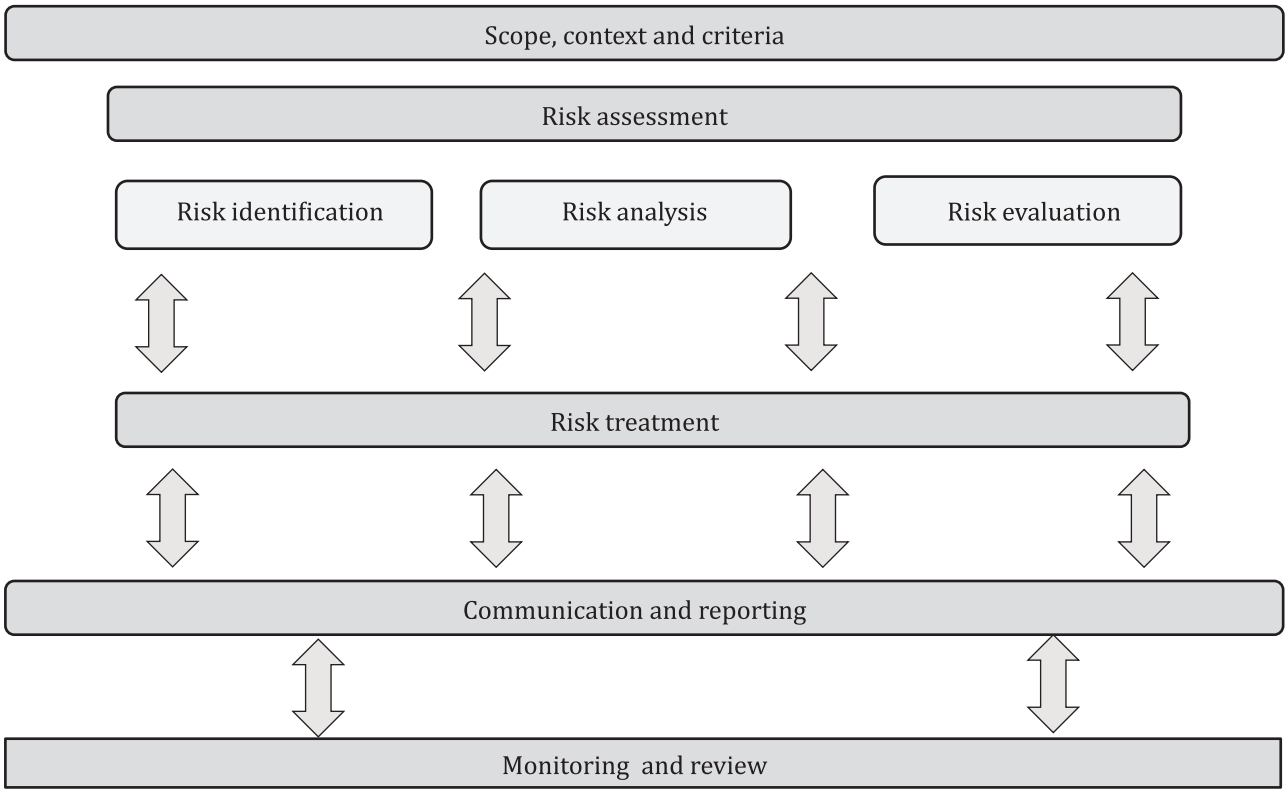

Figure 2 — High-level risk management process

6.2 Scope, context and criteria

6.2.1 General

Scope, context and criteria need to be defined based on an understanding of external and internal factors. This helps in customizing the risk management process in line with the organization and customers' objectives and risk appetite.

6.2.2 Scope

The ITES–BPO organization should define the objectives of each application of the risk management process, its boundaries and its scope. This should be documented to provide assurance that risk management is comprehensive, effective and efficient.

6.2.3 External and internal context

Risk management process should consider the following:

a) external intelligence on the current threats and vulnerabilities in the market, developments and/or customer expectations;

b) internal inputs for capability, risk exposure and severity.

While establishing the risk management process, those undertaking a risk assessment should understand the internal and external context, such as:

— contractual obligations with customers;

— risk appetite;

© ISO/IEC 2021 – All rights reserved

— risk tolerance level;

— nature and criticality of the services;

— associated business process;

— committed service level agreements (SLAs);

— relationships with other projects, processes and activities.

NOTE Risk appetite is the statement defined by top management that expresses how much risk the organization is recommended to take in the pursuit of its objectives. This is operationalized into criteria or a set of rules for decisions relevant to the organization where there can be uncertainty and is defined as part of the framework.

6.2.4 Criteria

The ITES-BPO organization should establish a set of rules or statements that enable decisions about risk to be made in a consistent way. These decisions can include:

— whether a risk needs further treatment;

— when a risk is intolerable and has to be avoided;

— how to allocate resources between risk treatments;

— when an expected benefit is worth the risk;

— how to decide between options, when both involve risk and trade-offs are necessary;

— which risks have particularly high significance.

The relevant criteria can differ according to the decision required. For example, a combination of consequence and likelihood (referred to as level of risk) can be used to determine the risks that have particular significance. However, resources can be allocated on the basis of the cost-benefit of the treatment options for different risks. Intolerability can be based on maximum credible consequence alone.

6.3 Risk assessment

6.3.1 General

Risk assessment is an important activity that should be performed at the initial stage of a new process requirement or a change in existing processes, and at a defined frequency for an ongoing process.

Risk assessment involves meaningful dialogue with customers, reviewing both existing risks, as well as emergent risks.

Risk assessment involves identification, analysis and evaluation of the risks to be treated effectively. These steps are described as follows:

a) risk identification: recognizing and describing risks;

b) risk analysis: understanding the nature and characteristics of risks;

c) risk evaluation: supporting decisions including comparing risks with risk criteria to determine whether additional action is required. The evaluation should aggregate analyzed risk, taking into account level of risk, proximity, manageability, context and the views of the interested parties.

The personnel conducting an assessment should have good domain knowledge and understand the lifecycle of the product or process in the scope of the assessment.

© ISO/IEC 2021 – All rights reserved

6.3.2 Risk identification

Risk identification helps ITES-BPO organizations to understand the potential risks that could impact the achievement of the objectives for a system, an ITES-BPO organization or a customer.

Risk identification should consider the following aspects:

a) identify and classify key risks across a number of different aspects. This can be achieved by building a repository of risks that could impact the achievement of objectives. These include risks from processes, people, customer policies, market and conformance with laws and regulations such as:

   — design and implementation risks;

   — risks identified from applicable regulations for the process or product, and any relevant laws or regulations for the geographical region;

   — risks identified through feedback from customers;

   — risks identified through audits;

   — risks due to changes in the market, environment, processes, regulations and policies;

   — risks related to human resources.

b) identify both controllable and non-controllable risks for the ITES-BPO organization and the customer;

c) ensure that personnel undertaking risk identification are competent;

d) adopt a systematic approach to risk identification. Different tools can be used to achieve this, for example, failure mode and effects analysis (FMEA), a risk prioritization matrix, or the 5 why analysis.

6.3.3 Risk analysis

Risk analysis involves a detailed consideration of:

— sources and causes of risk;

— the events and scenarios that can occur;

— possible consequences and their likelihood;

— the effectiveness of existing controls.

An understanding of causes of risk and scenarios that can lead to these consequences (positive or negative) helps in selecting appropriate treatments and assessing likelihood. Both consequences and likelihood are affected by the effectiveness of existing controls.

Consequences and likelihood can be combined to provide an indication of level of risk. However, by doing this, information is lost (for example, whether a risk is high-consequence and low-likelihood or vice versa). Separate information on possible consequences and their likelihood, and the factors that affect these, can be of more use to the decision-maker than a single value for level of risk.

Risk analysis should consider risk interactions and common causes. The analysis method and its format depends on the nature of the decisions to be made apart from the criteria defined for those decisions.

Risk analysis supports decision-making related to risk and risk treatment strategies, based on the impact, likelihood of occurrence and severity of the consequences. A risk can impact more than one objective. Risk analysis should consider the effectiveness of existing controls for an identified risk. Various techniques can be used for risk analysis.

© ISO/IEC 2021 – All rights reserved

An ITES-BPO organization should share the results of its risk analysis with its customers. This provides the customers with an opportunity to respond and collaborate in risk reduction measures.

6.3.4 Risk evaluation

Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.

The decision of risk treatment can depend on the cost and benefits associated with implementing improved controls.

Decision-making should consider the context of a risk, risk tolerance, and regulatory and financial impact. Decisions can include the type of treatment, priority of treatment and the approach.

Various decision-making techniques can be used for risk evaluation.

For example, a service provider conducting a risk evaluation to decide whether to adopt a new technology or product for the business process in addition to calculating return on investment.

6.4 Risk treatment

6.4.1 General

Risk treatment involves selecting and implementing measures to address risks. Risk treatment measures can include avoiding, mitigating, transferring or retaining risks. Risk treatment includes reduction of the likelihood that a risk event will occur. Risk treatment plans typically cover:

— addressing root causes of identified risks in earlier phases of the risk management process;

— identifying alternative mitigation strategies, methods and tools for each risk;

— assessing and prioritizing treatment alternatives;

— planning for the resources required for specific risk treatment;

— planning for communication of implementation progress and results;

— analyzing the overall impact of a treatment plan and validation.

6.4.2 Risk mitigation

Risk mitigation is one type of risk treatment, introducing new or modified controls to reduce residual risk and its impact on potential occurrences.

For example:

— implementation of dual controls or a quality assessment process to identify and rectify input errors prior to completion of an event to ensure a risk-managed outcome for the end user;

— implementation of authentication and authorization reviews for access control logs.

6.4.3 Risk avoidance

Risk avoidance is a risk treatment that removes the possibility of risk occurrence. Typically, this is achieved through a technology-enabled intervention or complete refresh of the process steps. Impact from similar occurrences can be avoided by opting to:

— stop, postpone or cancel an existing process activity;

— execute in a different manner (e.g. using technology);

© ISO/IEC 2021 – All rights reserved

— divert to a different activity.

For example:

— replacing data entry tasks by automation through optical character recognition (OCR) or a screen-scrape solution to eliminate the risk of data entry errors;

— implementing robotics for data scrubbing and formatting to eliminate the risk of data entry errors.

6.4.4 Risk transfer

Risk transfer is a risk treatment that transfers risk ownership to other parties. This can be achieved by outsourcing the task to a third party, who specializes in the task, or by co-owning the outcome between the ITES-BPO organization and the customer, since the impact of non-conformance will be the same for both the ITES-BPO organization and the customer.

For example:

— sub-contracting specific tasks to parties specializing in the required provision, e.g. an approved manpower third party providing task specific experts;

— sub-contracting to a third party for data or content enrichment.

In both examples, risk ownership is transferred as part of the risk treatment.

6.4.5 Risk retention

Risk retention is a risk treatment when the decision is made to retain the risk or its residual impact. Risk ownership is retained by either the ITES-BPO organization's management or the customer or jointly.

For example:

— identify and prepare customer retaining the risks that cannot be reduced, eliminated or transferred for authorization;

— implement a risk management committee to co-sign residual risks.

Risk retention is an acceptable treatment option. If risk retention is the appropriate treatment, it should be clearly defined, understood, and communicated to all participants.

In general, the cost of managing a risk should be compared with the benefits gained or expected. Cost-benefit assessments should consider all risk perspectives within the risk management framework (see 5.1). It is important to consider all direct and indirect costs, and benefits, whether tangible or intangible, measured in financial or other terms.

7 Communication and reporting

Risks and their proposed treatment plans should be communicated to the interested parties. Lessons from the risk framework, process and incidents should be shared as part of ongoing communication processes. The impact of changes, issues and improvements on risk policy and measures should be analyzed and reported.

Periodic reporting of the outcome of risk assessments and testing should provide the appropriate level of details. The report can include:

— summary of risks tested or assessed and their results;

— identified risks and treatments with trends;

— risk treatment plans, status and trends;

© ISO/IEC 2021 – All rights reserved

— key risk indicators status and trends.

8 Monitoring and review

8.1 General

Monitoring and review are critical elements of risk management processes for ensuring the effectiveness of the process design, implementation and outcomes. These elements will also ensure timely review and treatment of any potential strategic, tactical or operational risk having a significant impact the organization or customer's finances, regulatory conformance or reputation.

An organization needs to continuously monitor and review the appropriateness of the risk criteria, assessment, treatment and management framework throughout the lifecycle of the outsourced process. This should cover all aspects of risk and exposure for customers and the ITES-BPO organization.

The review process should involve all concerned interested parties to ensure input into the ongoing shaping of the risk management processes across all aspects of process, people and technology.

Typically, the following aspects are monitored and reviewed:

— risk framework;

— risk management competencies;

— risk appetite;

— risk tolerance;

— resources;

— any significant risks or exposures;

— independent audit results;

— open and overdue risk treatment plans;

— conformance with corporate policies, customer contracts through internal and external audits;

— incidents;

— future or emerging risks;

— gaps identified by the risk focus forum, with risk treatments and target dates for closure documented;

— effectiveness of controls at defined intervals.

Key risk indicators enable a quantitative approach for monitoring and review of the risk management process.

The ITES-BPO organization needs to implement procedures to actively monitor risks and be able to report on such activities to its customers, thereby building customer trust.

8.2 Monitoring and management review

8.2.1 Monitoring

An ITES-BPO organization's risk management framework and process should be monitored to compare actual performance against the expected performance. Additionally, periodic reviews assure implementation effectiveness and continued suitability to the current environment.

© ISO/IEC 2021 – All rights reserved

An ITES-BPO organization should monitor the sources of risks, the level of risk, effectiveness of the risk control measures and the treatment of risks. Risk monitoring should include periodic review of risks, the controls implemented to mitigate the risks and effectiveness of the controls.

An ITES-BPO organization should perform risk monitoring at an appropriate frequency, covering all key sub-processes, domains, risk families and lines of business or departments.

Risk monitoring responsibilities should be identified and communicated to the relevant interested parties and roles performing this activity. Risk owners are responsible for the efficient conduct of risk monitoring activities and should be able to demonstrate adequate efforts taken towards risk monitoring.

Risk monitoring should cover various elements of the business process, such as risk events (potential and materialized risk events), metrics identified as risk indicators (both lead and lag indicators), controls adequacy, results of control testing and control effectiveness**.**

The ITES-BPO organization should maintain a record of its identified risks. Generally, this includes information about the nature of the consequences and how they can occur, as well as the controls currently in place. The organization should share information about risks pertinent to each customer with that customer.

8.2.2 Management review

A risk management review should be conducted in a systemic and planned manner to continuously review the risk status and provide appropriate direction. A risk management review agenda should include:

— risk environment;

— resources;

— control effectiveness;

— risk criteria;

— risk levels and measures;

— risk treatment status;

— risk exposure;

— emerging risks;

— action status of the previous review meeting.

An ITES-BPO organization should define the roles, responsibilities and authorities to ensure effective implementation of the risk management framework. A risk management review should ascertain whether the risk management practices are sufficiently dynamic to meet the changing needs of the customer, regulations and the ITES-BPO organization’s strategic, tactical and operational policies. The review should focus on the current maturity level of risk management and the opportunities for continual improvement.

The outcome of the review and action status should also be reviewed in subsequent updates.

8.3 Key risk indicators (KRIs)

ITES-BPO organizations operate in a complex environment comprising multiple regulations, different domains, varieties of risks, multiple risk indicators and calculations, multiple service lines and multiple businesses spread across multiple geographies.

© ISO/IEC 2021 – All rights reserved

This can lead to many silos across an ITES-BPO organization with no unified view of risk and impact. In addition, multiple metrics are tracked and reported to multiple interested parties, with no unified reporting across the ITES-BPO organization. This can lead to a cumbersome decision-making process.

To provide a unified view, risk indicators and reporting should be standardized for the decision-makers through the use of key risk indicators (KRIs). KRIs should be specific, measurable, agreed, controllable and reportable. This will identify the key risk exposures for the ITES-BPO organization and the customer.

These KRIs and trends provide information to top management about risks and performance in order to make informed decisions, mitigate/minimize risks and ensure an acceptance level of risks to the organization.

A typical KRI is derived based on the underlying risk of the process. Examples of KRIs are shown in Table 1.

Table 1 — Example KRIs

Example #	Process	Key risk indicator	Threshold
#1	Employee onboarding process	Number of background checks not completed	100 % completion within 90 days
#2	Trade business process	Number of sanctions missed	Zero sanctions missed
#3	Telecom process	Number of calls outside the calling window	Zero calls
#4	Employee off-boarding process	Number of instances of access revocation not completed for exited employees	100 % revocation upon employment/contract termination

© ISO/IEC 2021 – All rights reserved

Annex A
(informative)

Case study

A.1 Background

A large retail organization, XYZ, outsources its payroll processing activity to an ITES-BPO organization, ABC. ABC performs back-office activities, maintaining salary accounts for the XYZ employees. This outsourced service involves debiting bank expense accounts and crediting individual salary accounts for more than 100 000 XYZ employees. XYZ also issues stop pay instructions for a small number of employees when salary accounts are not to be credited, based on specific human resource (HR) function decisions.

A.2 Risk management framework and deployment

ABC has established a risk management framework that requires risk assessment to be undertaken during transition to identify potential risks. ABC appoints a risk task force to perform the risk assessment. Through assessing XYZ's payroll operations process, a number of potential risks are identified.

Some of these identified risks are listed below:

a) double salary credits;

b) missed salary credits;

c) excess or underpayment of salaries;

d) not applying stop pay;

e) delayed salary credits;

f) unauthorized payments to employees who have left XYZ;

g) fraudulent approval for salary credit;

h) personal data breach such as salaries disclosure.

The risk task force shares the risk assessment report with the payroll operations team, top management and XYZ. Post-analysis and evaluation, the payroll operations team recognizes the identified risks and potential impacts and creates a set of controls to mitigate them. Some of the sample controls initiated by the payroll operations team, with approval and support from XYZ, are:

1) review of authorizations through approved delegation matrices;

2) review of stop pays through checker control;

3) systemic controls to act as deterrents;

4) duplicate processing alerts;

5) supervisory controls for high-value credits;

6) staff training in privacy and security controls, and non-disclosure agreements.

© ISO/IEC 2021 – All rights reserved

ABC establishes employee awareness training on the risks associated with payroll processing, consequences and the importance of controls. ABC runs periodic campaigns to reinstate the risk culture and rewards employees for proactive identification of risks in the process.

ABC believes in monitoring and reviewing controls continually, to ensure customers are not impacted and customer satisfaction is achieved.

ABC deploys a periodic review of controls and measures, such as number of complaints reported by customer, number of inactive bank accounts and number of exited employees. Additionally, ABC periodically reviews the effectiveness of the implemented controls.

ABC management conducts quarterly reviews to assess the control metrics and the health of the process.

These activities enable ABC to achieve the objective of higher customer satisfaction and zero risk incidents.

© ISO/IEC 2021 – All rights reserved

Annex B
(informative)

Indicative governance structure for risk management

Figure B.1 illustrates a sample risk management structure that uses three lines of defence to govern and control risk.

Figure B.1 — Indicative governance structure for risk management

Level 1: This is referred to as the first line of defence. These are functions that own and manage risks. This is the operations management control team that consists of the business owners responsible for identifying and managing risks and executing actions to manage and treat them.

Level 2: This is referred to as the second line of defence. These are functions that oversee or specialize in conformance of the management of risk. They comprise the risk oversight groups established by management function (e.g. enterprise risk management, conformance functions and legal). They provide the policies, frameworks, tools, techniques and support to enable risks and conformance to be managed at the first level.

Level 3: This is referred to as the third line of defence. These are functions that provide independent assurance. Their main role is to ensure that the first two levels are operating effectively. This is achieved by providing an evaluation, through a risk-based approach, on the effectiveness of governance, risk management and internal controls to the ITES-BPO organization's top management/risk committee.

© ISO/IEC 2021 – All rights reserved

Bibliography

[1] IEC 31010, *Risk management — Risk assessment techniques*

[2] ISO/IEC 30105-1, *Information technology — IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes — Part 1: Process reference model (PRM)*

[3] ISO/IEC 30105-2, *Information technology — IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes — Part 2: Process assessment model (PAM)*

[4] ISO/IEC 30105-4, *Information technology — IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes — Part 4: Terms and concepts*

[5] ISO 31022, *Risk management — Guidelines for the management of legal risk*

[6] ISO/TR 31004, *Risk management — Guidance for the implementation of ISO 31000*

© ISO/IEC 2021 – All rights reserved

ICS 35.020

Price based on 18 pages

© ISO/IEC 2021 – All rights reserved