INTERNATIONAL STANDARD
ISO 31000

First edition
2009-11-15

Risk management — Principles and guidelines

Международный Стандарт
ISO 31000

Первое издание
2009-11-15

Риск Менеджмент – Принципы и руководства

Contents

Содержание

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 31000 was prepared by the ISO Technical Management Board Working Group on risk management.

Предисловие

ISO (International Organization for Standardization – Международная Организация по Стандартизации) является всемирной федерацией национальных органов по стандартизации (органов-членов ISO). Работа над подготовкой Международных Стандартов выполняется, как правило, техническим комитетом ISO. Каждый орган-член ISO, заинтересованный в цели, для которой был создан технический комитет, имеет право быть представленным в данном комитете. Международные организации, правительственные и неправительственные, поддерживающие связь с ISO, также принимают участие в работе. ISO также тесно сотрудничает с Международной Электротехнической Комиссией (IEC), ведется совместная работа по всем вопросам электротехнической стандартизации. Международные Стандарты составляются в соответствии с правилами, изложенными в Директивах ISO/IEC, Часть 2.

Основной целью технического комитета является подготовка Международных Стандартов. Проекты Международных Стандартов направляются техническим комитетом органам-членам ISO для голосования. Публикация документа как Международного Стандарта происходит только после одобрения как минимум 75% голосовавших органов-членов ISO.

Особое внимание уделено тому, что некоторые элементы данного документа могут являться предметом патентных прав. ISO не должна нести ответственность за их идентификацию или все подобные патентные права.
Стандарт ISO 31000 был подготовлен ISO Technical Management Board Working Group (Группой Технического Руководства) по управлению рисками.

Introduction

Organizations of all types and sizes face internal and external factors and influences that make it uncertainwhether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is “risk”.

All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and thenevaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria.Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this International Standard establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and

Введение

Организации всех типов и размеров сталкиваются с внутренними и внешними факторами и влияниями, из-за которых становится невозможно определить, каким образом и когда они достигнут своих целей. Влияние неопределенности на цели организации определяется как “риск”.

Любая деятельность организации связана с риском. Организации управляют риском посредством его идентификации, анализа и последующего решения, следует ли его подвергнуть обработке с целью удовлетворения критериев риска. На протяжении всего процесса организации осуществляю коммуникации и консалтинг с заинтересованными сторонами, управляют и анализируют риск и средства управления, которые модифицируют риск с целью обеспечения того, что последующая обработка риска не потребуется. Данный Международный Стандарт описывает этот систематический и логический процесс в деталях.

В то время как все организации управляют риском до определенной степени, данный Международный Стандарт устанавливает некоторые принципы, при выполнении которых управление рисками становится более эффективным. Данный Международный Стандарт рекомендует организациям развивать, внедрять и постоянно улучшать систему, целью которой является интеграция процесса по управлению рисками с руководством, стратегией и планированием, управлением, процессами отчетности, политикой, ценностями и культурой.

Риск менеджмент можно применить к целой организации, к ее площадкам и уровням, в любое время, также как и к определенным функциям, проектам и видам деятельности.

Не смотря на то, что практика риск менеджмента развилась по прошествии длительного времени и в рамках многих отраслей для удовлетворения различных нужд, внедрение последовательных процессов в рамках всесторонней системы может помочь гарантировать, что риск управляется эффективно, рационально и последовательно во всей организации. Общий подход, описанный в данном Национальном Стандарте, изображает принципы и руководства для управления любой формой рисков систематическим и прозрачным

guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of "establishing the context" as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this International Standard are shown in Figure 1.

When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:

- ✓ increase the likelihood of achieving objectives;
- ✓ encourage proactive management;
- ✓ be aware of the need to identify and treat risk throughout the organization;
- ✓ improve the identification of opportunities and threats;
- ✓ comply with relevant legal and regulatory requirements and international norms;
- ✓ improve mandatory and voluntary reporting;
- ✓ improve governance;
- ✓ improve stakeholder confidence and trust;
- ✓ establish a reliable basis for decision making and planning;
- ✓ improve controls;
- ✓ effectively allocate and use resources for risk treatment;
- ✓ improve operational effectiveness and efficiency;

способом для любой области и любого контекста.

Каждая определенная область риск менеджмента применима к индивидуальным нуждам, аудитории, восприятию и критериям. Поэтому главной особенностью данного Международного Стандарта является "установление контекста" как мероприятия в начале общего процесса управления рисками. Установление контекста зафиксирует цели организации, условия, при которых организация пытается достичь своих целей, заинтересованные стороны и разнообразие критериев риска – каждый из которых поможет выявить и оценить природу и сложность риска организации.

Отношение между принципами управления риском, системой, в которой оно появляется и процессом управления рисками описано в данном Международном Стандарте, как показано на рис. 1.

Когда система внедрена и поддерживается в соответствии с Международным Стандартом, управление рисками позволяет организации:

- ✓ Увеличить вероятность достижения целей
- ✓ Поддерживать упреждающее управление
- ✓ Улучшить финансовую отчетность
- ✓ Улучшить осведомленность о необходимости идентифицировать и обрабатывать риск во всей организации
- ✓ Улучшить идентификацию возможностей и обработки рисков
- ✓ Соответствовать релевантным законодательным требованиям и регламентам, а также международным нормам
- ✓ Улучшить деятельность управления
- ✓ Усилить доверие заинтересованных сторон
- ✓ Установить надежную основу для принятия решений и планирования
- ✓ Улучшить контроль
- ✓ Эффективно распределить и использовать ресурсы для обработки риска
- ✓ Улучшить оперативную эффективность и результативность
- ✓ Улучшить показатели профессиональной безопасности и здоровья, а также экологические показатели
- ✓ Улучшить предупреждение потерь и действия по ликвидации последствий происшествий

- ✓ enhance health and safety performance, as well as environmental protection;
- ✓ improve loss prevention and incident management;
- ✓ minimize losses;
- ✓ improve organizational learning; and
- ✓ improve organizational resilience.

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

a) those responsible for developing risk management policy within their organization;
b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;
c) those who need to evaluate an organization's effectiveness in managing risk; and
d) developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this International Standard.

In this International Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, while “managing risk” refers to applying that architecture to particular risks.

- ✓ Минимизировать потери
- ✓ Улучшить обучение на рабочем месте
- ✓ Улучшить работоспособность коллектива

Данный Международный Стандарт предназначен для удовлетворения потребностей широкого круга заинтересованных сторон, включая:

- ответственных лиц за развитие политики риск менеджмента в своей организации

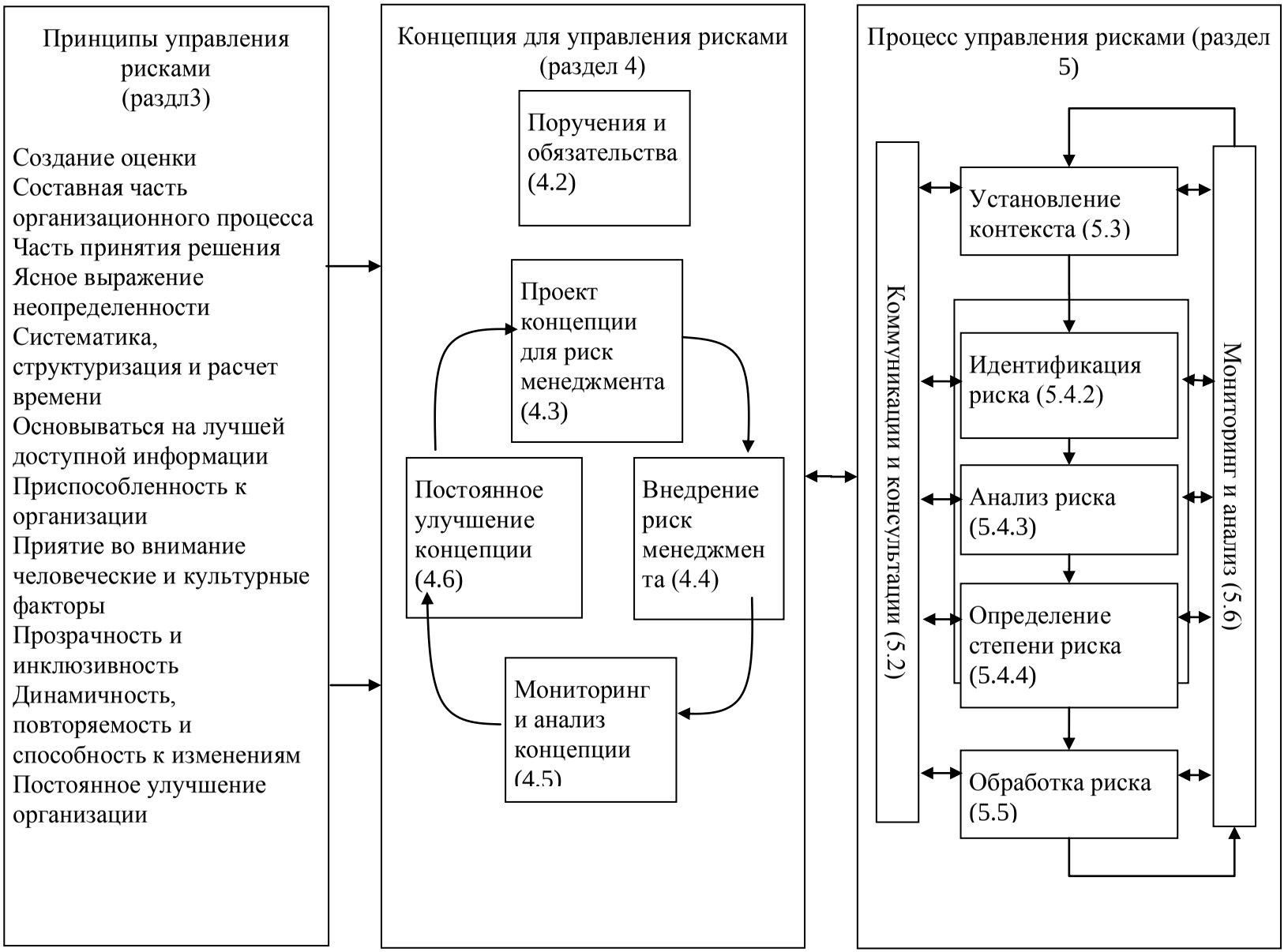
- ответственных лиц за обеспечение того, что риском эффективно управляют во всей организации или в какой-то определенной области, проекте или деятельности

- лиц, которым необходима оценка производительности организации в области управления рисками

- разработчиков стандартов, руководств, процедур и кодексов правил, которые полностью или частично устанавливают, каким образом следует управлять рисками в контексте данного документа.

Текущие процессы управления многих организаций включают компоненты управления рисками, также многие организации уже официально приняли формальные процессы управления рисками для особых типов рисков или обстоятельств. В подобных случаях организация может выполнять анализ существующих практик и процессов в свете данного Международного Стандарта.

В данном Международном Стандарте используются выражения «риск менеджмент» и «управление риском». Сформулированное в общем смысле, выражение «риск менеджмент» относится к «архитектуре» (т.е. принципам, условиям и процессам) эффективного управления рисками, при этом выражение «управление риском» относится к применению данной архитектуры к определенному риску.


Принципы управления рисками (раздл3)
Создание оценки
Составная часть организационного процесса
Часть принятия решения
Ясное выражение неопределенности
Систематика, структуризация и расчет времени
Основываться на лучшей доступной информации
Приспособленность к организации
Приятие во внимание человеческие и культурные факторы
Прозрачность и инклюзивность
Динамичность, повторяемость и способность к изменениям
Постоянное улучшение организации
Концепция для управления рисками (раздел 4)
Поручения и обязательства (4.2)
Проект концепции для риск менеджмента (4.3)
Внедрение риск менеджмен та (4.4)
Мониторинг и анализ концепции (4.5)
Постоянное улучшение концепции (4.6)
Процесс управления рисками (раздел 5)
Коммуникации и консультации (5.2)
Установление контекста (5.3)
Идентификация риска (5.4.2)
Анализ риска (5.4.3)
Определение степени риска (5.4.4)
Обработка риска (5.5)
Мониторинг и анализ (5.6)

Risk management — Principles and guidelines

1 Scope

This International Standard provides principles and generic guidelines on risk management.

This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.

NOTE For convenience, all the different users of this International Standard are referred to by the general term “organization”.

This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks

Риск менеджмент – принципы и руководства

1. Область применения

Данный Международный Стандарт предоставляет принципы и концептуальные руководства по управлению рисками.

Данный Международный Стандарт может быть использован любым государственным, частным или общественным предприятием, ассоциацией, группой компаний или отдельной компанией. Поэтому данный Международный Стандарт может официально принять любая индустрия или область деятельности.

ПРИМЕЧАНИЕ: для удобства все пользователи данного Международного Стандарта в данном документе обозначаются термином «организация».

Данный Международный Стандарт может быть применим на всем протяжении жизненного цикла организации, а также к широкому спектру деятельности, включая стратегии и решения, операции, процессы, функции, проекты, продукцию, услуги и активы.

Данный Международный Стандарт может быть применим к любому типу рисков, независимо от того, какую природу они имеют, а также позитивные или негативные последствия.

Не смотря на то, что данный Международный Стандарт предлагает концептуальные руководящие принципы, его целью не является провозглашение единообразия риск менеджмента во всех организациях. При разработке и внедрении проектов и концепций риск менеджмента следует учитывать различные потребности каждой организации, конкретные цели, контекст, структуру, операции, процессы, функции, проекты, продукцию, услуги и активы, а также практическую работу.

Предполагается, что данный стандарт будет использоваться для согласования процессов по управлению рисками в существующих и будущих стандартах. Он предоставляет общий подход при содействии стандартам, в которых речь идет об особых рисках и/или рисковых

and/or sectors, and does not replace those standards.

This International Standard is not intended for the purpose of certification.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential **events** (2.19) and **consequences** (2.20), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (2.21) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.
[ISO Guide 73:2009, definition 1.1]

2.2
risk management
coordinated activities to direct and control an organization with regard to **risk** (2.1)
[ISO Guide 73:2009, definition 2.1]

2.3
risk management framework
set of components that provide the foundations and organizational

сферах, не заменяя данные стандарты.

Данный Международный стандарт не предназначен для целей сертификации.

2. Термины и определения

В целях данного документа применяются следующие термины и определения:

2.1
Риск
Влияние неопределенности на цели

ПРИМЕЧАНИЕ 1: Влияние рассматривается как отклонение от ожидаемого — с позитивными или негативными последствиями.
ПРИМЕЧАНИЕ 2: Цели могут иметь различные аспекты (такие как финансовые; аспекты, касающиеся профессиональной безопасности и здоровья; экологические задачи) и могут относиться к различным уровням (таким как стратегический уровень, организационный, уровень проекта, продукции и процесса).
ПРИМЕЧАНИЕ 3: риск часто характеризуется отношением к потенциальным **событиям** (2.19) и **последствиям** (2.20) или сочетанию данных пунктов.
ПРИМЕЧАНИЕ 4: риск часто выражается в комбинации последствий событий (включая изменения в обстоятельствах) и связанной с ними **вероятности** (2.21) инцидентов.
ПРИМЕЧАНИЕ 5: неопределенность — это состояние, также частично, отсутствия информации относительно понимания или знания события, его последствий или вероятности.
[Руководство ISO 73:2009, определение 1.1]
2.2
риск менеджмент
скоординированные действия для того, чтобы направлять и контролировать организацию в отношении **рисков** (2.1)
[Руководство ISO 73:2009, определение 2.1]

2.3
концепция риск менеджмента
набор компонентов, которые предоставляют основы и организационные мероприятия для проектирования, внедрения, **мониторинга**

arrangements for designing, implementing, **monitoring** (2.30), reviewing and continually improving **risk management** (2.2) throughout the organization

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage **risk** (2.1).
NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.
NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.
[ISO Guide 73:2009, definition 2.1.1]

2.4
risk management policy
statement of the overall intentions and direction of an organization related to **risk management** (2.2)
[ISO Guide 73:2009, definition 2.1.2]

2.5
risk attitude
organization's approach to assess and eventually pursue, retain, take or turn away from **risk** (2.1)
[ISO Guide 73:2009, definition 3.7.1.1]

2.6
risk management plan
scheme within the **risk management framework** (2.3) specifying the approach, the management components and resources to be applied to the management of **risk** (2.1)
NOTE 1 Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

NOTE 2 The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.
[ISO Guide 73:2009, definition 2.1.3]

2.7
risk owner

(2.30), анализа и постоянного улучшения **риск менеджмента** (2.2) во всей организации

ПРИМЕЧАНИЕ 1: основы включают политику, цели, поручение и обязательство управлять **рисками** (2.1).
ПРИМЕЧАНИЕ 2: организационные мероприятия включают планирование, отношения, отчетность, ресурсы, процессы и деятельность.
ПРИМЕЧАНИЕ 3: концепция риск менеджмента включена в общую стратегию организации, оперативную политику и деятельность.
[Руководство ISO 73:2009, определение 2.1.1]

2.4
политика риск менеджмента
положение общих намерений и направление организации по отношению к **риск менеджменту** (2.2)
[Руководство ISO 73:2009, определение 2.1.2]

2.5
отношение к риску
организационный подход для оценки и своевременного решения, стоит ли идти на **риск** (2.1)
[Руководство ISO 73:2009, определение 3.7.1.1]

2.6
план риск менеджмента
схема в составе **концепции риск менеджмента** (2.3), определяющая подход, компоненты менеджмента и ресурсы, применимые к управлению **рисками** (2.1)
ПРИМЕЧАНИЕ 1: компоненты менеджмента обычно включают процедуры, практики, назначение ответственных лиц, последовательность и время действий.
ПРИМЕЧАНИЕ 2: план риск менеджмента может быть применен к определенному продукту, процессу и проекту, а также к части и целой организации.
[Руководство ISO 73:2009, определение 2.1.3]

2.7
владелец риска
лицо или объект, несущий ответственность за управление **рисками** (2.1)
[Руководство ISO 73:2009, определение 3.5.1.5]

person or entity with the accountability and authority to manage a **risk** (2.1)
[ISO Guide 73:2009, definition 3.5.1.5]

2.8
risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** (2.28) and reviewing **risk** (2.1)
[ISO Guide 73:2009, definition 3.1]

2.9
establishing the context
defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** (2.22) for the **risk management policy** (2.4)
[ISO Guide 73:2009, definition 3.3.1]

2.10
external context
external environment in which the organization seeks to achieve its objectives

NOTE External context can include:
– the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
– key drivers and trends having impact on the objectives of the organization; and
– relationships with, and perceptions and values of external **stakeholders** (2.13).
[ISO Guide 73:2009, definition 3.3.1.1]

2.11
internal context
internal environment in which the organization seeks to achieve its objectives

NOTE Internal context can include:
– governance, organizational structure, roles and accountabilities;
– policies, objectives, and the strategies

2.8
процесс управления рисками
систематическое применение политики менеджмента, процедур и практик по отношению к коммуникации, консалтингу, установлению контекста, а также идентификации, анализу, оценке, исследования, **мониторинга** (2.30) и анализа **риска** (2.1).
[Руководство ISO 73:2009, определение 3.1]

2.9
Установление контекста
Определение внешних и внутренних параметров, которые следует принять во внимание во время управления рисками, а также установление области и **критериев риска** (2.22) для **политики риск менеджмента** (2.4).
[Руководство ISO 73:2009, определение 3.3.1]

2.10
Внешний контекст
Внешняя среда, в которой организация стремится достигнуть своих целей

ПРИМЕЧАНИЕ: внешний контекст может включать:

- культурную, социальную, политическую, правовую, регулятивную, финансовую, технологическую, экономическую, природную и конкурентную среду, либо международную, национальную, региональную или локальную

- ключевые движущие силы и тренды, влияющие на цели организации

- отношения с внешними заинтересованными сторонами, их восприятие и оценка
[Руководство ISO 73:2009, определение 3.3.1.1]

2.11
Внутренний контекст
Внутренняя среда, в которой организация стремится достигнуть своих целей

ПРИМЕЧАНИЕ: внутренний контекст может включать:

- управление, организационную структуру, роли и ответственность

that are in place to achieve them;
– the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
– information systems, information flows and decision-making processes (both formal and informal);
– relationships with, and perceptions and values of, internal stakeholders;
– the organization's culture;
– standards, guidelines and models adopted by the organization; and
– form and extent of contractual relationships.
[ISO Guide 73:2009, definition 3.3.1.2]

- политики, цели, стратегии, которые используются для достижения целей

- возможности, понимание в рамках ресурсов и знаний (напр., финансы, время, процессы, системы и технологии)

- восприятие и оценку внутренних заинтересованных сторон

- информационные системы, информационные потоки, а также процесс принятия решений (формальных и неформальных)

- отношения с внутренними заинтересованными сторонами, их восприятие и оценка

- культуру организации

- стандарты, руководства и модели, официально принятые организацией

- форму и объем договорных отношений
[Руководство ISO 73:2009, определение 3.3.1.2]

2.12
communication and consultation
continual and iterative processes that an organization conducts to provide, share or obtain information and to
engage in dialogue with **stakeholders** (2.13) regarding the management of **risk** (2.1)

NOTE 1 The information can relate to the existence, nature, form, **likelihood** (2.19), significance, evaluation,
acceptability and treatment of the management of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders
on an issue prior to making a decision or determining a direction on that issue.
Consultation is:
– a process which impacts on a decision through influence rather than power; and
– an input to decision making, not joint decision making.

2.12
Коммуникации и консультации
Постоянный и повторяющийся процесс, которым управляет организация для того, чтобы предоставить, поделиться или приобрести информацию, а также для того, чтобы вступить в диалог с **заинтересованными сторонами** (2.15) и другими относительно управления **рисками** (2.1).

ПРИМЕЧАНИЕ 1: информация может относиться к существу, природе, **вероятности** (2.21), строгости, оценке, приемлемости, обработке или другим аспектам управления рисками.

ПРИМЕЧАНИЕ 2: консультация – это двусторонний процесс информационной коммуникации между организацией и ее заинтересованными сторонами или другими сторонами по определенному вопросу, принятию решения или определению направления по конкретной теме. Консультация – это:

- процесс, влияющий на решение посредством влияния лучше, чем полномочия

- входные данные для принятия решения, а не

[ISO Guide 73:2009, definition 3.2.1]

совместное принятие решения
[Руководство ISO 73:2009, определение 3.2.1]

2.13
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
NOTE A decision maker can be a stakeholder.
[ISO Guide 73:2009, definition 3.2.1.1]

2.13
Заинтересованная сторона
Лицо или организация, которая может повлиять на (или на них может повлиять, а также ощущать себя под влиянием) решение или деятельность.

ПРИМЕЧАНИЕ: Лицо, принимающее решение может быть заинтересованной стороной.
[Руководство ISO 73:2009, определение 3.2.1.1]

2.14
risk assessment
overall process of **risk identification** (2.15), **risk analysis** (2.21) and **risk evaluation** (2.24)
[ISO Guide 73:2009, definition 3.4.1]

2.14
Оценка риска
Общий процесс **идентификации риска** (2.17), **анализ риска (**2.23) и **определение степени риска** (2.26).
[Руководство ISO 73:2009, определение 3.4.1]

2.15
risk identification
process of finding, recognizing and describing **risks** (2.1)
NOTE 1 Risk identification involves the identification of **risk sources** (2.16), **events** (2.17), their causes and their potential **consequences** (2.18).
NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s (2.13) needs.
[ISO Guide 73:2009, definition 3.5.1]

2.15
Идентификация риска
Процесс нахождения, распознавания и описания **риска** (2.1)

ПРИМЕЧАНИЕ 1: идентификация риска включает идентификацию **источников** риска (2.18), **событий** (2.19), их причин и потенциальных **последствий** (2.20).

ПРИМЕЧАНИЕ 2: идентификация риска может включать исторические данные, теоретический анализ, информационные и экспертные опции и потребности **заинтересованных сторон** (2.15)
[Руководство ISO 73:2009, определение 3.5.1]

2.16
risk source
element which alone or in combination has the intrinsic potential to give rise to **risk** (2.1)
NOTE A risk source can be tangible or intangible.
[ISO Guide 73:2009, definition 3.5.1.2]

2.16
Источник риска
Элемент, который сам по себе или в комбинации с другими имеет внутренний потенциал для возникновения **риска** (2.1)

ПРИМЕЧАНИЕ: источник риска может быть материальный или нематериальный
[Руководство ISO 73:2009, определение 3.5.1.2]

2.17
event
occurrence or change of a particular set of circumstances
NOTE 1 An event can be one or more occurrences, and can have several causes.

2.17
Событие
Появление или изменение определенных обстоятельств

ПРИМЕЧАНИЕ 1: событие может представлять

NOTE 2 An event can consist of something not happening.
NOTE 3 An event can sometimes be referred to as an “incident” or “accident”.
NOTE 4 An event without **consequences** (2.18) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.
[ISO Guide 73:2009, definition 3.5.1.3]

собой одно или многие обстоятельства и может иметь несколько причин.

ПРИМЕЧАНИЕ 2: событие может состоять из того, что не происходит.

ПРИМЕЧАНИЕ 3: иногда событие можно отнести к терминам «инцидент» или «случайность».

ПРИМЕЧАНИЕ 4: событие без последствий также можно отнести к терминам «частичная удача», «случай», «угроза происшествия», «опасное положение».
[Руководство ISO 73:2009, определение 3.5.1.3]

2.18
consequence
outcome of an **event** (2.17) affecting objectives
NOTE 1 An event can lead to a range of consequences.
NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.
NOTE 3 Consequences can be expressed qualitatively or quantitatively.
NOTE 4 Initial consequences can escalate through knock-on effects.
[ISO Guide 73:2009, definition 3.6.1.3]

2.18
Последствие
Исход **события** (2.19), влияющий на цели

ПРИМЕЧАНИЕ 1: событие может привести к ряду последствий

ПРИМЕЧАНИЕ 2: последствие может быть определенным или неопределенным и иметь позитивное или негативное влияние на цели

ПРИМЕЧАНИЕ 3: последствия могут быть выражены качественно и количественно

ПРИМЕЧАНИЕ 4: начальные последствия могут повлечь за собой более серьезные
[Руководство ISO 73:2009, определение 3.6.1.3]

2.19
likelihood
chance of something happening
NOTE 1 In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).
NOTE 2 The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term.

2.19
Вероятность
Возможность того, что что-то произойдет

ПРИМЕЧАНИЕ 1: в терминологии риск менеджмента слово «вероятность» используется для ссылки на возможность, что что-то произойдет, измеряется и определяется объективно и субъективно, количественно и качественно, и описывается с помощью общих терминов или математически (напр., вероятность или частота в данный период времени).

ПРИМЕЧАНИЕ 2: английский термин «вероятность» во многих языках не имеет прямого эквивалента, в то время как термин «возможность» часто используется. Не смотря на это, в английском языке «вероятность» часто интерпретируется как математический термин.

Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.
[ISO Guide 73:2009, definition 3.6.1.1]

2.20
risk profile
description of any set of **risks** (2.1)
NOTE The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.
[ISO Guide 73:2009, definition 3.8.2.5]

2.21
risk analysis
process to comprehend the nature of **risk** (2.1) and to determine the **level of risk** (2.23)
NOTE 1 Risk analysis provides the basis for **risk evaluation** (2.24) and decisions about **risk treatment** (2.25).
NOTE 2 Risk analysis includes risk estimation.
[ISO Guide 73:2009, definition 3.6.1]

2.22
risk criteria
terms of reference against which the significance of a **risk** (2.1) is evaluated
NOTE 1 Risk criteria are based on organizational objectives, and **external** (2.10) and **internal context** (2.11).
NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.
[ISO Guide 73:2009, definition 3.3.1.3]

2.23
level of risk
magnitude of a **risk** (2.1) or combination of risks, expressed in terms of the combination of **consequences** (2.18) and their **likelihood** (2.19)
[ISO Guide 73:2009, definition 3.6.1.8]

2.24

Поэтому в терминологии риск менеджмента используется «вероятность», т.к. этот термин имеет более широкую интерпретацию, чем «возможность».
[Руководство ISO 73:2009, определение 3.6.1.1]

2.20
Структура риска
Описание любой группы **рисков** (2.1)

ПРИЕЧАНИЕ: группа рисков может содержать такие риски, которые относятся к целой организации, части организации или другим компонентам.
[Руководство ISO 73:2009, определение 3.8.2.5]

2.21
Анализ риска
Процесс понимания природы **риска** (2.1) и определения **уровня риска** (2.25)

ПРИМЕЧАНИЕ 1: анализ риска предоставляет основу для **определения степени риска** (2.26) и для решения **обработки риска** (2.27).

ПРИМЕЧАНИЕ 2: анализ риска включает оценку риска.
[Руководство ISO 73:2009, определение 3.6.1]

2.22
Критерии риска
Данные, по которым оценивается значимость **риска** (2.1)

ПРИМЕЧАНИЕ 1: критерии риска основаны на целях организации, ее **внешнем** (2.12) и **внутреннем контексте** (2.13)

ПРИМЕЧАНИЕ 2: критерии риска могут быть производными от стандартов, законов, политик и других требований.
[Руководство ISO 73:2009, определение 3.3.1.3]

2.23
Уровень риска
Величина **риска** (2.1), выраженная в рамках комбинации **последствий** (2.20) и их **вероятности** (2.21)
[Руководство ISO 73:2009, определение 3.6.1.8]

2.24
Определение степени риска

risk evaluation
process of comparing the results of **risk analysis** (2.21) with **risk criteria** (2.22) to determine whether the **risk**
(2.1) and/or its magnitude is acceptable or tolerable
NOTE Risk evaluation assists in the decision about **risk treatment** (2.25).
[ISO Guide 73:2009, definition 3.7.1]

Процесс сравнения результатов **анализа риска** (2.23) с **критериями риска** (2.24) для определения того, можно ли принять величину **риска** (2.1)

ПРИМЕЧАНИЕ: определение степени риска способствует об обработке риска (2.27).
[Руководство ISO 73:2009, определение 3.7.1]

2.25
risk treatment
process to modify **risk** (2.1)
NOTE 1 Risk treatment can involve:
– avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
– taking or increasing risk in order to pursue an opportunity;
– removing the **risk source** (2.16);
– changing the **likelihood** (2.19);
– changing the **consequences** (2.18);
– sharing the risk with another party or parties (including contracts and risk financing); and
– retaining the risk by informed decision.
NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.
NOTE 3 Risk treatment can create new risks or modify existing risks.
[ISO Guide 73:2009, definition 3.8.1]

2.25
Обработка риска
Процесс модификации риска (2.1)

ПРИМЕЧАНИЕ 1: обработка риска может включать:

- обходной путь риска посредством решения не начинать или не продолжать деятельность, которая провоцирует появление риска

- сохранение или увеличение риска с целью исследовать обстоятельство

- удаление **источника риска** (2.18)

- изменение **вероятности** (2.21)

- изменение **последствий** (2.20)

- разделение риска с другой стороной или сторонами (включая контракты и финансирование риска)

- сохранение риска при наличии полной информации

ПРИМЕЧАНИЕ 2: обработки рисков, которые имеют дело с негативными последствиями, иногда относятся к «уменьшению рисков», «устранению рисков», «избеганию рисков» и «редукции рисков».

ПРИМЕЧАНИЕ 3: обработка риска может создать новые риски или модифицировать уже существующие.
[Руководство ISO 73:2009, определение 3.8.1]

2.26
control
measure that is modifying **risk** (2.1)
NOTE 1 Controls include any process, policy, device, practice, or other actions which modify risk.

2.26
Контроль
Измерение, способное изменить **риск** (2.1)

ПРИМЕЧАНИЕ 1: контроль включает любой процесс, политику, прибор, практику или другие

NOTE 2 Controls may not always exert the intended or assumed modifying effect.
[ISO Guide 73:2009, definition 3.8.1.1]

действия, которые модифицируют риск.

ПРИМЕЧАНИЕ 2: контроль не всегда влияет на ожидаемый или предполагаемый модифицирующий эффект.
[Руководство ISO 73:2009, определение 3.8.1.1]

2.27
residual risk
risk (2.1) remaining after **risk treatment** (2.25)
NOTE 1 Residual risk can contain unidentified risk.
NOTE 2 Residual risk can also be known as “retained risk”.
[ISO Guide 73:2009, definition 3.8.1.6]

2.27
Остаточный риск
Риск (2.1), который остается после **обработки риска** (2.27)

ПРИМЕЧАНИЕ 1: остаточный риск может содержать в себе неидентифицированный риск.

ПРИМЕЧАНИЕ 2: остаточный риск может также называться «сохраненный риск».
[Руководство ISO 73:2009, определение 3.8.1.6]

2.28
monitoring
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected
NOTE Monitoring can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).
[ISO Guide 73:2009, definition 3.8.2.1]

2.28
мониторинг
постоянная проверка, надзор, критическое наблюдение или определение статуса идентифицировать изменения показателей и ожидаемых результатов.

ПРИМЕЧАНИЕ: мониторинг может быть применен к **концепции риск менеджмента** (2.3), **процессу риск менеджмента** (2.10), **риску** (2.1) или **контролю** (2.28).
[Руководство ISO 73:2009, определение 3.8.2.1]

2.29
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
NOTE Review can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).
[ISO Guide 73:2009, definition 3.8.2.2]

2.29
Анализ
Действие, предпринятое для определения пригодности, адекватности и эффективности предпринятых действий для достижения установленных целей.

ПРИМЕЧАНИЕ: анализ может быть применен к **концепции риск менеджмента** (2.3), **процессу риск менеджмента** (2.10), **риску** (2.1) или **контролю** (2.28).
[Руководство ISO 73:2009, определение 3.8.2.2]

3 Principles

For risk management to be effective, an organization should at all levels comply with the principles below.

3. Принципы

Для того чтобы управление рисками было эффективным, организация должна на всех уровнях соответствовать принципам, перечисленным ниже.

a) **Risk management creates and protects value**.
Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b) **Risk management is an integral part of all organizational processes**.
Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of
all organizational processes, including strategic planning and all project and change management processes.

c) **Risk management is part of decision making**.
Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

d) **Risk management explicitly addresses uncertainty**.
Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) **Risk management is systematic, structured and timely**.
A systematic, timely and structured approach to risk management contributes to efficiency and to
consistent, comparable and reliable results.

f) **Risk management is based on the best available information**.
The inputs to the process of managing risk are based on information sources such as historical data,
experience, stakeholder feedback,

a) **Риск менеджмент создает и защищает оценки**

Риск менеджмент способствует очевидному достижению целей и улучшению показателей, например, здоровья и безопасности человека, защиты, соответствию законодательству и регламенту, публичному признанию, защите окружающей среды, качества продуктов, проектного управления, эффективности деятельности, руководства и репутации.

b) **Риск менеджмент - это составная часть всех организационных процессов**

Риск менеджмент – это не автономная деятельность, она отделена от главной деятельности и процессов организации. Риск менеджмент – это часть ответственности управления и составная часть всех организационных процессов, включая стратегическое планирование и управление процессами проектов и изменений.

c) **Риск менеджмент является частью принятия решения**

Риск менеджмент помогает лицам, принимающим решение, сделать правильный выбор, расставить приоритеты и определить альтернативные курсы действий.

d) **Риск менеджмент ясно выражает неопределенность**

риск менеджмент учитывает неопределенность, природу данной неопределенности и каким образом их можно выразить.

e) **Риск менеджмент систематизирован, структурирован и согласован по времени**

Систематический, структурированный и согласованный по времени подход к риск менеджменту способствует эффективности, а также последовательным, соизмеримым достоверным результатам.

f) **Риск менеджмент основан лучшей доступной информации**

observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

входные данные для процесса управления рисками основаны на информационных ресурсах, таких, как исторические данные, опыт, обратная связь заинтересованных сторон, наблюдения, прогнозы и высказывания экспертов. Однако лица, принимающие решение, должны быть осведомлены и принимать во внимание любые ограничения в данных или использование моделирования, а также возможность расхождения мнений экспертов.

g) **Risk management is tailored**.
Risk management is aligned with the organization's external and internal context and risk profile.

g) **Риск менеджмент особенный для каждой организации**

риск менеджмент сконцентрирован на внешнем и внутреннем контексте организации и структуре риска.

h) **Risk management takes human and cultural factors into account**.
Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

h) **Риск менеджмент принимает во внимание человеческие и культурные факторы**

Риск менеджмент распознает потенциал, восприятие и намерения внешних и внутренних заинтересованных сторон, которые могут способствовать или мешать достижению целей организации.

i) **Risk management is transparent and inclusive**.
Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining riskcriteria.

i) **риск менеджмент обладает транспарентностью и инклюзивностью**

соответствующее и правильное по времени вовлечение заинтересованных сторон, в частности, лиц, которые должны принимать решения на всех уровнях организации, гарантирует, что риск менеджмент остается релевантным и обновленным. Вовлечение также позволяет заинтересованным сторонам быть представленными соответствующим образом и осознавать, что их взгляды приняты во внимание при определении критериев риска.

j) **Risk management is dynamic, iterative and responsive to change**.
Risk management continually senses and responds to change. As external and internal events occur,
context and knowledge change, monitoring and review of risks take place,

j) **Риск менеджмент – это динамичный, повторяющийся и способный к изменениям процесс**

Как случаются внутренние и внешние события, меняется контекст и знания, имеют место мониторинг и анализ, возникают новые риски, так что-то меняется, а другое исчезает. Поэтому риск менеджмент реагирует на изменения.

new risks emerge, some change, and others disappear.

k) **Risk management facilitates continual improvement of the organization**.
Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.
Annex A provides further advice for organizations wishing to manage risk more effectively.

4 Framework

4.1 General

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process (see Clause 5) at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.
This clause describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner, as shown in Figure 2.

k) **Риск менеджмент способствует постоянному улучшению организации**

Организации должны развивать и внедрять стратегии для улучшения развития их риск менеджмента на ряду с другими аспектами организации.

Приложение А предлагает дальнейшие советы по желанию организации сделать управление рисками более эффективным.

4. Концепция

4.1 Общие положения

Успех менеджмента рисков будет зависеть от эффективности управленческой концепции, которая предоставляет основы и соглашения, которые внедряются в организацию на всех ее уровнях. Концепция делает вклад в эффективный риск-менеджмент путем применения процессов риск-менеджмента (см. п. 5) на различных уровнях и в определенных контекстах внутри организации. Такая система дает гарантию того, что об информации, собранной в ходе реализации процессов риск-менеджмента, был сделан целесообразный отчет и что она же лежит в основе принятия решений и что на нее опираются на всех соответствующих организационных уровнях. Этот пункт описывает неотъемлемые компоненты риск-менеджмента, и то, как они взаимодействуют в повторяющейся среде, как это показано в Схеме 2.

Схема 2 – Взаимосвязи между компонентами концепции риск-менеджмента

This framework is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system. Therefore, organizations should adapt the components of the framework to their specific needs.

If an organization's existing management practices and processes include components of risk management or if the organization has already adopted a formal risk management process for particular types of risk or situations, then these should be critically reviewed and assessed against this International Standard, including the attributes contained in Annex A, in order to determine their adequacy and effectiveness.

Цель данной концепции – не предписание системы менеджмента, а скорее помощь организации в процессе интеграции риск-менеджмента в общую систему менеджмента. Таким образом, организации должны освоить компоненты концепции для собственных нужд.

Если существующие практики и процессы управления внутри организации включают компоненты риск-менеджмента или если организация уже применяет формальные процессы риск-менеджмента для определенных типов риска, все это должно быть проанализировано с критической точки зрения и оценено относительно Международного Стандарта, включая информацию которая содержится в Приложении А, чтобы увериться в их целесообразности и эффективности.

4.2 Mandate and commitment

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained
commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels. Management should:

– define and endorse the risk management policy;
– ensure that the organization's culture and risk management policy are aligned;
– determine risk management performance indicators that align with performance indicators of the organization;
– align risk management objectives with the objectives and strategies of the organization;
– ensure legal and regulatory compliance;
– assign accountabilities and responsibilities at appropriate levels within the organization;
– ensure that the necessary resources are allocated to risk management;
– communicate the benefits of risk management to all stakeholders; and
– ensure that the framework for managing risk continues to remain appropriate.

4.2 Поручения и обязательства

Введение в риск-менеджмент и непрерывная гарантия его эффективности требуют сильную и оправданную приверженность со стороны руководства организации, а также стратегическое и тщательное планирование, чтобы достигнуть приверженности на всех уровнях. Руководству необходимо:

- ✓ Определить и утвердить политику риск-менеджмента;
- ✓ Быть уверенным в том, что уровень культуры внутри организации и политики риск-менеджмента соответствуют друг другу;
- ✓ Определить показатели эффективности риск-менеджмента , те, что соответствуют показателям эффективности организации;
- ✓ Сравнить цели риск-менеджмента с целями и стратегиями организации;
- ✓ Быть уверенным в своем соответствии по юридическим и нормативным вопросам;
- ✓ Распределить ответственности и обязанности на всех уровнях организации ;
- ✓ Дать гарантию того что ресурсы, необходимые для риск-менеджмента, были распределены;
- ✓ Донести до всех заинтересованных сторон преимущества риск-менеджмента
- ✓ Быть уверенным в том, что концепция риск-менеджмента по-прежнему остается целесообразной.

4.3 Design of framework for managing risk
4.3.1 Understanding of the organization and its context

Before starting the design and implementation of the framework for managing risk, it is important to evaluate and understand both the external and internal context of the organization, since these can significantly influence the design of the framework.
Evaluating the organization's external context may include, but is not limited to:

4.3 Проект концепции риск-менеджмента
4.3.1 Понимание организации и ее контекста

Перед началом разработки и внедрения концепции риск-менеджмента, важно оценить и понять как внешний, так и внутренний контекст организации, так как они могут в значительной степени повлиять на разработку концепции

Оценка внешнего контекста организации может включать (но не ограничиваться):

а) социальной и культурной, политической, законодательной, нормативной, финансовой, технологической, экономической, естественной и конкурентной средой, как международной, так и

a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
b) key drivers and trends having impact on the objectives of the organization; and
c) relationships with, and perceptions and values of, external stakeholders.

Evaluating the organization's internal context may include, but is not limited to:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows and decision making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the organization's culture;
- standards, guidelines and models adopted by the organization; and
- the form and extent of contractual relationships.

4.3.2 Establishing risk management policy

The risk management policy should clearly state the organization's objectives for, and commitment to, risk management and typically addresses the following:

- the organization's rationale for managing risk;
- links between the organization's objectives and policies and the risk management policy;
- accountabilities and responsibilities for managing risk;
- the way in which conflicting interests are dealt with;

национальной, региональной и местной;
b) ключевые движущие силы и течения, которые влияют на цели организации; и
c) отношения с внешними заинтересованными сторонами, их перспективы и ценности.

Оценка внутреннего контекста организации может включать (но не ограничиваться):

- ✓ Правление, организационную структуру, роли и обязанности;
- ✓ Политики, цели и стратегии, которые необходимо достигнуть;
- ✓ Возможности, в смысле ресурсов и знаний (напр. Капитал, время, человеческие ресурсы, процессы, системы и технологии);
- ✓ Информационный системы , информационные потоки и процессы принятия решений (формальные и неформальные);
- ✓ Отношения с внутренними заинтересованными сторонами, их перспективы и ценности.
- ✓ Культура внутри организации;
- ✓ Стандарты, руководства и модели принятые внутри организации; а также
- ✓ Форма и объем контрактных взаимоотношений

4.3.2 Установление политики риск-менеджмента

Политика риск-менеджмента должна в ясной манере отражать цели и приверженность организации в области риск-менеджмента и отвечать следующим критериям:

- ✓ Стремлению организации к обработке рисков;
- ✓ Связям между целями организации и политиками, в том числе политике риск-менеджмента;
- ✓ Ответственностям и обязанностям по обработке рисков;
- ✓ Способу, к которому прибегают в решении конфликта интересов;
- ✓ Обязательству по обеспечению необходимыми ресурсами того, кто

– commitment to make the necessary resources available to assist those accountable and responsible for managing risk;
– the way in which risk management performance will be measured and reported; and
– commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.

The risk management policy should be communicated appropriately.

4.3.3 Accountability

The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:
– identifying risk owners that have the accountability and authority to manage risks;
– identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
– identifying other responsibilities of people at all levels in the organization for the risk management process;
– establishing performance measurement and external and/or internal reporting and escalation processes; and
– ensuring appropriate levels of recognition.

4.3.4 Integration into organizational processes

Risk management should be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from,

отвечает за управление рисками;
- ✓ Тому, как будет измеряться и подтверждаться эффективность риск-менеджмента; и
- ✓ Обязательству по постоянной оценке и улучшению политики риск-менеджмента и концепции, или вследствие какого-либо события, а также в ходе изменения каких-либо обстоятельств.
- ✓ Тому, что политика риск-менеджмента должна управляться должным образом.

4.3.3 Ответственность

Организация должна дать гарантию того, что существует ответственность, уполномоченные и должный уровень компетенции для управления рисками, включая внедрение и поддержание процессов риск-менеджмента, а так же дать гарантию целесообразности, эффективности и достаточности любых методов управления. Этому может способствовать:

- ✓ Идентификация владельцев риска, которые несут ответственность и уполномочены управлять рисками;
- ✓ Идентификация лиц, несущих ответственность за развитие, применение и поддержание концепции управления рисками;
- ✓ Идентификация иных ответственностей по процессам риск-менеджмента, возлагаемых на персонал всех уровней внутри организации for the risk management;
- ✓ Установление мер эффективности, а также внешних и/или внутренних процессов подтверждения и рассмотрения руководством; и
- ✓ Гарантия признания на всех соответствующих уровнях.

4.3.5 Интеграция в процессы организации

Риск-менеджмент должен быть внедрен во все практики организации, до тех пор пока он носит уместный, эффективный и достаточный характер. Процессы риск-менеджмента должны стать частью процессов организации, а никак не стоять в стороне от них. В частности, риск-менеджмент должен быть внедрен в политику развития, оценку

those organizational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.
There should be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes. The risk management plan can be integrated into other organizational plans, such as a strategic plan.

бизнес- и стратегического планирования, а также в процессы управления изменениями.

Во всей организации должен существовать план риск-менеджмента, в целях гарантии того, что политика риск-менеджмента применяется ко всем процессам и практикам этой организации. План риск-менеджмента может быть интегрирован в другие планы организации, например в стратегический план.

4.3.5 Resources

The organization should allocate appropriate resources for risk management.
Consideration should be given to the following:
– people, skills, experience and competence;
– resources needed for each step of the risk management process;
– the organization's processes, methods and tools to be used for managing risk;
– documented processes and procedures;
– information and knowledge management systems; and
– training programmes.

4.3.6 Ресурсы

Организация должна распределить необходимые для риск-менеджмента ресурсы:
Должны быть рассмотрены следующие аспекты:

- ✓ Человеческие ресурсы, навыки, опыт и конкурентоспособность;
- ✓ Ресурсы, необходимые для каждого шага процесса риск-менеджмента;
- ✓ Процессы организации, методы и средства обработки рисков;
- ✓ Документированные процессы и процедуры;
- ✓ Системы менеджмента информации и знаний; и
- ✓ Учебные программы.

4.3.6 Establishing internal communication and reporting mechanisms

The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that:

– key components of the risk management framework, and any subsequent modifications, are communicated appropriately;
– there is adequate internal reporting on the framework, its effectiveness and the outcomes;
– relevant information derived from the

4.3.7 Установление внутренней коммуникации и отчетного механизма

Организация должна установить внутреннюю коммуникацию и механизмы отчетности, для того, чтобы поддержать процессы контроля и владения рисками. Эти механизмы должны давать гарантию того, что:

- ✓ Ключевые компоненты концепции риск-менеджмента и любых последующих модификаций управляются должным образом;
- ✓ Существует понятная система внутренней отчетности по концепции, ее эффективности и результатах;
- ✓ Необходимая информация, почерпнутая в ходе применения риск-менеджмента доступна в любое время и на соответствующих уровнях; и

application of risk management is available at appropriate levels and times; and
– there are processes for consultation with internal stakeholders.
These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

- ✓ Существуют процессы консультации с внутренними заинтересованными сторонами.

Механизмы должны, там где применимо, включать процессы по объединению информации по рискам из множества ресурсов, а также принимать во внимание секретность такой информации.

4.3.7 Establishing external communication and reporting mechanisms

The organization should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

– engaging appropriate external stakeholders and ensuring an effective exchange of information;
– external reporting to comply with legal, regulatory, and governance requirements;
– providing feedback and reporting on communication and consultation;
– using communication to build confidence in the organization; and
– communicating with stakeholders in the event of a crisis or contingency.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

4.3.8 Установление внутренней коммуникации и отчетного механизма

Организация должна разработать и внедрить план того, как будет происходить коммуникация с внешними заинтересованными сторонами. Он должен включать:

- ✓ Привлечение соответствующих внешних заинтересованных сторон, и гарантию эффективного обмена информацией;
- ✓ Систему внешней отчетности, чтобы соответствовать юридическим, нормативным, и правительственным требованиям;
- ✓ Предоставление отзывов по коммуникациям и консалтингу;
- ✓ Использование коммуникации в качестве метода создания атмосферы доверия внутри организации; и
- ✓ Коммуникацию с заинтересованными сторонами в случае возникновения кризиса или нештатной ситуации.

Механизмы должны, там где применимо, включать процессы по объединению информации по рискам из множества ресурсов, а также принимать во внимание секретность такой информации.

4.4 Implementing risk management

4.4.1 Implementing the framework for managing risk

In implementing the organization's framework for managing risk, the organization should:
– define the appropriate timing and strategy for implementing the framework;
– apply the risk management policy and process to the organizational processes;
– comply with legal and regulatory

4.4 Внедрение риск-менеджмента

4.4.1 Внедрение концепции для управления рисками

В процессе внедрения концепции организации по управлению рисками, эта организация должна:

- ✓ Определить подходящие временные рамки и стратегии для внедрения концепции;
- ✓ Применять политику риск-менеджмента и его процессы к процессам внутри организации;

requirements;
– ensure that decision making, including the development and setting of objectives, is aligned with the
outcomes of risk management processes;
– hold information and training sessions; and
– communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

- ✓ Соответствовать юридическим и нормативным требованиям;
- ✓ Дать гарантию того, что процесс принятия решений, включая разработку и постановку целей, соответствует результатам процессов риск-менеджмента;
- ✓ Проводить ознакомительные и обучающие семинары; а также
- ✓ Сообщать заинтересованным сторонам концепция риск-менеджмента остается целесообразной.

4.4.2 Implementing the risk management process

Risk management should be implemented by ensuring that the risk management process outlined in Clause 5
is applied through a risk management plan at all relevant levels and functions of the organization as part of its
practices and processes.

4.4.2 Внедрение процессов по управлению рисками

Риск-менеджмент должен быть внедрен при полной гарантии того что его процессы, определенные в пункте 5, применяются в соответствии с планом риск-менеджмента на всех соответствующих уровнях и позициях организации, как часть его практик и процессов.

4.5 Monitoring and review of the framework

In order to ensure that risk management is effective and continues to support organizational performance, the organization should:
– measure risk management performance against indicators, which are periodically reviewed for
appropriateness;
– periodically measure progress against, and deviation from, the risk management plan;
– periodically review whether the risk management framework, policy and plan are still appropriate, given
the organizations' external and internal context;
– report on risk, progress with the risk management plan and how well the risk management policy is being
followed; and
– review the effectiveness of the risk management framework.

4.5 Мониторинг и анализ концепции

Для того, чтобы дать гарантию того, что риск-менеджмент эффективен и продолжает поддерживать производительность организации, такая организация должна:

- ✓ Измерять эффективность риск-менеджмента относительно показателей, которые периодически анализируются на соответствие требованиям;
- ✓ Время от времени измерять рост относительно и отдельно от плана риск-менеджмента;
- ✓ Периодически выяснять, соответствуют ли по прежнему концепция, политика и план риск-менеджмента требованиям, беря во внимание внутренний и внешний контекст организации;
- ✓ Вести отчет о рисках и росте в соответствии с планом риск-менеджмента, а также о том, как соблюдается политика риск-менеджмента; и
- ✓ Анализировать эффективность концепции риск-менеджмента

4.6 Continual improvement of the framework

4.6 Постоянное улучшение концепции

Основанные на результатах мониторинга и оценки,

Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organization's management of risk and its risk management culture.

5 Process

5.1 General

The risk management process should be

– an integral part of management,

– embedded in the culture and practices, and

– tailored to the business processes of the organization.

It comprises the activities described in 5.2 to 5.6. The risk management process is shown in Figure 3.

должны приниматься решения по улучшению концепции риск-менеджмента, его политики и плана. Такие решения должны привести к улучшениям управления рисками внутри организации и общей культуры управления рисками.

5 Процесс

5.1 Общие положения

Процессы риск-менеджмента должны быть

- ✓ Неотъемлемой частью менеджмента,
- ✓ Внедрены в культуру и практики, а также
- ✓ Приспособлены к бизнес-процессам организации.

Они объединяют действия, определенные в пунктах 5.2-5.6 6. Процесс риск-менеджмента показан на Схеме 3.

5.2 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

A consultative team approach may:

- help establish the context appropriately;
- ensure that the interests of stakeholders are understood and considered;
- help ensure that risks are adequately identified;
- bring different areas of expertise together for analyzing risks;
- ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;
- secure endorsement and support for a treatment plan;
- enhance appropriate change management during the risk management process; and
- develop an appropriate external and internal communication and consultation plan.

Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and taken into

5.2 Коммуникации и консультации

Коммуникации и консультации с внешними и внутренними заинтересованными сторонами должны происходить на всех стадиях процесса управления рисками. Поэтому, планы относительно коммуникации и консультации должны быть разработаны еще в начальной стадии. Они должны обращаться к вопросам, касающимся рисков непосредственно, его причин, и его последствий (если таковые известны), и мерам, которые были приняты с целью обработки такого риска. Эффективные внешние и внутренние коммуникации и консультации должны давать гарантию что те, кто несут ответственность за процесс управления риском и заинтересованные стороны осознают основания для принятия решений, и причины, того, почему требуются определенные действия.

Консультационный подход внутри команды способен:

- ✓ Помочь в должном установлении контекста;
- ✓ Гарантировать, что интересы заинтересованных сторон понятны и что с ними считаются;
- ✓ Гарантировать, что риски должным образом идентифицированы;
- ✓ Сводить разные области экспертных знаний воедино для анализа рисков;
- ✓ Гарантировать то, что, при определении критериев риска и их оценке, рассматриваются различные точки зрения;
- ✓ Обеспечить подтверждение и поддержку плана обработки;
- ✓ Повысить целесообразность управления изменениями в ходе процесса риск-менеджмента; и
- ✓ Разработать целесообразный план внутренней и внешней коммуникации.

Коммуникации и консультации с заинтересованными сторонами важны, поскольку они дают суждения о риске, которые основаны на их собственном восприятии риска. Эти восприятия могут измениться из-за разницы в ценностях, потребностях, предположениях, понятиях и ожиданиях заинтересованных сторон. Поскольку их взгляды могут оказать существенное влияние на принимаемые решения, восприятие заинтересованных сторон должно быть идентифицировано, документировано, и должно приниматься во внимание при принятии решений.

account in the decision making process.
Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

Коммуникации и консультации должны способствовать обмену достоверной, важной, точной и понятной информации, принимая во внимание конфиденциальные и личные аспекты ее целостности.

5.3 Establishing the context

5.3.1 General

5.3 Установление контекста

5.3.1 Общие положения

By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process. While many of these parameters are similar to those considered in the design of the risk management framework (see 4.3.1), when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process.

Устанавливая контекст, организация ясно формулирует свои цели, определяет внешние и внутренние параметры, которые будут приняты во внимание при управлении рисками, а также устанавливает область распространения и критерии рисков для оставшихся процессов. В то время как многие из этих параметров подобны тем, которые были рассмотрены при разработке концепции риск-менеджмента (см. 4.3.1), при установлении контекста для процесса управления рисками, они должны быть рассмотрены детально, и то, как они относятся к процессу управления в области конкретного риска.

5.3.2 Establishing the external context

5.3.2 Установление внешнего контекста

The external context is the external environment in which the organization seeks to achieve its objectives. Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

Внешний контекст это внешняя среда, в которой организация стремится достигнуть своих целей. Понимание внешнего контекста важно в порядке гарантии того, что цели и ожидания внешних заинтересованных сторон будут рассмотрены при разработке критериев риска. Он основан на контексте всей организации, но с определенными тонкостями в виде юридических и нормативных требований, восприятиях заинтересованных сторон и других аспектах риска, естественных для области применения процессов риск-менеджмента.

The external context can include, but is not limited to:

- the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organization; and
- relationships with, perceptions and

Внешний контекст может включать (но не быть ограниченным):

- ✓ Социальную и культурную, политическую, законодательную, нормативную, финансовую, технологическую, экономическую, естественную и конкурентную среду, как международную, так и национальную, региональную и местную.
- ✓ Ключевые движущие силы и направления, которые влияют на цели организации; и
- ✓ Отношения, восприятия и ценности

values of external stakeholders.

5.3.3 Establishing the internal context

The internal context is the internal environment in which the organization seeks to achieve its objectives.

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way in which an organization will manage risk. It should be established because:

a) risk management takes place in the context of the objectives of the organization;

b) objectives and criteria of a particular project, process or activity should be considered in the light of objectives of the organization as a whole; and

c) some organizations fail to recognize opportunities to achieve their strategic, project or business objectives, and this affects ongoing organizational commitment, credibility, trust and value.

It is necessary to understand the internal context. This can include, but is not limited to:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- the relationships with and perceptions and values of internal stakeholders;
- the organization's culture;
- information systems, information flows and decision making processes (both formal and informal);
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual relationships.

5.3.4 Establishing the context of the risk management process

внешних заинтересованный сторон.

5.3.3 Установление внутреннего контекста

Внутренний контекст это внутренняя среда, в которой организация стремится достигнуть своих целей.

Процесс риск-менеджмента должен соответствовать культуре, процессам, структуре и стратегиям организации. Внутренний контекст это что-то, что может повлиять изнутри на то, как организация будет управлять рисками. Он должен быть установлен, так как:

a) Риск-менеджмент представлен в контексте целей организации;

b) Цели и критерии определенного проекта, процесса или деятельности должны рассматриваться в свете целей организации в общем; и

c) Некоторые организации не могут определить возможности для достижения их стратегических, проектных или бизнес целей, и это не лучшим образом отражается на активности, доверии, надежности и ценности организации.

Необходимо понимать, что такое внутренний контекст. Он может включать (но не быть ограниченным):

- ✓ Правление, организационную структуру, роли и обязанности;
- ✓ Политики, цели и стратегии, которые необходимо достигнуть;
- ✓ Возможности, в смысле ресурсов и знаний (напр. Капитал, время, человеческие ресурсы, процессы, системы и технологии);
- ✓ Информационный системы, информационные потоки и процессы принятия решений (формальные и неформальные);
- ✓ Отношения с внутренними заинтересованными сторонами, их перспективы и ценности.
- ✓ Культура внутри организации;
- ✓ Стандарты, руководства и модели принятые внутри организации; а также
- ✓ Форма и объем контрактных взаимоотношений

5.3.4 Установление контекста процесса управления рисками

The objectives, strategies, scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified.

The context of the risk management process will vary according to the needs of an organization. It can involve, but is not limited to:

– defining the goals and objectives of the risk management activities;
– defining responsibilities for and within the risk management process;
– defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;
– defining the activity, process, function, project, product, service or asset in terms of time and location;
– defining the relationships between a particular project, process or activity and other projects, processes or activities of the organization;
– defining the risk assessment methodologies;
– defining the way performance and effectiveness is evaluated in the management of risk;
– identifying and specifying the decisions that have to be made; and
– identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

Attention to these and other relevant factors should help ensure that the risk management approach adopted is appropriate to the circumstances, to the organization and to the risks affecting the achievement of its objectives.

Должны быть установлены цели, стратегии, область применения и параметры деятельности организации, или тех частей организации, в которых применяется процесс риск-менеджмента. Менеджмент рисков должен проводиться с рассмотрением необходимости согласования ресурсной базы, используемой при обработке риска. Требуемые ресурсы, обязанности и уполномоченные, записи, которые должны вестись, так же необходимо определить. Контекст процесса риск-менеджмента будет разниться ввиду потребностей организации. Он может включать (но не быть ограниченным):

- ✓ Определение целей и задач мероприятий по риск-менеджменту;
- ✓ Определение ответственностей по процессу в ходе процесса риск-менеджмента;
- ✓ Определение области применения, так же как и глубины и ширины мероприятий по риск-менеджменту, в том числе необходимые включения и исключения;
- ✓ Определение мероприятий, процессов, функций, проектов, продукции, услуг или активов в отношении времени и расположения;
- ✓ Определение взаимоотношений между определенным проектом, процессом или деятельностью и другими проектами, процесса или действиями организации;
- ✓ Определение методологий оценки рисков;
- ✓ Определение метода, каким будет оцениваться эффективность управления риском;
- ✓ Идентификация и установление решений, которые необходимо принять; и
- ✓ Идентификация, определение области применения, или составление необходимых исследований и ресурсов, требуемых для таких исследований.

Внимание к тем или иным факторам может гарантировать, что применяемый процесс риск-менеджмента соответствует обстоятельствам, организации, и рискам, тормозящим осуществление такой организацией ее целей.

5.3.5 Defining risk criteria

The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy (see 4.3.2), be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered should include the following:

– the nature and types of causes and consequences that can occur and how they will be measured;
– how likelihood will be defined;
– the timeframe(s) of the likelihood and/or consequence(s);
– how the level of risk is to be determined;
– the views of stakeholders;
– the level at which risk becomes acceptable or tolerable; and
– whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

5.4 Risk assessment

5.4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

NOTE ISO/IEC 31010 provides guidance on risk assessment techniques.

5.4.2 Risk identification

The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated

5.3.5 Определение критериев риска

Организация должна определить критерии для использования в процессе оценки значимости риска. Критерии должны отражать ценности, цели и ресурсы организации. Некоторые критерии могут быть введены или извлечены из юридических и нормативных или же других требований, тех, которым следует организация. Критерии рисков должны соответствовать политике риск-менеджмента организации (см. 4.3.2), быть определены в начале процесса риск-менеджмента, а также должны постоянно обновляться.

При определении критериев риска, должны быть рассмотрены следующие факторы:

- ✓ Природа и тип причин и последствий, которые могут возникнуть и то, как они будут измеряться;
- ✓ Как будет определена вероятность;
- ✓ Временные рамки вероятности и/или последствий;
- ✓ Каким образом будет определен уровень риска;
- ✓ Взгляды заинтересованных сторон;
- ✓ Уровень, на котором риск становится допустимым или приемлемым; и
- ✓ Должны ли рассматриваться комбинации множественных рисков, и если да, то как и какие комбинации должны быть рассмотрены.

5.4 Оценка риска

5.4.1 Общие положения

Оценка риска это всеобщий процесс идентификации, анализа и оценки степени риска.

ПРИМЕЧАНИЕ ISO/IEC 31010 предоставляет руководство по техникам оценке риска.

5.4.2 Идентификация риска

Организация должна определить источник риска, области его влияния, рисковые случаи (включая изменение обстоятельств), их причины, а также их потенциальные последствия. Цель данного шага – составить исчерпывающий список рисков, основанный на тех рисковых случаях, которые могут создать почву для, увеличить возможность, предотвратить, ухудшить, сократить достижение целей. Важно идентифицировать риски, связанные с утраченной возможностью. Исчерпывающая

with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.
Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.
The organization should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks.

идентификация критически важна, так как риск, который не был идентифицирован на этой стадии, не будет включен в дальнейший анализ.

Идентификация должна охватывать все риски (находится ли их источник под контролем организации или нет), даже если источник риска или его причина неочевидны. Идентификация риска должна включать проверку цепной реакции некоторых определенных последствий, включая каскадный эффект и суммарные действия. Она также должна рассматривать широкий спектр последствий, даже если источник риска или его причина неясны. Наряду с идентификацией возможных последствий необходимо рассматривать возможные причины и сценарии, которые могут указать на предположительные последствия. Все значимые причины должны быть приняты во внимание.

Организация должна применять инструменты и техники идентификации рисков, которые соответствуют ее целям и возможностям, а также рискам, с которыми она столкнулась. Соответствующая и актуальная информация очень важна при идентификации рисков. Она по возможности должна включать в себя и общую информацию. Работники, обладающие соответствующими знаниями, должны быть вовлечены в процесс идентификации рисков.

5.4.3 Risk analysis

Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk.
Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is

5.4.3 Анализ риска

Чтобы проанализировать риск, необходимо прийти к его пониманию. Анализ риска предоставляет входы для оценки степени риска и обсуждений по вопросам необходимости проведения обработки риска, а также стратегий и методов его обработки. Анализ риска может также предоставлять входы для принятия решений по рискам разных типов и уровней, особенно тех, где стоит выбор.

Анализ рисков включает в себя рассмотрение причин и источников риска, его положительных и отрицательных последствий и вероятности возникновения этих последствий. Факторы, которые влияют на последствия и вероятность должны быть определены. Риск анализируется путем определения последствий и их вероятности, а также других сопутствующих риску характеристиках. Рисковой случай может повлечь

analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.
The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different risks and their sources.
The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and, as appropriate, other stakeholders. Factors such as divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modelling should be stated and can be highlighted.
Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.
Consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data.
Consequences can be expressed in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.

за собой множественные последствия и может отразиться на множестве целей. Существующие методы управления, их эффективность и достаточность также должны приниматься во внимание.

То, как выражаются последствия и вероятность и то, как они комбинируются при определении уровня риска – должно отражать тип риска, доступную информацию и цель, для которой используется выход процесса обработки риска. Все это должно соответствовать критериям риска. Также важно учитывать независимость различных риском и их источников.

Достоверность при определении уровня риска и его чувствительности к предварительным условиям и предположениям должна быть неотъемлемой частью анализа, и доводиться до сведения тех, кто принимает решения и, соответственно, заинтересованным лицам. Таки факторы как расхождения во мнениях экспертов, неуверенности, доступность, качество, количество и постоянная актуальность информации, или ограничения при моделировании должны быть четко сформулированы и выведены на первый план.

Анализ риска может быть предпринят с различными видами деталей, в зависимости от риска, цели анализа, и информации, данных и доступных ресурсов. Анализ может быть качественным, полуколичественным или количественным, или их сочетанием, в зависимости от обстоятельств.

Consequences and their likelihood can be determined by modeling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.
Последствия и их вероятность могут быть определены моделированием результатов рискового случая или случаев, или экстраполяцией экспериментальных исследований или доступных данных. Последствия могут быть выражены материально и нематериально. В некоторых случаях, больше чем одна числовая ценность или признак обязаны определять последствия и их

5.4.4 Risk evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.
Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.
Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk.
Decisions should be made in accordance with legal, regulatory and other requirements.
In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls.
This decision will be influenced by the organization's risk attitude and the risk criteria that have been established.

5.5 Risk treatment
5.5.1 General

Risk treatment involves selecting one or more options for modifying risks, and implementing those options.
Once implemented, treatments provide or modify the controls.
Risk treatment involves a cyclical process of:
- assessing a risk treatment;
- deciding whether residual risk levels are tolerable;
- if not tolerable, generating a new risk treatment; and
- assessing the effectiveness of that

вероятность в течение различных времен, мест, групп или ситуаций.

5.4.4 Определение степени риска

Цель определения степени риска состоит в содействии при принятии решений, основанных на выходах анализа риска, а именно, какие риски необходимо обработать и приоритетность в применении обработки.

Определение степени риска включает в себя сравнение уровня обнаруженного в процессе анализа риска с критериями риска, определенными при установлении контекста. Необходимость обработки рассматривается на основании такого сравнения.

Решения должны принимать во внимание более широкий контекст риска и включать в себя рассмотрение умеренности риска, имеющего отношении к сторонам, за исключением тех организаций, которые от риска только выиграют.
Решения должны приниматься в соответствии с законодательными, нормативными иными требованиями.

В некоторых обстоятельствах, оценка степени риска может привести к тому, что будет необходим дополнительный анализ. Также, оценка степени риска может привести к решению не обрабатывать риск, а поддерживать его в существующем состоянии.
На такое решение может повлиять отношение организации к рискам и установленным для него критериям.

5.5 Обработка риска
5.5.1 Общие положения

Обработка риска включает в себя одну или более позиций модификации рисков, и применение таких модификаций.
Как только они были применены, методы обработки предоставляют или модифицируют способы управления.
Обработка риска включает циклический процесс:
- ✓ Оценки обработки риска;
- ✓ Принятия решения о допустимости существующего риска;
- ✓ Генерации нового способа обработки, если риск недопустим; и
- ✓ Оценки эффективности обработки.

treatment.
Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options
can include the following:
a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
b) taking or increasing the risk in order to pursue an opportunity;
c) removing the risk source;
d) changing the likelihood;
e) changing the consequences;
f) sharing the risk with another party or parties (including contracts and risk financing); and
g) retaining the risk by informed decision.

5.5.2 Selection of risk treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of
implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as
social responsibility and the protection of the natural environment. Decisions should also take into account
risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative
consequence) but rare (low likelihood) risks.
A number of treatment options can be considered and applied either individually or in combination. The
organization can normally benefit from the adoption of a combination of treatment options.
When selecting risk treatment options, the organization should consider the values and perceptions of
stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can
impact on risk elsewhere in the organization or with stakeholders, these should be involved in the decision.
Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

Способы обработки риска необязательно исключают друг друга, и не обязательно уместны при всех обстоятельствах. Способы могут включать:
a) Избежание риска путем решения не начинать или не продолжать деятельность, приведшую к риску;
b) Взятие на себя риска или повышение его уровня чтобы использовать возможность;
c) Уничтожение источника риска;
d) Изменение вероятности;
e) Изменение последствий;
f) Распределение риска с другой стороной или сторонами (включая контракты и финансирование риска); и
g) Обоснованным решением принятие на себя страхового риска.

5.5.2 Выбор опций обработки риска

Выбор наиболее целесообразной опции обработки риска включает в себя балансировку цен и попыток внедрения относительно выгод, в соответствии с юридическими, нормативными и иными требованиями, такими как социальная ответственность и защита окружающей среды. Решения должны также принимать во внимание риски, которые могут потребовать ту обработку риска, которая не будет оправдана с экономической точки зрения, например тяжелые риски (влекущие за собой крайне негативные последствия), но редкие (с низкой вероятностью).

Некоторые опции обработки могут быть приняты во внимание и применены совместно или по отдельности. Организация, как правило, может извлечь выгоду при применении совокупности опций обработки рисков.

При выборе опции обработки риска, организация должна принять во внимание ценности и восприятия заинтересованных сторон, и наиболее подходящие способы коммуникации с ними. Там, где опции обработки риска могут повлиять на риски вне организации или в отношениях с заинтересованными сторонами, это также должно во внимание. И, хотя, опции обработки риска одинаково эффективны, некоторые из них могут быть более допустимы для некоторых заинтересованных сторон, чем другие.

План по обработке рисков должен ясно

The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk. The link between the two risks should be identified and maintained.

идентифицировать приоритетный порядок в котором будут применяться отдельные опции обработки риска.

Обработка риска сама по себе может вызвать риск. Значительным риском может быть ошибка или неэффективности мер обработки рисков. Мониторинг должен быть неотъемлемой частью плана по обработке риска, как гарантия того что предпринимаемые меры по прежнему эффективны.

Обработка риска может повлечь за собой вторичные риски, которые также необходимо рассматривать, обрабатывать, за которыми необходимо следить и анализировать. Таки вторичные риски должны быть включены в тот же план по обработке рисков, как и первоначальные риски, таким образом нет никакой необходимости в обработке такого риска как нового. Связь между двумя рисками необходимо идентифицировать и поддерживать.

5.5.3 Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented.

The information provided in treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- resource requirements including contingencies;
- performance measures and constraints;
- reporting and monitoring requirements; and
- timing and schedule.

Treatment plans should be integrated with the management processes of the organization and discussed with appropriate stakeholders.

Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring,

5.5.3 Подготовка и внедрение планов обработки риска

Цель планов по обработке риска – документировать то, как выбранная опция обработки риска будет применена.

Информация, которая предоставляется в планах по обработке должна включать:

- ✓ Причины выбора опций обработки, включая ожидаемые выгоды;
- ✓ Тех, кто несет ответственность по утверждению плана, и тех кто ответственен за внедрение такого плана;
- ✓ Предлагаемые действия;
- ✓ Ресурсные требования, включая нештатные ситуации;
- ✓ Меры эффективности и ограничения;
- ✓ Требования по отчетности и мониторингу; и
- ✓ Временные рамки и планы-графики.

Планы обработки должны быть интегрированы с процессами управления внутри организации и должны обсуждаться с заинтересованными сторонами.

Те, кто принимают решения и заинтересованные стороны должны осознавать природу и степень остаточного риска после его обработки.

Остаточный риск должен быть документирован. К такому риску должен быть применен мониторинг, оценка, и если применимо, то дополнительная обработка.

review and, where
appropriate, further treatment.

5.6 Monitoring and review

Both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or *ad hoc*.

Responsibilities for monitoring and review should be clearly defined.

The organization's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

– ensuring that controls are effective and efficient in both design and operation;
– obtaining further information to improve risk assessment;
– analyzing and learning lessons from events (including near-misses), changes, trends, successes and failures;
– detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and
– identifying emerging risks.

Progress in implementing risk treatment plans provides a performance measure. The results can be incorporated into the organization's overall performance management, measurement and external and internal reporting activities.

The results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the risk management framework (see 4.5).

5.7 Recording the risk management process

Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Decisions concerning the creation of records should take into account:

– the organization's needs for continuous

5.6 Мониторинг и анализ

Как мониторинг, так и оценка должны быть спланированы в ходе процесса риск-менеджмента и должны подвергаться регулярной проверке и надзору. Они могут носить как периодический, так и ситуативный характер.

Ответственности по мониторингу и анализу должны быть четко определены.

Процессы организации по мониторингу и анализу должны включать все аспекты процесса риск менеджмента с целью:

- ✓ Гарантии того, что методы управления эффективны и достаточны как при разработке, так и при функционировании;
- ✓ Приобретения дополнительной информации в целях улучшения оценки риска
- ✓ Анализа и извлечения уроков из рисковых случаев (включая инциденты), изменения, течения, удачи и провалы;
- ✓ Обнаружения изменений во внешнем и внутреннем контексте, включая изменениям в критериях риска и самом риске, который может потребовать проверки обработки риска и приоритетов; и
- ✓ Идентификации появляющихся рисков.

Прогресс в применении планов по обработке рисков представляет собой меру эффективности. Результат может быть включен в общий менеджмент эффективности внутри организации, измерения, внешние и внутренний отчетные мероприятия.

Результаты мониторинга и анализа должны быть записаны и должным образом донесены до сведения внешних и внутренних заинтересованных сторон, и также должны быть использованы как входа анализа концепции риск-менеджмента (см. 4.5).

5.7 Запись процессов риск-менеджмента

Мероприятия по риск-менеджменту должны быть доступны для анализа. В процессе риск-менеджмента записи представляют собой основу улучшения методов и инструментов, так де как и процесса в целом.

Решения, касающиеся создания записей должны принимать во внимание:

- ✓ Потребности организации в непрерывном обучении;

learning;
– benefits of re-using information for management purposes;
– costs and efforts involved in creating and maintaining records;
– legal, regulatory and operational needs for records;
– method of access, ease of retrievability and storage media;
– retention period; and
– sensitivity of information.

- ✓ Преимущества от повторного использования информации в управленческих целях;
- ✓ Затраты на и попытки создания и поддержания записей;
- ✓ Юридические, нормативные и операционные потребности записей;
- ✓ Метод оценки, доступность извлечения и способы хранения;
- ✓ Период хранения; и
- ✓ Конфиденциальность информации.

Annex A
(informative)
Attributes of enhanced risk management

Приложение А
(информативное)
Свойства улучшенного риск менеджмента

A.1 General
All organizations should aim at the appropriate level of performance of their risk management framework in line with the criticality of the decisions that are to be made. The list of attributes below represents a high level of performance in managing risk. To assist organizations in measuring their own performance against these criteria, some tangible indicators are given for each attribute.

A.1 Общие положения
Все организации должны стремиться к высокому уровню эффективности концепции риск-менеджмента, согласующейся с принимаемыми решениями. Ниже приведен список признаков высокого уровня эффективности в управлении рисками. Чтобы помочь организациям в измерении их эффективности относительно этих критериев ниже приведены принципиальные индикаторы каждого признака.

A.2 Key outcomes
A.2.1 The organization has a current, correct and comprehensive understanding of its risks.
A.2.2 The organization's risks are within its risk criteria.

A.2 Ключевые выходы
A.2.1 Организация обладает актуальным, правильным и исчерпывающим понимание рисков.
A.2.2 Риски организации соответствуют ее критериям рисков

A.3 Attributes
A.3.1 Continual improvement
An emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.
This can be indicated by the existence of explicit performance goals against which the organization's and

A.3 Признаки
A.3.1 Постоянное улучшение

Упор делается на постоянное улучшение риск-менеджмента, путем постановки целей организации, измерений, анализа и дальнейшей модернизации процессов, систем, ресурсов, возможностей и навыков.

Все это может быть подчеркнуто существованием открытых целей в области производительности, что измеряется в индивидуальной производительности организации и отдельных ее менеджеров. Производительность организации может быть измерена и доведена до сведения заинтересованных лиц. Обычно, анализ производительности имеет место быть по крайней

individual manager's performance is measured. The organization's performance can be published and communicated. Normally, there will be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.
This risk management performance assessment is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

A.3.2 Full accountability for risks
Enhanced risk management includes comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. Designated individuals fully accept accountability, are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders.
This can be indicated by all members of an organization being fully aware of the risks, controls and tasks for which they are accountable. Normally, this will be recorded in job/position descriptions, databases or information systems. The definition of risk management roles, accountabilities and responsibilities should be part of all the organization's induction programmes.
The organization ensures that those who are accountable are equipped to fulfil that role by providing them with the authority, time, training, resources and skills sufficient to assume their accountabilities.

мере раз в год, а затем происходит проверка процессов, постановка проверенных целей в области производительности на следующий период.

Такая оценка эффективности риск-менеджмента – неотъемлемая часть всей оценки производительности организации и системы измерений отделов и отдельных сотрудников.

A.3.2 Полная ответственность за риски

Улучшенный риск-менеджмент включает всеобъемлющую, полностью определенную и полностью допустимую ответственность за риски, методы управления и задачи по обработке рисков. Уполномоченный работники в полной степени принимают ответственность, они обладают достаточными навыками и располагают уместными ресурсами для проверки систем управления, мониторинга рисков, улучшения управления, а также способны эффективно доводить риски до сведения внутренних и внешних сторон.

Все это может быть отмечено всеми членами организации при условии, что они полностью осведомлены о рисках, методах управления и задач, по которым они несут ответственность. Обычно это записывается в должностных инструкциях, базах данных или информационных системах. Определение ролей риск-менеджмента, обязанностей и ответственностей должно быть частью программ по введению должностей в организации.

Организация дает гарантию того, что те, кто несут ответственность, полностью снабжены полномочиями, временем, обучением, ресурсами и навыки, достаточными для выполнения их обязательств.

A.3.3 Внедрение риск-менеджмента в процесс принятия решений

Все решения, принимаемые внутри организации, независимо от уровня значимости и важности, требуют открытого рассмотрения рисков и применения риск-менеджмента до некоторой требуемой степени.

Это может быть отмечено записями совещаний и

A.3.3 Application of risk management in all decision making

All decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree.

This can be indicated by records of meetings and decisions to show that explicit discussions on risks took place. In addition, it should be possible to see that all components of risk management are represented within key processes for decision making in the organization, e.g. for decisions on the allocation of capital, on major projects and on re-structuring and organizational changes. For these reasons, soundly based risk management is seen within the organization as providing the basis for effective governance.

A.3.4 Continual communications

Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.

This can be indicated by communication with stakeholders as an integral and essential component of risk management. Communication is rightly seen as a two-way process, such that properly informed decisions can be made about the level of risks and the need for risk treatment against properly established and comprehensive risk criteria.

Comprehensive and frequent external and internal reporting on both significant risks and on risk management performance contributes substantially to

решений, в целях показа того, что открытые обсуждения по рискам имели место. Более того, должна присутствовать возможность увидеть что все компоненты риск-менеджмента представлены в соответствии с ключевыми процессами принятия решений в организации, например обсуждения по поводу распределения капитала, по главным проектам, по реструктуризации и изменениям внутри организации. По этим причинам, научно-методологический риск-менеджмент видится в пределах организации как основа эффективного управления.

A.3.4 Постоянные коммуникации

Улучшенный риск-менеджмент включает постоянные коммуникации с внешними и внутренними заинтересованными сторонами, включая всеобъемлющее и частое предоставление отчетов по эффективности риск-менеджмента, как части надлежащего управления.

Это может быть отмечено коммуникацией с заинтересованными сторонами как неотъемлемая и естественная часть риск-менеджмента. Коммуникация видится как двусторонний процесс, так, чтобы должным образом информированные решения могут быть сделаны относительно уровня риска и необходимости его обработки относительно должным образом установленных и современных критериев риска.

Исчерпывающая и регулярная внутренняя и внешняя отчетность и по значительным рискам, и по эффективности риск-менеджмента в свою очередь делает вклад в эффективное управление внутри организации.

A.3.5 Полная интеграция в структуру управления организации

Риск-менеджмент рассматривается как центральный процесс управления в организации, такой, при котором риски рассматриваются в свете влияния несоответствий на цели. Структура управления и процесс основаны на управлении рискам. Эффективный риск-менеджмент считается руководителями естественным средством достижения целей организации.

Это подтверждается языком руководителей и

effective governance within an organization.

A.3.5 Full integration in the organization's governance structure

Risk management is viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization's objectives. This is indicated by managers' language and important written materials in the organization using the term "uncertainty" in connection with risks. This attribute is also normally reflected in the organization's statements of policy, particularly those relating to risk management. Normally, this attribute would be verified through interviews with managers and through the evidence of their actions and statements.

Bibliography

[1] ISO Guide 73:2009, *Risk management — Vocabulary*
[2] ISO/IEC 31010, *Risk management — Risk assessment techniques*

важными письменными материалами организации, использующей термин «неясности» применительно к рискам. Этот признак также отражается в политике организации, особенно той, что относится к риск-менеджменту. Как правило, этот признак верифицируется путем проведения интервью с руководителями и путем освидетельствования из действий и утверждений.

Библиография

[1] Руководство ISO 73:2009, *Риск-менеджмент - Словарь*
[2] ISO/IEC 31010, *Риск-менеджмент — Техники оценки риска*