ФЕДЕРАЛЬНОЕ АРХИВНОЕ АГЕНТСТВО
(РОСАРХИВ)

ФЕДЕРАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ДОКУМЕНТОВЕДЕНИЯ И АРХИВНОГО ДЕЛА
(ВНИИДАД)

УТВЕРЖДАЮ
Руководитель Росархива
_____ А.Н. Артизов
«____» _____ 2014 г.

ОТЧЕТ
О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

по теме 2.2.1 плана НИОКР:

«Исследование международных стандартов и проектов международных стандартов ИСО по управлению документами за 2013 г., определение целесообразности разработки на их основе соответствующих национальных стандартов Российской Федерации»
(заключительный)

Директор ВНИИДАД,
д.и.н., профессор _____ М.В. Ларин

«28» ноября 2014 г.

Руководитель темы
Зав. отделом документоведения,
к.и.н., профессор _____В.С. Мингалев

«28» ноября 2014 г.

Москва - 2014

СПИСОК ИСПОЛНИТЕЛЕЙ

Директор ВНИИДАД, д.и.н., профессор	_____	М.В. Ларин
Зам. директора ВНИИДАД, к.и.н. доцент	_____	В.Ф. Янковая
Руководитель темы, Зав. отделом документоведения, к.и.н., профессор	_____	В.С.Мингалев
Зав. сектором, к.и.н., доцент	_____	Н.Г. Суровцева
Инженер-проектировщик		А.П.Терентьев
	_____	
Инженер-проектировщик	_____	Н.И. Ивановский
Мл. науч. сотр.	_____	А.Г. Бороздина

РЕФЕРАТ

Объем 28 с., прил. 2.

ДОКУМЕНТ, ДОКУМЕНТАЦИЯ, УПРАВЛЕНИЕ ДОКУМЕНТАМИ, СИСТЕМА УПРАВЛЕНИЯ ДОКУМЕНТАМИ, ТРЕБОВАНИЯ К СИСТЕМАМ УПРАВЛЕНИЯ ДОКУМЕНТАМИ, МЕЖДУНАРОДНЫЙ СТАНДАРТ

Объектом исследования являются проекты международных стандартов и технических отчетов ИСО по управлению документами на каждом из этапов разработки и обсуждения, разрабатываемые Международной организацией по стандартизации (ИСО) в профильном техническом подкомитете ИСО/ТК46/ПК 11 «Управление документами/архивами» и взаимодействующих с ним комитетах в 2013 году.

Источниковой базой исследования послужили оригиналы проектов международных стандартов ИСО, полученные через официальную рассылку секретаря ИСО/ТК 46/ ПК 11 ответственным исполнителем данной темы, как полноправным членом этого подкомитета ИСО.

В работе над обзором применялся аналитический метод исследования.

Результатом работы является отчет по НИР, содержащий предложения о целесообразности разработки национальных стандартов РФ на базе международных стандартов ИСО, разработанных ИСО/ТК46/ПК 11 в 2013 году.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 5
1. ОБЗОР ПРОЕКТОВ МЕЖДУНАРОДНЫХ СТАНДАРТОВ И ТЕХНИЧЕСКИХ ОТЧЕТОВ ИСО, РАЗРАБАТЫВАЕМЫХ В 2013 ГОДУ ПК 11 «УПРАВЛЕНИЕ ДОКУМЕНТАМИ/АРХИВАМИ»ИСО/ТК 46 «ИНФОРМАЦИЯ И ДОКУМЕНТАЦИЯ» 9
1.1. Развитие проекта «Система управления документами» в стандартах ИСО серии 30300 ... 9
1.2. Пересмотр ISO 15489 «Информация и документация. Управление документами. Часть 1. Общие положения» 16
2. ОБЗОР ПРОЕКТОВ МЕЖДУНАРОДНЫХ СТАНДАРТОВ И ТЕХНИЧЕСКИХ ОТЧЕТОВ ИСО, РАЗРАБАТЫВАЕМЫХ В 2013 ГОДУ ТЕХНИЧЕСКИМИ КОМИТЕТАМИ, ВЗАИМОДЕЙСТВУЮЩИМИ С ТК46 19
ЗАКЛЮЧЕНИЕ 25
СПИСОК ИСТОЧНИКОВ 27
ПРИЛОЖЕНИЕ А 29
ПРИЛОЖЕНИЕ Б 32

ВВЕДЕНИЕ

Разработка международных норм и стандартов в сфере информации и документации в Международной организации по стандартизации осуществляется Техническим комитетом (ТК) № 46 «Информация и документация», в работе которого принимают участие 34 национальных комитета - члена ИСО, в числе которых и Федеральное агентство по техническому регулированию и метрологии (Ростехрегулирование). Российские специалисты (ВНИИДАД), являющиеся экспертами ИСО с правом голоса от России, осуществляют свою деятельность в составе ПК 11 «Управление документами/ архивами» данного комитета.

В рамках ТК46/ПК11 работает пять рабочих групп (WG) деятельность которых и определяет основные направления стандартизации в сфере архивов и управления документами:

SWG Координационная рабочая группа

WG 01 Метаданные

WG 07 Международная рабочая группа по сохранению цифровых документов

WG 08, WG 09 Система управления документами

WG 10 Рекомендации по внедрению отбора и передачи документов

WG 13 Пересмотр ИСО 15489-1 и ИСО/ТО 15489-2.

В 2013 году наиболее активно шла работа по направлениям, связанным с развитием системы управления документами, разработкой рекомендаций по отбору и передаче документов на последующее хранение или уничтожение, идентификацией рисков и их оценкой для документных систем и пересмотром стандарта 15489. Вместе с тем следует обратить внимание на проведенное голосование по необходимости пересмотра стандарта ISO 23081-2:2009 «Информация и документация – Управление метаданными документов – Часть 2: Концептуальные вопросы и вопросы внедрения» (Information and documentation - Managing metadata for records - Part 2: Conceptual and implementation issues), а также на резолюцию июльского заседания ТК 46, в которой говорится о необходимости пересмотра терминологического стандарта ISO 5127 «Информация и документация. Словарь» (Information and documentation – Vocabulary), восстановлении в проекте данного стандарта перевода каждого английского термина на французский язык и необходимости согласования этой работы со стандартами ТК 37 «Терминология.

(Принципы и координация)», что свидетельствует о планомерной работе других рабочих групп комитета.

Целью работы является изучение передового международного опыта по стандартизации процессов управления документами и информирование о нем отечественных специалистов, а также выработка позиции ВНИИДАД по вопросу о целесообразности разработки на основе вышеперечисленных международных стандартов национальных стандартов России.

Основными задачами работы являлись:

- изучение проектов международных стандартов и технических отчетов ИСО на всех стадиях их разработки* в ИСО/ТК46/ПК11 и взаимодействующих с ним комитетах;

- краткое аннотирование проектов стандартов, относящихся к тематике работы отдела документоведения ВНИИДАД;

- анализ целесообразности использования утвержденных международных стандартов ИСО в России путем разработки на их основе национальных стандартов, либо достаточности осуществления их официальных переводов.

Источниковой базой отчета послужили проекты международных стандартов и технических отчетов ИСО на английском языке, полученные через официальную рассылку секретаря ИСО/ТК46/ПК11 «Управление документами/ архивами» руководителем (М.В.Лариным) и ответственным исполнителем (Л.Н.Варламовой) данной темы НИР, как полноправными членами этого подкомитета ИСО с правом голоса от России. Помимо них большое значение для понимания общих тенденций развития международной стандартизации имеют другие материалы справочно-информационного характера (отчеты о деятельности комитетов, презентации продуктов стандартизации, электронные журналы и пресс-релизы и др.), которые содержат дополнительную информацию, позволяющее лучше понять актуальность, универсальность, обоснованность тех или иных решений в области стандартизации.

Особенностью деятельности ИСО как международной организации по стандартизации является организация эффективного взаимодействия комитетов, предлагающих решения в смежных областях и профессиональных сферах. Это решается за счет обязательной рассылки проектов стандартов и технических отчетов

* Международные согласованные коды стадий разработки стандарта приведены в Приложении А

этих комитетов не только с целью ознакомления, но и внесения предложений, возможного учета их положений в своей нормотворческой деятельности, а может быть даже некоторой корректировки методологических позиций. Для ТК 46/ПК 11 таким комитетом является главным образом ТК 171 «Прикладные системы создания и хранения документов», но и ТК 154 «Документы и информация в управлении, торговле и промышленности» и ТК 10 «Техническая документация на продукцию» и др. информируют о результатах своей деятельности.

Кроме того, ИСО осуществляет взаимодействие с рядом международных организаций по координации деятельности в электронном бизнесе (Memorandum of Understanding Electronic Business Management Group Referene: MoU/MG). Среди вопросов требующих координации, наиболее важными признаются, в том числе, проблемы координации работ по цифровой подписи, выработка общих подходов по «онлайн-терминологии», стандартизация требований в отношении облачных технологий, развитие электронного правительства и др. Поскольку документация является непременным атрибутом функционирования любой организации стандарты в области информации и документации должны отражать эти аспекты. Очевидно, следствием именно этой тенденции стала необходимость пересмотра стандартов ИСО 15489. Возникнув как признание лучшего национального опыта в отдельной отрасли, они должны трансформироваться в универсальную методологию управления документами в организации.

Еще одним интересным источником для анализа международной стандартизации в области информации, документации и архивного хранения является электронный журнал ISO/CASCO Комитета ИСО по оценке соответствия (ISO Committee on conformity assessment). Поскольку в круг полномочий этого комитета входит изучение средств оценки на соответствие различных систем управления требованиям стандартов соответствующих систем при проведении сертификации, то с принятием стандартов ИСО серии 30300, требования ISO/CASCO также становятся актуальными при сертификации по стандарту 30301.

На страницах этого журнала не только представлена актуальная информация о сертификации различных организаций на соответствие различным системам менеджмента, но и последовательно продвигаются механизмы по реализации согласованного подхода к деятельности по оценке соответствия, для гармонизации

которого ISO/CASCO разработал инструментарий, содержащий нормы и руководства.

Все представленные материалы обусловили структуру аналитического отчета, первая глава которого посвящена работе над стандартами и техническими отчетами ТК 46/ ПК11, а во второй рассматриваются актуальные аспекты, которые содержатся в стандартах смежных технических комитетов и имеют значение для формирования методологических подходов к стандартизации в сфере документации.

Косвенная экономическая эффективность и значимость плановой работы по НИР заключается в использовании передового международного опыта по управлению документами; гармонизации национальной базы стандартов с международными аналогами; облегчении подготовки официальных переводов этих стандартов, а в случае принятия положительного решения вопроса о целесообразности их внедрения в РФ – разработки национальных стандартов

1. ОБЗОР ПРОЕКТОВ МЕЖДУНАРОДНЫХ СТАНДАРТОВ И ТЕХНИЧЕСКИХ ОТЧЕТОВ ИСО, РАЗРАБАТЫВАЕМЫХ В 2013 ГОДУ ПК 11 «УПРАВЛЕНИЕ ДОКУМЕНТАМИ/АРХИВАМИ» ИСО/ТК 46 «ИНФОРМАЦИЯ И ДОКУМЕНТАЦИЯ»

1.1. Развитие проекта «Система управления документами» в стандартах ИСО серии 30300

Как мы уже говорили выше, работа в подкомитете осуществляется рабочими группами одновременно по нескольким направлениям. Одним из основных направлений работы в 2013 году стало дальнейшее развитие проекта по созданию системы управления документами серии стандартов ISO 30300. Данный проект был подробно представлен в предыдущих отчетах НИР[*]. В 2013 году предметом рассмотрения стал стандарт ИСО 30302 «Информация и документация. Системы управления документами. Руководство по внедрению» (Information and documentation – Management systems for records – Guidelines for implementation), содержащий практическое руководство по внедрению и использованию систем управления документами, созданных на базе ИСО 30301. В 2012 году проект стандарта получил свое развитие, но так и не вышел за рамки концепции, оставшись на стадии предложения рабочей группы (WI). Вместе с тем, разработчики предложили на рассмотрение экспертов 8 принципов которыми, по их мнению, следует руководствоваться при внедрении систем управления документами, и запросили мнение экспертов по ним. Поскольку большинство экспертов посчитали необходимым уточнить предлагаемые принципы и провести повторное голосование, его доработка была перенесена на 2013 год.

Именно поэтому при представлении проекта данного стандарта в 2013 году разработчики особенно подробно остановились на его обосновании.

---

[*] См. отчет НИР «Участие в разработке международных стандартов ИСО по управлению документами серии 30300 «Информация и документация. Системы управления документами («Information and documentation. Records management systems»), подготовленный сектором стандартизации отдела документоведения ВНИИДАД в 2010 г., а также отчет НИР «Обзор международных стандартов и проектов международных стандартов ИСО по управлению документами за 2012 год, определении целесообразности разработки на их основе соответствующих национальных стандартов Российской Федерации», подготовленный сектором стандартизации отдела документоведения ВНИИДАД в 2012 г.

ISO 30302 может использоваться в качестве руководства для реализации системы управления документами (СУД) организацией, частью организации, или двумя или более организациями с общими бизнес-процессами. Он может быть использован для: а) разработки, внедрения, поддерживания в актуальном состоянии и улучшения СУД; б) подтверждении в соответствии заявленной политики; в) подготовки организации для демонстрации соответствия ИСО 30301.

Этот стандарт предназначен для использования в сочетании с ISO 30300 и ISO 30301. Кроме того, он взаимосвязан с ISO 15489-1: 2001 «Информация и документация - Управление документами. Часть 1. Общие положения», ISO / TR 15489-2: 2001 «Информация и документация - Управление записями. Часть 2: Руководящие принципы», ISO TR 26122: 2008 «Информация и документация - Анализ рабочих процессов для документов», ISO 19011: 2011 «Руководящие указания по аудиту систем управления».

Разработка ISO 30302 велась двумя рабочими группами (WG8 и 9), созданными специально для работы над серией стандартов по системам управления документами: 60 человек было назначено в качестве экспертов для WG 8, и 58 человек для WG9. Разработчики постарались более полно представить сформулированные ранее принципы, особенно подробно остановившись на первом из них, представляющим актуальность данного стандарта. Для раскрытия этого принципа потребовалось выявить и представить все заинтересованные стороны, к числу которых относятся организации различных типов и размеров и должностные лица, принимающие решения в рамках организации, которые используют стандарты для улучшения бизнес-процессов и подотчетности.

Актуальность данного стандарта обусловлена также и тем, что многие потенциальные пользователи, ознакомившись с принятыми в 2011 году ISO 30301 просят инструкции по внедрению, каковыми по сути и является стандарт ISO 30302.

Обращается внимание на то обстоятельство, что предлагаемый ISO 30302 необходим для поддержки системы управления новой области и позволит повысить уровень совместимости и интероперабельности при внедрении различных систем управления в рамках организации. Управление документами является областью организационного управления, которой ранее не осмысливалась и практически не рассматривалась как система.

Поскольку документы, как один из видов информации, являются активами организации, которые позволят ей добиться эффективного ведения бизнеса, управления рисками и способности реагировать на вызовы в открытом и глобальной окружающем мире, использование ISO 30302 возможно для малых, средних и крупных организаций в любой отрасли. Он обеспечивает:

– общее управление с учетом политики и практики в различных странах, с разной культурой и юрисдикцией;

– соблюдение законодательства и защиты в суде, в том числе поддержку судебной практики;

– возможность удовлетворения нормативных требований, в том числе этических и корпоративных требований управления, соответствие нормативным требованиям в сфере финансовой отчетности и практики проверок;

– соблюдение национального и международного законодательства и кодексов поведения;

– поддержку управления рисками, в том числе обеспечение безопасности;

– возможность установки и оценки показателей эффективности и включения их в коммерческие контракты;

– возможности поддержки других наиболее часто используемых серий стандартов на системы управления, например, ISO 9000;

– реализацию скоординированного, последовательного и комплексного подхода к созданию политики, целей, задач и методов реализации в масштабе всей организации;

– демонстрацию приверженности улучшению оказания услуг, управления ресурсами и контроля затрат;

– потенциал сделать организацию более рентабельной и эффективной;

– повышение согласованности предоставления услуг на основе подлинной, достоверной и полезной информации.

Разработчики отмечают, что подобные документы или руководства не существует ни в одной стране на национальном уровне и могут способствовать значительному облегчению связей между различными странами для решения общих проблем.

Стоимость внедрения стандарта соизмерима с масштабом каждой организации и определяется потребностями бизнеса и оценкой рисков, а сокращение расходов

может быть достигнуто путем комплексного осуществления СУД с другой системой управления, принятой в организации.

Интересно, что разработчики проекта стандарта видят ожидаемую ценность для общества от его внедрения через развитие проектов электронного ведения бизнеса и электронного правительства, отмечая повышение эффективности и оперативности правительства, подотчетность системы управления государственных, частных и некоммерческих организаций, соблюдение международных договоров и законодательства на любом уровне, создание надежных условий для ведения бизнеса между правительством и гражданами, и бизнесом и гражданами, в частности с участием в электронном взаимодействии, а также улучшение доступа к информации и сохранение коллективной памяти.

Другие принципы[*] были разъяснены, но раскрыты менее подробно.

Стандарт состоит из десяти разделов, первые три носят традиционный характер и содержат область применения, ссылки на нормативные документы, в которых указано взаимодействие со стандартами ISO 30300 и ISO 30301, а также термины и определения, используемые в данном стандарте и соответствующие терминологии ISO 30300. В четвертом разделе «Контекст организации», раскрывается важность понимания контекста деятельности организации, включающего особенности сферы деятельности, наличие внутренних и внешних факторов, масштаб организации, для определения рамок внедрения стандарта, определяются внешние и внутренние источники, на основе которых можно говорить о контексте организации и, наконец, определение сферы применения СУД. При этом каждый этап анализа контекста деятельности организации требует на выходе формирования соответствующих документов, подтверждающих выполненные действия, что соответствует принципам процессного подхода к управлению.

Пятый раздел посвящен роли высшего руководства организации в реализации СУД. Этот раздел очень важен для всех стандартов на системы управления, поскольку именно от понимания высшим руководством, реализацией им своих обязательств по распределению ресурсов, установлению связей, осуществлению анализа системы, зависит результативность и эффективность внедрения всей системы

[*] Отчет НИР «Обзор международных стандартов и проектов международных стандартов ИСО по управлению документами за 2012 год, определении целесообразности разработки на их основе соответствующих национальных стандартов Российской Федерации». ВНИИДАД, 2013. С. 14.

управления документами. На практике это должно быть реализовано через разработку политики, в которой отражены общие стратегические аспекты по управлению документами в организации, а также через распределение ответственности, причем как на уровне руководства, так и на уровне исполнителей.

Шестой раздел раскрывает вопросы планирования деятельности, которые базируются на анализе внутренних и внешних факторов, определяющих контекст деятельности организации, и определении на их основе возможностей и угроз, особое внимание при этом должно быть уделено управлению рисками.

В седьмом разделе «Поддержка» раскрываются механизмы, которые обеспечивают поддержку внедрения и развития системы управления документами. К ним относятся ресурсы (инфраструктура, человеческие, финансовые ресурсы, средства логистики и др.), компетентность, осведомленность и обучение персонала, а также определенные коммуникационные процедуры, в которых должны быть определены:

– сфера и содержание взаимодействия;

– способы коммуникации;

– ответственность в сфере взаимодействия;

– методы оценки эффективности коммуникации.

Основой взаимодействия относительно СУД является документация, поэтому и предметом этого взаимодействия должны быть роли и обязанности, расположение и доступ к документации о СУД, содержание операционных процедур, связанных с документированием процессов, средств управления и систем и источники помощи в соблюдении политики управления документами, целей и оперативных элементов, связанных с поддержкой системы.

Документация СУД включает в себя:

– сферу применения СУД,

– документированную политику,

– документированные цели,

– отношения между СУД и другими системами управления, реализованными в организации, или в других организациях,

– процедуры в соответствии с требованиями ISO 30301,

– документацию по планированию, эксплуатации и управления процессами СУД, которая будет зависеть от размера организации и сферы применения СУД.–

документы по контролю над СУД, которые определены ISO 30301 (п. 7.5.1, 7.5.2 и «Приложение А»).

В восьмом разделе «Операции» речь идет о необходимости разработки процедур по планированию и управлению процессами в рамках СУД. Они должны быть разработаны специально для каждой организации. Организация планирует работу СУД путем установления процессов документирования, которые будут реализованы, определения критериев выполнения этих процессов и описания (на уровне необходимой детализации) различных видов деятельности, ее результатов, участвующих в ней систем и исполнителей. При определении документирования процессов необходимо определить, какие виды контроля должны быть осуществлены для демонстрации каждого запланированного процесса.

Основой этой деятельности является проектирование процессов документирования, подробно описанное в «Приложении А» ISO 30301.

Документы процессов управления предназначены для интеграции бизнес-процессов организации. Это требует понимания основных бизнес-процессов организации и требований к документам в качестве доказательства, а также необходимости поддержания этих процессы. Проектирование документов процессов управления включает в себя обзор существующих документов процессов или создание новых документов процессов, основанных на анализе этих процессов и приоритетах работы организации для предотвращения рисков и возможностей для улучшения. Это может включать разработку новых документов процессов и систем.

Отдельный подраздел посвящен внедрению документных систем.

Девятый раздел дает рекомендации по оценке эффективности системы на основе мониторинга, анализа, измерений и оценки, описывает систему внутреннего аудита для оценки СУД и необходимый анализ системы со стороны руководства. И, наконец, в десятом разделе «Улучшение» рассматриваются необходимость проведения корректирующих и предупреждающих действий в целях постоянного улучшения СУД.

Таким образом, рассмотренная структура ISO 30302 в полной мере раскрывает содержание работ по внедрению отдельных элементов системы управления документами, соответствующим требованиям на любую систему управления и основывающуюся на тщательном и последовательном документировании всех выполняемых действий. На самом деле в этом заключается и особенность, и

сложность понимания данной системы менеджмента (СУД), поскольку документы здесь рассматриваются и как предмет управления и как средство управления, тогда как в других системах управления они выступают только в качестве средства управления, предметом же являются отдельные характеристики продукции или услуг. Но в подобной сложности заключается и большой потенциал СУД по интегрированию других систем управления, которые могут быть внедрены в организации.

В ходе голосования по проекту данного стандарта многими странами были высказаны замечания и предложения, большая часть которых касалась основных содержательных разделов 6-8. В результате большинством голосов было принято решение оставить проект на этапе 20.00 в качестве нового проекта в рамках программы работы Комитета и продолжить консультации. Рабочим группам 8 и 9 было предложено к 15 октября 2013 года доработать проект и предложить его на голосование на стадии 30.00 Регистрация проекта комитета (CD).

Дальнейшую работу над проектами стандартов ISO 30303 и ISO 30304 было решено приостановить. Относительно ISO 30304 эксперты посчитали, что оно будет дублировать ISO 30302 и работа над ним приостановлена до завершения ИСО 30302. После чего ISO 30302 будет направлен контрольно-ревизионным органам, которые используя инструменты ISO 19 011 определят, можно ли его использовать в качестве аудиторского инструмента. Если ISO 30304 окажется не нужен, проект не будет продолжаться.

Что касается ISO 30303, то его разработка входит в противоречие с ISO/ КАСКО 17021 – «Требования к органам, проводящим аудит и сертификация систем управления». Это стандарт для проведения аудита в отношении любой системы менеджмента, в том числе ISO 30301. В рамках развития проекта КАСКО в ISO 17021 специальные требования к оценке и аудиту конкретных систем менеджмента будут пронумерованы: 17021-2 для ISO 14000, 17021-3 для ISO 9000, и т.д ... Таким образом могут быть разработаны требования и к аудиту ISO 30301. Этот вопрос еще будет обсуждаться.

На совместном заседании рабочих групп 8 и 9 был представлен краткий отчет об участии ТК46/ПК11 в работе ИСО/ТМВ JTCG (Joint technical Coordination Group) по стандартам на системы менеджмента. В отчете сообщалось, что при разработке новых или пересмотре стандартов на системы управления решено использовать не

только формальную обязательную общую структуру основного текста, но и согласовать определения, которые будут использоваться. По инициативе ТК46/ПК11 для документации в стандартах на системы менеджмента и для управления документацией в системах менеджмента установлен термин «records». Вся документированная информация в рамках процессов систем менеджмента должна управляться как документ («records») в соответствии с процессами определенными системой управления документами, за исключением некоторых аспектов управления версиями.

Таким образом, в развитии проекта по разработке стандартов на систему управления документами были достигнуты определенные успехи: более реальные очертания получил стандарт ISO 30302, определились перспективы с разработкой стандартов ISO 30303 и ISO 30304 и были закреплены важные решения относительно понимания документных процессов во всех стандартах на системы управления.

1.2. Пересмотр ISO 15489 «Информация и документация. Управление документами. Часть 1. Общие положения»

Созданная в конце 2012 года рабочая группа 13 по пересмотру стандарта ISO 15489 приступила к своей работе в январе 2013 года и только в ноябре представила новую версию указанного стандарта, причем первую его часть.

В представленном проекте стандарт претерпел значительные изменения. Его область применения представлена более компактно, как идентификация основных процессов управления документами. Четко сказано, что он адресован специалистам в области управления документами. Полностью обновлены нормативные ссылки стандарта. Теперь они связаны только со стандартами сферы информации и документации, тогда как ранее имели более широкий спектр взаимодействия со стандартами на другие системы управления. Раздел «Термины и определения» не содержит ни одной дефиниции и носит отсылочный характер на стандарт ISO 30300. Все это свидетельствует о новой концепции представления данного стандарта.

Первой частью ядра этой концепции является четвертый раздел стандарта «Документы, документы метаданных и документы системы», в котором подробно представлены особенности различных видов документов в сфере управления документами, а также их основные характеристики.

Пятый раздел посвящен анализу делового контекста при формировании требований к управлению документами, на основе которого определяются требования к обеспечению доступа к документам. Здесь же рассматриваются вопросы правового регулирования, анализа деловых процессов и оценки соответствия.

В шестом разделе речь идет о построении системы управления документами на основе схемы метаданных, определения прав доступа к документам, распределения ответственности и анализа финансово-хозяйственной деятельности организации.

Седьмой раздел описывает собственно процессы создания и управления документами и носит более традиционный характер, определяя основные процедуры организации работы с документами: их создание, включение в систему, классификацию документов, индексирование, реализацию решений по обеспечению доступа к документам, поддержание системы в рабочем состоянии, конвертацию и миграцию документов в системе и хранение документов.

Последний восьмой раздел «Создание организационной инфраструктуры» посвящен главным образом проектированию и внедрению системы управления документами, но также раскрывает вопросы политики и распределения ответственности, ее постоянного мониторинга и улучшения и, обучения персонала.

Таким образом, даже беглый взгляд на содержание проекта данного стандарта говорит о действительно инновационном предложении. Обращают на себя внимание как минимум два фактора: во-первых, стандарт ориентирован на управление главным образом электронными документами, и, во-вторых, он полностью воспроизводит механизмы и инструменты стандартов ISO серии 30300.

Как воспримет эти инновации профессиональное сообщество, которому адресован стандарт будет видно в следующем году.

Несколько слов следует сказать относительно разрабатываемого ТК 46/ПК11 технического отчета, ISO/DTR 18128 «Информация и документация. Идентификация рисков и их оценка для документных систем» *(Information and documentation – Risk assessment for records processes and systems).* Общие вопросы менеджмента рисков были рассмотрены в международном стандарте ISO 31000:2009 «Менеджмент рисков. Принципы и руководящие указания». Большая часть комментариев и правок ISO/DTR 18128 в 2013 году касалась гармонизации терминологии проекта с ранее принятыми стандартами: ISO 30300, ISO 15489 – в терминологическом аспекте и ISO 31000 - в вопросах общего подхода к управлению рисками. Основная работа над проектом

была продела в 2012 году[*], а в 2013 году Приложения A и C были приведены в соответствие с требованиями ISO 27000 по обеспечению информационной безопасности. Таким образом, работа над текстом ISO/DTR 18128 была завершена на данном этапе.

[*] Отчет НИР «Обзор международных стандартов и проектов международных стандартов ИСО по управлению документами за 2012 год, определении целесообразности разработки на их основе соответствующих национальных стандартов Российской Федерации». ВНИИДАД, 2013. С. 23-24.

2. ОБЗОР ПРОЕКТОВ МЕЖДУНАРОДНЫХ СТАНДАРТОВ И ТЕХНИЧЕСКИХ ОТЧЕТОВ ИСО, РАЗРАБАТЫВАЕМЫХ В 2013 ГОДУ ТЕХНИЧЕСКИМИ КОМИТЕТАМИ, ВЗАИМОДЕЙСТВУЮЩИМИ С ТК46

Комитет по оценке соответствия (КАСКО) представил ISO / IEC TS 17023 «Оценка соответствия. Руководящие указания по определению срока действия аудита сертификации системы менеджмента» *(Conformity assessment - Guidelines for determining the duration of management system certification audits)*. Определение времени аудита является одним из наиболее важных мероприятий, проводимых органом по сертификации. Опыт показывает, что время аудита зависит от нескольких факторов, и различные методологии и процедуры могут быть использованы для его вычисления. Чтобы найти взаимопонимание того, как подойти к этому процессу, ISO / КАСКО создал в 2012 году рабочую группу, в состав которой вошли представители национальных органов по стандартизации. Эти технические требования основаны на применении требований стандарта ISO/IEC 17021 содержит рекомендации органам, проводящим аудит и сертификации. В стандарте раскрываются факторы, определяющие продолжительность проверок, к числу которых относятся размер организации, сложность ее системы управления, технологический и нормативный контекст, риски, связанные с продукцией, процессами или деятельностью организации, особенности корпоративной культуры, наличие интегрированных систем управления и др. При разработке методологии расчета продолжительности аудита необходимо выделить ключевые факторы и, ориентируясь на них, а также на требования соответствующей системы управления, произвести аргументированный (документально подтвержденный) расчет продолжительности, который в процессе проведения аудита может быть скорректирован. Технические требования были приняты и введены в действие с 28 июля 2013 года.

В 2013 году в ИСО рассматривалось три проекта стандартов ТК 171«Прикладные системы создания и хранения документов»:

1. ISO/DIS 32000-2 Document management - Portable document format - Part 2: PDF 2.0 *(Управление документацией. Формат переносимого документа. Часть 2. PDF 2.0)*

2. ISO/DIS 24517-2 Document management - Engineering document format using PDF - Part 2: Use of 32000-2 including support for long-term preservation (PDF/E-2) *(Управление документацией. Формат технического документа в системе PDF.*

Часть 2. Использование 32000-2, включая поддержку для долгосрочной сохранности (PDF/E-2)

3. ISO/WD 18829 «Document management – Assessing trusted systems for compliance with industry standards and best practices*» (Оценка надежности систем на соответствие стандартам и лучшей практике)*.

Первые два проекта подготовлены ТК 171 / ПК 2 «Прикладные программы для управления документооборотом» Document Management Applications), рабочими группами 7 и 8 соответственно, которые занимаются разработкой спецификации формата PDF файлов.

PDF самый популярный формат файлов электронных документов во всех отраслях независимо от размеров организации. PDF-файлы могут быть созданы изначально в виде PDF, преобразованы из других электронных форматов и является подходящим форматом для документов, оцифрованных с бумажных носителей, микроформ. Предприятия, правительства, библиотеки, архивы и другие учреждения и люди во всем мире используют PDF чтобы представлять важную информации. С момента своего введения в 1993 году, опираясь на взрывной рост Интернета, PDF стал широко используемым для электронного обмена документами. Поскольку крупные корпорации, правительственные учреждения, образовательные учреждения оптимизируют свою деятельность путем замены использования в рабочих процессах бумажных документов на электронный обмен информацией, влияние и возможности для применения PDF будет продолжать расти быстрыми темпами.

ISO/DIS 32000-2 предназначен дня разработчиков программного обеспечения, которое создает PDF файлы, считывает и отображает их содержимое. Этот стандарт объемом 919 страниц состоит из четырнадцати разделов, в которых представлены особенности представления в формате PDF 2.0 различных типов документированной информации – от текстовых до интерактивных документов. Он заменяет 32000-1, поскольку содержит дополнительные функции для PDF файлов и включает некоторые поправки к существующему стандарту. ISO/DIS 32000-2 устанавливает цифровую (digital) форму для представления электронных (electronic) документов для предоставления пользователям возможности просмотра, обмена электронными документами независимо от той среды в которой они были созданы и среды в которой они рассматриваются или распечатываются.

PDF, вместе с программным обеспечением для создания, просмотра, печати и обработки PDF файлов в различных формах, выполняет набор требований к электронным документам в том числе:

• сохранение точности документа,

• слияние содержания (контента) из различных источников (веб-сайты, программы обработки текстов и электронных таблиц, отсканированные документы, фотографии и графики) в один автономный документ при сохранении целостности всех оригинальных исходных документов,

• цифровые подписи для подтверждения подлинности,

• безопасность и контроль права доступа,

• доступность содержания для лиц с ограниченными возможностями,

• поиск и повторное использование контента для использования с других файловых форматов и приложений, и

• создание электронных форм для сбора данных и интегрирования их с бизнес-системами.

Эта часть ISO/DIS 32000 не определяет конкретные способы превращения бумажных или электронных документов в формат PDF; конкретные технические параметры, пользовательский интерфейс; конкретные физические методы хранения этих документов и условия хранения; требуемую компьютерную технику и / или операционную систему.

В стандарте очень тщательно и четко указано, что представляет собой документированная информация в формате PDF, почему та или иная функция включена в файл и для каких целей она предназначена.

В отличие от ISO 32000-1, эта спецификация включает новые возможности, наиболее интересные из которых отраженные в нескольких разделах. Для нас особенно интересным может оказаться раздел

12.8. Цифровая подпись (Digital signatures)

Цифровая подпись может быть использована для аутентификации личности пользователя с содержимым документа. Она хранит информацию о подписавшем и о состоянии документа в тот момент, когда он был подписан.

Подпись может быть чисто математической, такой как открытый / закрытый ключ, с помощью которого шифруется документ, или это может быть биометрические документ, удостоверяющий личность, например, собственноручная

подпись, отпечатки пальцев, или сканирование сетчатки глаза. Специфическая форма проверки подлинности осуществляется с помощью специального модуля программного обеспечения под названием «обработчик подписи». Требования к такому модулю приведены в приложении Е стандарта.

При работе с цифровыми подписями в PDF сейчас может осуществляться четыре вида действий:

– добавление цифровой подписи к документу;

– проверка действительности подписи, которая была уже применена к документу;

– добавление информации, связанной с проверкой (12.8.4.3);

– добавление метки времени (12.8.5)

Последняя операция появилась только в последней версии PDF 2.0.

Речь идет об использовании, проверке, в том числе долгосрочной (12.8.4. данный раздел введен впервые в этой версии стандарт, под долгосрочной проверкой рассматривается период, например, в 5 лет), подтверждении и обеспечении безопасности при использовании криптографической расширенной электронной подписи (Cryptographic Advanced Electronic Signatures – CAdES). Приводятся все атрибуты данного типа цифровой подписи, которые поддерживаются форматом PDF 2.0

Этот стандарт отражает все функциональные возможности PDF. В то же время есть несколько конкретных приложений, которые развивались с использованием только некоторых функций PDF для более специализированных применений и реализованы в нескольких отраслевых стандартах. В их число входит ISO 19005 «Управление документацией. Формат файлов электронных документов для долговременного сохранения». *(Document management - Electronic document file format for long-term preservation)* в настоящее время является отраслевым стандартом для архивирования электронных документов.

Второй из предлагаемых к обсуждению проектов стандарта ISO/DIS 24517-2:2013 «Document management - Engineering document format using PDF - Part 2: Use of 32000-2 including support for long-term preservation (PDF/E-2)» *(Управление документацией. Формат технического документа в системе PDF. Часть 2. Использование 32000-2, включая поддержку для долгосрочной сохранности (PDF/E-2)* уже в своем названии отразил основную инновацию стандарта ISO 32000-2,

связанную с поддержкой долгосрочной сохранности документов. Целью его является улучшить обмен документированной информацией в процессе сотрудничества и обеспечить точность печати для инженерных процессов. Этот стандарт определяет формат файла для обмена технической конструкторской документацией на основе PDF и устанавливает правильное его использование для отображения на экране и печати конструкторской документации.

ISO/DIS 24517-2:2013 расширяет возможности части 1, так как основан на PDF 2.0 (как определено ISO/DIS 32000-2), а не на PDF 1.7, как первая часть. Это обеспечивает дополнительные возможности, которые реализуются через соответствие требованиям ISO/DIS 32000-2 и включают в себя:

– поддержку многочисленных усовершенствований в 3D, включая поддержку PRC;

– поддержку геопространственной информации (GIS) в 3D и 2D;

– сжатие объекта и потоки внешней ссылки;

– прозрачность (транспарентность);

– JPEG сжатие 2000;

Сфера распространения этого стандарта ограничена также как и для ISO/DIS 32000-2, а особые требования на соответствие PDF 2.0 содержатся в Приложении А стандарта. Стандарт состоит из шести разделов, в последнем из которых отражены технические требования для представления в формате PDF технической и конструкторской документации различных типов. Также как и в ISO/DIS 32000-2 особое внимание уделено цифровой подписи, требования к представлению которой в соответствие с ISO/DIS 32000-2 приведены в «Приложении С» проекта данного стандарта.

Кроме того, ТК 171 представил ISO/ 18829 «Оценка надежности систем на соответствие стандартам и лучшей практике» (*Document management – Assessing trusted systems for compliance with industry standards and best practices*) на стадии 30.00

Поскольку организации должны обеспечить безопасное и надежное хранение и доступ к информации, а также иметь механизм для определения, действительно ли система соответствует юридическим, техническим и этическим обязательствам организации, необходимо, чтобы любое решение для хранения данных было проверяемыми с воспроизводимыми результатами этой проверки. Поэтому должен быть какой-то способ самостоятельной проверки уровня программного и аппаратного

обеспечения для того, чтобы убедиться, что информация будет храниться соответствующим способом. Независимо от того, технология хранения стандартизирована или является собственной разработкой, организация сталкивается с одинаковой проблемой: как определить функционирует ли система в соответствии с проектом, как ожидалось. Целью данного отраслевого стандарта является определение мероприятий и операций, которым организация должна следовать, чтобы убедиться, что хранимая в электронном виде информация (ESI) создается, включается в систему и поддерживается надежным и добросовестным образом, путем оценки существующей системы ECM. При этом стандарт не претендует на полновесный стандарт по оценке ECM системы. Речь идет об определении уровня доверия.

ЗАКЛЮЧЕНИЕ

Анализ проектов международных стандартов и технических отчетов (TR) и требований (TS) ИСО ТК 46/ПК11 и взаимодействующих с ним комитетов, над которыми велась работа в 2013 году, позволяет сделать следующие выводы:

1. Наблюдается значительное усиление интеграционных процессов в международной стандартизации, связанной со сферой управления на основе современных информационно-коммуникационных технологий, что приводит к осознанию необходимости большей координации при использовании терминологии и при принятии решений о целесообразности разработки стандартов.

2. В условиях взаимодействия активно продолжается работа по развитию стандартов серии 30300 «Системы управления документами», в частности над ISO-30302.

3. Предложенный проект 15489-1 в полном объеме соответствует концепции стандартов серии 30300 «Системы управления документами». Несмотря на это предполагается его использование совместно со стандартами серии 30300 для организаций, которые не будут сертифицированы на соответствие системе управления документами.

4. Особого внимания требует работа над терминологическими стандартами и терминологией в целом, поскольку усиливается координация этой деятельности в различных сферах системы управления.

5. Одними из наиболее актуальных остаются вопросы организации долговременного хранения электронных документов в информационных системах, над техническим решением которых работают комитеты, взаимодействующие с ТК46/ПК11.

Исходя из вышеизложенного, считаем необходимым:

- продолжать работу по мониторингу и анализу международных стандартов ИСО по управлению документами, разрабатываемых в профильном ВНИИДАД техническом подкомитете ИСО/ТК 46/ПК11 «Управление документам/архивами» и взаимодействующих с ним комитетах;

- принять участие в переработке основополагающего стандарта ИСО по управлению документами ИСО 15489-1 «Information and documentation – Records

management – Part 1: General» и технического отчета ISO/TR 15489-2 «Information and documentation – Records management – Part 2: Guidelines», привлекая к этой работе специалистов – переводчиков отдела ОЦНТИ.

Поскольку в 2013 году не были приняты международные стандарты, разработанные ИСО/ТК 46/ПК11, то, проведя анализ технических отчетов разработанных ИСО/ТК 46/ПК11, предлагаем подготовить официальный перевод технического отчета: ISO/TR 18128 «Информация и документация. Идентификация рисков и их оценка для документных систем» *(Information and documentation – Risk assessment for records processes and systems)*, учитывая актуальность вопросов управления рисками.

СПИСОК ИСТОЧНИКОВ

1. ISO 30300:2011 «Information and documentation. Management system for records. Fundamentals and vocabulary» (Международный стандарт ИСО 30300:2011 «Информация и документация. Системы управления документами. Основные положения и словарь»)

2. ISO 30301:2011 «Information and documentation. Management system for records. Requirements» (Международный стандарт ИСО 30301:2011 «Информация и документация. Системы управления документами. Требования»)

3. Проект международного стандарта ISO 30302 «Information and documentation – Management systems for records – Guidelines for implementation» («Информация и документация. Системы управления документами. Руководство по внедрению»)

4. Проект международного стандарта ISO 30303 « Information and documentation – Requirements for bodies providing audit and certification» («Информация и документация. Система управления документами. Требования к органам, проводящим сертификацию»)

5. Проект международного стандарта ISO 30304 «Information and documentation – Management systems for records – Guidance for auditing and performance measurement» («Информация и документация. Системы управления документами. Руководство для аудита и измерения работ»)

6. Проект международного стандарта ISO 15489-1 «Information and documentation – Records management – Part 1: General» («Информация и документация. Управление документами. Часть 1: Общие требования»)

7. Проект технического отчета ISO/TR 18800:2012 «Information and documentation — Implementation guidelines for disposition of records» («Информация и документация. Рекомендации по внедрению отбора и передачи документов (на последующее хранение или уничтожение)»).

8. Проект технического отчета ISO/D TR 18128 «Information and documentation – Risk identification and assessment for records systems («Информация и документация. Идентификация рисков и их оценка для документных систем»).

9. Проект международного стандарта ISO/DIS 32000-2 «Document management - Portable document format - Part 2: PDF 2.0» *(*Управление документацией. Формат переносимого документа. Часть 2. PDF 2.0);

10. Проект международного стандарта ISO/DIS 24517-2 Document management - Engineering document format using PDF - Part 2: Use of 32000-2 including support for long-term preservation (PDF/E-2) (Управление документацией. Формат технического документа в системе PDF. Часть 2. Использование 32000-2, включая поддержку для долгосрочной сохранности (PDF/E-2)) ;

11 Проект международного стандарта ISO/WD 18829 «Document management – Assessing trusted systems for compliance with industry standards and best practices» (Оценка надежности систем на соответствие стандартам и лучшей практике);

12. Проект технических требований ISO / IEC TS 17023 «Conformity assessment - Guidelines for determining the duration of management system certification audits» (Оценка соответствия. Руководящие указания *по определению срока действия аудита сертификации системы менеджмента).*

14. Отчет по НИР «Участие в разработке международных стандартов ИСО по управлению документами серии 30300 «Информация и документация. Системы управления документами («Information and documentation. Records management systems»)». – М., ВНИИДАД, 2010.

15. «Обзор международных стандартов и проектов международных стандартов ИСО по управлению документацией за 2011 год, определение целесообразности разработки на их основе соответствующих национальных стандартов Российской Федерации. Аналитический обзор». – М., ВНИИДАД, 2012.

ПРИЛОЖЕНИЕ А

Международные согласованные коды стадий разработки

СТАДИЯ	ПОДСТАДИЯ						
				90 Решение			
	00 Регистрация	**20** Начало основных действий	**60** Окончание основных действий	**92** Повторить более раннюю фазу	**93** Повторить текущую фазу	**98** Аннулировать	**99** Продолжить
00 Предварительная стадия	**00.00** Предложение новой рабочей темы	**00.20** Рассмотрение предложения новой рабочей темы	**00.60** Рассылка результатов рассмотрения			**00.98** Исключение предложения новой рабочей темы	**00.99** Голосование по предложению новой рабочей темы
10 Стадия, связанная с внесением предложения	**10.00** Регистрация предложения новой рабочей темы	**10.20** Начало голосования по новой рабочей теме	**10.60** Рассылка отчета по голосованию	**10.92** Возврат предложения автору для дальнейшего рассмотрения		**10.98** Новая рабочая тема отклонена	**10.99** Новая рабочая тема утверждена
20 Подготовительная стадия	**20.00** Регистрация новой рабочей темы в программе работ ТК/ПК	**20.20** Начало изучения рабочего проекта **(WD)**	**20.60** Рассылка комментариев			**20.98** Проект исключен	**20.99** Рабочий проект принят для регистрации в качестве проекта комитета
30 Стадия, связанная с подготовкой проекта комитета	**30.00** Регистрация проекта комитета **(CD)**	**30.20** Начало изучения и голосования по проекту комитета	**30.60** Рассылка комментариев и отчета по голосованию	**30.92** Проект комитета возвращен в рабочую группу		**30.98** Проект исключен	**30.99** Проект комитета принят для регистрации в качестве проекта

							международного стандарта
40 Стадия, связанная с рассмотрением проекта международного стандарта	**40.00** Регистрация проекта международного стандарта **(DIS)**	**40.20** Начало голосования по проекту международного стандарта: 5 мес.	**40.60** Рассылка краткого отчета по итогам голосования	**40.92** Рассылка полного отчета: проект международного стандарта возвращен в ТК/ПК	**40.93** Рассылка полного отчета: решение относительно нового голосования по проекту международного стандарта	**40.98** Проект исключен	**40.99** Рассылка полного отчета: проект международного стандарта принят для регистрации в качестве окончательного проекта международного стандарта
50 Стадия, на которой осуществляется принятие стандарта	**50.00** Регистрация окончательного проекта международного стандарта **(FDIS)** для официального принятия	**50.20** Начало голосования по окончательному проекту международного стандарта: 2 мес. Уведомление направлено в секретариат	**50.60** Рассылка краткого отчета по итогам голосования Уведомление от секретариата	**50.92** Окончательный проект международного стандарта возвращен в ТК/ПК		**50.98** Проект исключен	**50.99** Окончательный проект международного стандарта принят для опубликования
60 Стадия, на которой осуществляется публикация	**60.00** Подготовка международного стандарта к публикации		**60.60** Опубликование международного стандарта				
90		**90.20**	**90.60**	**90.92**	**90.93**		**90.99**

Стадия пересмотра		Систематический пересмотр между-народного стандарта	Рассылка краткого отчета о пересмотре	Между-народный стандарт подлежит пересмотру	Подтверждение действия между-народного стандарта		Отмена международного стандарта по инициативе ТК/ПК
95 Стадия, на которой осуществляется отмена стандарта		**95.20** Начало голосования по отмене международного стандарта	**95.60** Рассылка краткого отчета по итогам голосования	**95.92** Решение об отмене международного стандарта			**95.99** Отмена международного стандарта

ПРИЛОЖЕНИЕ Б

Проект технического отчета ISO/D TR 18128 «Information and documentation – Risk identification and assessment for records systems («Информация и документация. Идентификация рисков и их оценка для документных систем»)

Document type: Technical Report Document subtype: Document stage: (30) Committee Document language: E \\syd-fs1\home$\simai\My Documents\USER Agnes1\Anne\2012-03-05\ISO_DTR_2nd 18128_(E) for ballot.xml STD Version 2.1c

ISO TC 46/SC 11 N N1337

Date: 2013-02-27

ISO/DTR 2nd 18128

ISO TC 46/SC 11/WG 11
Secretariat: SA

Information and documentation — Risk assessment for records processes and systems

Information at documentation — Evaluation du risque pour les processus et systèmes d'enregistrement

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation. **ISO/PDTR 18128**

Contents Page

1 Scope 1
2 Normative references 1
3 Terms and definitions 2
4 Risk assessment criteria for the organization 2
5 Risk identification 4
5.1 General 4
5.2 Analyzing Context 5
5.3 Context: External factors 5
5.4 Context: Internal factors 7
5.5 Records Systems 8
5.6 Records processes 11
6 Analysing identified risks 13
6.1 General 13
6.2 Likelihood analysis and probability estimation 13
7 Evaluating risks 15
7.1 General 15
7.2 Assessing impact of adverse events 16
7.3 Assessing the risk 17
8 Responding to the identified risks 19
8.1 Communicating the risks..... 19
Annex A (informative) Example of a risk register entry 20
Annex B (informative) Example checklists for areas of uncertainty 21
B.1 External factors 21
B.2 Internal factors 22
B.3 Systems 22
B.4 Processes 24

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.
In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.
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/TR 18128 was prepared by Technical Committee ISO/TC 46, *Information and documentation*, Subcommittee SC 11, *Archives/records management*.
This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised. **ISO/PDTR 18128**

Introduction

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

ISO 31000 *Risk management -- Principles and guidelines* provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context. These principles and guidelines 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 technical report is intended to help records professionals to assess the risks related to records processes and records systems. This is distinct from the task of identifying and assessing the organization’s business risks to which creating and keeping adequate records is one strategic response. The decisions to create or not create records in response to general business risk are business decisions which should be informed by the analysis of the organization’s records requirements undertaken by records professionals together with business managers. The premise of this Technical Report is that the organization has created records of its business activities to meet operational and other purposes and has established at least minimal mechanisms for the systematic management and control of the records.

The over-arching consequence of not managing uncertainties/risk affecting records processes and record systems is records which can no longer meet the needs of the organization.

The Technical Report provides guidance and examples to apply the general risk management process established in ISO 31000 (Figure 1) for risks related to records processes and the records systems in which records are managed (or reside). It is specifically focused on risk assessment, which includes:

- risk identification,
- risk analysis,
- risk evaluation.

The results of the analysis of risk to records processes and records systems should be incorporated into the organization’s general risk management framework As a result the organization will be in better control of its records and their quality and use for business purposes

Clause 5 is about risk identification. Following ISO 31000 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. This Technical Report provides a comprehensive list of areas of uncertainty related to records and records systems that can be used as a guide for risks identification.

Clause 6 is about risk analysis, which consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. This Technical Report provides a guide for records professionals on how to analyse identified risks, assessing potential events or changes, their consequences and the likelihood of occurrence and documenting them as measurable and manageable risks.

Clause 7 is about risk evaluation, which involves determining the significance of the level and type of risk. This Technical report provides a means for records professionals to establish levels of risks depending on the context of each organization. **ISO/PDTR 18128**

The approach taken, while it is applicable to a variety of organizations, large or small, government or non-government, should be adapted to the size, nature of the business and complexity of the organization which uses it. There are other methods of risk assessment: see for example ISO 31010:2009.

This Technical report is not about risk treatment. Once the assessment of risks related to records processes and record systems has been completed, the assessed risks are documented and communicated to the organization's risk management section. Response to the assessed risks is undertaken as part of the organization's overall risk management program. The priority assigned by the records professional to the assessed risks is provided to inform the organization's decisions about managing those risks

This Technical Report may be used by all organizations regardless of size, nature of their activities or complexity of their functions and structure. These factors, and the regulatory regime in which the organization operates which prescribes the creation and control of its records, should be taken into account when assessing risk related to the records processes and the records systems.

The Technical Report may be used by records professionals and by auditors and managers who have responsibility for risk management programs in their organizations.

Figure 1 — Risk Management process

NOTE Figure 1 adapted from ISO 31000:2009

Information and documentation — Risk assessment for records processes and systems

1 Scope

This Technical Report intends to assist organizations in assessing risks with respect to records processes and systems, so they can ensure records are of value to the organization and the identified business needs as long as required.

As such it:

☐Establishes a method of analysis for identifying risks related to records processes and records systems;

☐Provides a method of analysing the potential effects of adverse events on records processes and record systems;

☐Provides guidelines for conducting an assessment of risks related to records processes and record systems;

☐Provides guidelines for documenting identified and assessed risks in preparation for mitigation.

This Technical Report does not address the general risks to an organization's operations which can be mitigated by creating records.

This Technical Report may be used by all organizations regardless of size, nature of their activities or complexity of their functions and structure. These factors, and the regulatory regime in which the organization operates which prescribes the creation and control of its records, should be taken into account when identifying and assessing risk related to the records and the records systems.

NOTE Defining an organization or identifying its boundaries should take into account the complex structures and partnerships and contractual arrangements for outsourcing services and supply chains which are a common feature of contemporary government and corporate entities. Identifying the boundaries of the organization is the initial step in defining the scope of the project of risk assessment related to records.

This Technical Report does not address directly mitigation of risks as methods for these will vary from organization to organization.

The Technical Report may be used by records professionals, and by auditors or managers who have responsibility for risk management programs in their organizations.

2 Normative references

ISO 15489-1:2001, *Information and documentation — Records management — Part 1: General*

ISO/TR 15489-2:2001, *Information and documentation — Records management — Part 2: Guidelines*

ISO 30300:2011, *Information and documentation — Management systems for records — Fundamentals and vocabulary*

ISO 30301:2011, *Information and documentation — Management systems for records — Requirements*
ISO 31000:2009, *Risk management -- Principles and guidelines*
ISO 31010:2009, *Risk management -- Risk assessment techniques*
ISO Guide 73:2009*, Risk management – Vocabulary*

3 Terms and definitions

For the purpose of this document, the terms and definitions given in ISO 30300 apply.

3.1 Terms specific to risk

3.1.1
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 and consequences 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 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]

3.2 Terms specific to records

3.2.1
Records system
An information system which captures manages and provides access to records through time.
NOTE This can include business applications or systems which create and maintain records.
[ISO 30300, Clause 3.4.4]
3.2.2
Records processes
Set of activities by which records are created, controlled, used and kept and ultimately disposed of, by the organization.

4 Risk assessment criteria for the organization

Assessing risks for records processes and systems should be included, where it exists, in the organization's general risk management process. In this case, records professionals should take into account the organization's established external and internal context and the context of the risk management process itself, including:

☐Roles and responsibilities: the role of records professionals in the assessment of risk related to records processes and systems should be specified;

☐Extent and scope of the risk assessment activities: relationships with other risk assessment areas, such as information security, should be made explicit to avoid redundancy and conflicts;
☐Methodology: the standard risk assessment methodology should be applied using the available risk assessment tools and reporting to the designated area or person;
☐Risk criteria: where general risk criteria for the organization are established, risks related to records processes and systems should be assessed using these criteria;

Where the organization has not established a general risk management process, records professionals need to establish the risk criteria prior to the assessment process.
Criteria should be based in the legal requirements for each jurisdiction and should include:
☐the nature and types of consequences to be included and how they will be measured;
☐the way in which probabilities are to be expressed;
☐how a level of risk will be determined;
☐the criteria by which it will be decided when a risk needs treatment;
☐the criteria for deciding when a risk is acceptable and/or tolerable;
☐whether and how combinations of risks will be taken into account;

Regarding the nature and types of consequences to be included in the risk assessment of records processes and systems, there is a general starting point which should be applied to all organizations. Records which are authentic, reliable, have integrity and are useable for as long as they are required will support the needs of the organization. Risks are identified based on their potential to undermine those general characteristics of records which would make them fail to meet the purposes for which they are created.
For discussion of probability and frequency of events in risk assessment, see below 6.2.
Criteria for evaluating risks, including the criteria by which it will be decided when a risk is acceptable or needs treatment, include the size and reach of the records systems in the organization, the number of users and the use made of the system in the operations of the organization.
Similarly criteria for evaluating risks affecting records processes should include the frequency of the process, how many systems it is used in, its relative importance in creating or managing records, the tracking of processes and the potential for reversing or remedying adverse effects.
The priority assigned to individual records, their aggregations, records processes, or specific records systems may also be assessed in relation to responses to major disasters affecting all or many business operations. For example, certain records are needed in the immediate aftermath of a natural disaster, such as security contacts and access records, contact details of disaster plan response teams and insurance contacts and policy details. Second, the organization’s business continuity planning should identify the functions which need to be restored first and the records needed to do so.
More generally, the organization must determine which records are the core records of its operations and the level of significance attached to them. These are business decisions, based on the advice of both records professionals and the business managers.
NOTE Special attention should be paid to where a combination of risks applies to records identified as core operational or otherwise significant.

5 Risk identification

5.1 General

Identification of risks is structured under the following categories: context, systems, and processes involved in creating and controlling the records of the organization.

The external context of the organization refers to the political and societal, the economic and technological, and the physical environmental factors beyond its control, which impact on its operations and are taken into account when determining its records requirements. The external context includes the external stakeholders, who or which have a particular interest in the organization's operations.

The organization also has an internal context by which is meant the internal factors not controlled by the records professional(s) responsible for the records, records processes and records systems. The internal context includes factors such as the structure and finances of the organization, the technology it deploys, the resourcing of activities (people and budgets) and the workplace culture, all of which influence the policies and practices for managing records.

Potential events with uncertain effects may be external or internal to the organization.

Uncertain effects caused by change in the external context may differ according to the perspective of the different levels of the organization (see Figure 2). It is also recognized that all change presents opportunities which may be positive in effect.

Figure 2 — The multiple layers of context of an organisation's records and records processes

The purpose of risk identification is to identify what may happen or what situations may exist that could affect the capacity of records to support the needs of the organization.

The risk identification process includes identifying the causes and source of the risk, events, situations or circumstances which could have a material impact upon the organization's objectives, and the nature of that

impact. Numerous methods for risk identification exist in ISO 31010, Annex B, for a comparison of major methods.
Identified risks should be documented in a risk register, both in one specific to records, and in the organization's risk register, see the example given at Annex A.

5.2 Analyzing Context

When analyzing the context of the organization to identify risks related to the records (and records processes and systems), the following aspects should be taken into account as shown in Figure 2:
a) the political and societal, the economic and technological, and the physical environment,

b) the key drivers and trends in the operating context of the organization which may affect the objectives,

EXAMPLE competition, adoption of new technology, amalgamation or downsizing
c) the organization's relationships with external stakeholders.

While changes in the external context are outside of the control of the organization, their potential impact on the records should be anticipated and assessed in Sub-clause 6.1.2. This type of change may have first of all an impact on the records requirements of the organization, and subsequently on the policies and practices for managing records.

5.3 Context: External factors

Records processes and systems must be compliant with legal and regulatory requirements which arise from the political and societal context of the organisation. Other factors which must be analysed are the macro economic circumstances which may influence the technological choices of the organization, the security environment and the actual physical environment. Where the first two may have consequences for policies and practices for managing records, the other two can have a more immediate impact on the records system(s).

5.3.1 Areas of uncertainty: Changes in political-societal context

Changes in the political and societal climate can affect public attitudes to governments' and corporate behaviour. This may bring about regulatory change, which impacts the organization's operations and consequently its records requirements.
Examples of areas of changing public attitudes are national security, access to government and corporate information, privacy, intellectual property rights and corporate reporting responsibilities. More generally, examples of areas of uncertainty include:
☐Legal and regulatory changes affecting the organization's records requirements;
☐Changes in government policies affecting the organization's records, records processes and records systems;
☐New standards or codes of practice that affect the organization's records, records processes, and records systems;
☐Changing demand for records services;
☐Changing stakeholders' expectations;
☐Changes to reputation of, or trust in, the organization's ability to deliver its services.

5.3.2 Areas of uncertainty: Macro-economic technological environment

Global financial markets can undergo periods of turmoil that can have widespread impacts on the economic and business environment in many countries. Changes in industrial and information technology have continued with high impact on communication and information and records management, driven by competition and customer or user demand. The latter changes are examples of areas of uncertainty which offer positive opportunities.

Examples of areas of uncertainty arising from such changes to the economic and business environment include:

- ☐Changes in revenue or other funding of the organization;
- ☐Changes in ownership of the organization affecting management priorities including managing records;
- ☐Changes in the aims and operations of the organisation;
- ☐Introduction of new or upgrading of technologies;
- ☐Adoption of new technology across society;

EXAMPLE use of social media in business

- ☐Changes in the market or client base of the organization.

5.3.3 Areas of uncertainty: Physical environment and infrastructure

The possibility of large-scale, natural or man-made, disasters on the general operations of the organization is a major area of uncertainty requiring identification and assessment. The impact of such disasters include both potential damage with direct impact and the less direct impact of loss of services upon which the organisation depends, for example water and power supplies and other services. Areas of uncertainty include:

- ☐Regional or local destructive or disruptive environmental phenomena such as earthquake, hurricane/cyclone, tsunami, flood, fire, major storms or prolonged drought;
- ☐The potential for acts of war or terrorism to cause major structural damage or disruption to service supply to premises or vicinity of the organization;
- ☐Other disruption to organization's power, water, waste management, information technology, transport services or other core utilities and services.

5.3.4 Areas of uncertainty: External security threats

Risk identification must include hostile external security threats with the potential impacts ranging from damage to premises or service supply to unauthorised access to systems including records systems.

Examples of external security threats include:

- ☐Unauthorised external intrusion/access into records systems and unauthorised changes to records. Unidentified security compromise or exploitation of vulnerability that is not monitored and leads to information degradation;

EXAMPLE use of spy- and malware, unpatched software security loophole hack

- ☐Physical intrusion into records storage or IT hardware space;
- ☐Cyber-terrorism attack;

☐Physical vandalism;
☐Loss of third party services on which the records systems are dependent.

NOTE For greater detail and instructions see ISO 27005

5.4 Context: Internal factors

The organization's own economic, technological and structural character changes in response to the key drivers of its activities as well as the external environment and the demands of its stakeholders. These are taken into account when identifying areas of uncertainty and assessing risk to records and/or records systems.

5.4.1 Areas of uncertainty: organizational change

Management decisions affecting the organization such as amalgamations, mergers and acquisitions, restructuring, downsizing, outsourcing or the reverse, off-shoring of services constitute a significant area of uncertainty in the internal context of the organisation. The decisions have the potential to affect the records systems and processes, for example:

☐Change of ownership of records, and consequent transfer of records to and from the organization;
☐New internal policies or modified existing ones within the organization that affect the records systems and processes;
☐Loss of personnel or corporate memory affecting knowledge of current records and systems, including knowledge of procedures to retrieve and use them and of older records inherited through organizational change;
☐Change of terms within third party service contracts;
☐Policies and procedures which have not been reviewed and updated, and are inefficient, inconsistent or contradictory consequent to organizational change; and
☐Changes in organization's staffing policy that may affect the records staff;
☐Changes in training budget and opportunities that affect the capacity of records staff;
☐Untested disaster recovery plan leads to information being lost in the event of a disaster.

5.4.2 Areas of uncertainty: Technological change

Introduction of new technologies and systems are opportunities for improvement but as well, constitute areas of uncertainty with potential for adverse effects. The areas of uncertainty include:

☐Technological changes that affect interoperability between systems that create, keep or manage records;
☐Compatibility with previous platforms and systems;
☐Migration of records and metadata;
☐Transfer of access controls;
☐Effectiveness of implementation of change;
☐Extent to which the existing policies cover new technologies that the organization has adopted;

EXAMPLE using cloud services, social media, RFID, GPS
☐Capacity of existing technical infrastructure to meet new requirements resulting from organization's or records systems' technological development.

5.4.3 Areas of uncertainty: Resources: People and competencies

The organization is dependent on competent staff to deliver all its operations including the records systems and processes. This may not be within the control of the records professional responsible for records management overall so the areas of uncertainty can include:
☐Sufficiency of staff resources to create and control records, and to design and maintain records systems;
☐Staff awareness of records policies and processes;
☐Sufficiency of engagement of top management in supporting the records program;
☐Awareness of risks related to records systems and processes and ability to make decisions on appropriate mitigation among the top management;
☐Separation of administrative roles from operational users of records system ("front office" separate from "back office");
☐Sufficiency of staff competencies to create and control records;
☐Losing key staff with vital skills, in-depth organizational knowledge or undocumented corporate history;
☐Deterioration of skills level of staff;
☐Inadequate means to evaluate staff effectiveness or suitability.

5.4.4 Areas of uncertainty: Resources: Finances and materials

The funding and material resources available to the records professional to manage the record systems and processes adequately are affected by both the external, economic and business, environment and by the level of support for the records function in the organization. Areas of uncertainty include:
☐Adequacy of financial resources to meet commitments and goals of the records program;
☐Adequacy of financial resources to purchase, upgrade or maintain adequate systems.

5.5 Records Systems

When assessing the impact of risk on the systems deployed by the organization to manage its records, the issues of maintenance, sustainability and continuity, interoperability and security, should be taken into account. The records systems used by the organization change over time according to the economic circumstances, changes in its activities and personnel and changes in its size and structure.
NOTE all references to systems in this section should be understood as references to records systems 3.2.1.

5.5.1 Areas of uncertainty: System design

System design and configuration is critical to record creation and longevity. It intersects with the risk identification for records processes. **ISO/PDTR 18128**

Based on contemporary experience, identification of risks in system design, especially in the digital context includes:
☐Ability to define “records” in digital systems;
☐Explicit identification of retention requirements;
☐Effectiveness of design of the records systems appropriate to organization’s personnel and technology;
☐Management of dependence on vendor support;
☐Access to vendor documentation.

5.5.2 Areas of uncertainty: Maintenance
Maintenance of the records systems refers primarily to the technological platform and systems support aspects which are affected by structural change in the organization, implementation of new systems, technological change, competence and reliability of the technical support.
Areas of uncertainty include:
☐Changes in business and operating systems affecting records systems;
☐Skill level of system administrators and their understanding of requirements for managing records in systems;
☐Reliability of systems suppliers and their ability to keep maintaining the systems and keeping them technologically up to date;
☐Adequacy of documentation of procedures for operational maintenance;
☐Adequacy of technical documentation of the systems;
☐Adequacy of documented back-up procedures for the records systems;
☐Adequacy of restoration from backups.

5.5.3 Areas of uncertainty: Sustainability and Continuity
The sustainability of the records systems depends on the monitoring of change in the external and internal context of the organization by the records professional so the records systems are updated to respond to changes in needs.
Continuity planning for the records systems takes into account the organization’s planning for business continuity. In the absence of a business continuity plan for the organisation the records professional assesses the records systems to establish priority and procedures for restoration following a disruption to service.
Areas of uncertainty include:
☐Change in external and internal context affecting the organization’s records requirements;
☐Adequacy of quality assurance monitoring to identify changes in records requirements;
☐Adequacy of assessment of actual costs of implementation and maintenance of the records systems including human resources;
☐Adequacy of identification and documentation of records systems;

☐Maintenance and accessibility of system specifications and documentation;
☐Adequate documentation of decisions taken in the implementation of records systems available to all users who need them;
☐Ability of the records system to maintain the usability of records;
☐Duplication of functionality for managing records in the organization's various systems;
☐Capacity to import records from legacy or other business systems;
☐Migration of records to new records system due to either change in records requirements or in technology;
☐Adequacy of the records system's event history;
☐Ability of records systems to support business continuity by providing access to records in a disaster event;
☐Contingency planning for disruptions of service.

5.5.4 Areas of uncertainty: Interoperability

Records systems have dependencies on and relationships with other systems which can be points of vulnerability.
Areas of uncertainty include:
☐Adequacy of identification and specification of interoperability required between records systems and other business systems;
☐Dependency of records systems on data sources external to the records system and capacity to exchange data with these systems (e.g. cloud, other external storage services);
☐Compatibility of standards or specifications for the exchange of records or interoperability between systems;
☐The effectiveness of system interoperability after changes or technological upgrades to either or both of the integrated systems;
☐Management of metadata relating to record controls between systems to sustain usability and meaning of the records.

5.5.5 Areas of uncertainty: Security

Risk assessment of security of records systems can be conducted using the ISO 27000 series of standards and applied as part of the organisation's information security management system, where available. National information system security standards or requirements may also be applicable to records systems.
Annex B, C and D of ISO 27005 include examples of uncertainty areas that apply to any information system.
Uncertainties more specific to records systems include also:
☐Adequacy of the organization's security policy with respect to records, records processes and records systems;
☐Ability to enforce and protect access rules and permissions related to records and records systems;

☐Policy and controls for third parties working on behalf of the organization that affects the storage, access and processing of records and records systems.

5.6 Records processes

The risk identification process focuses on the creation and control processes for managing the records and the records systems.
Based on determining what, when and how records will be created and captured for each business process as identified in the records requirements of the organization, the processes for creating records include:
a) designing the records for each specified business process, including the metadata needed and the format and structure of the records;

b) designing and implementing systems to manage the records including selecting the technologies and determining the metadata created and captured by the records processes to maintain the records over time.

The control processes to be employed by the records systems are categorized as follows:
1) Determining what control information (metadata) shall be created through the records processes and how the metadata will be linked to the records and managed over time;

2) Establishing and complying with rules and conditions for use of the records over time;

3) Maintaining the usability of the records over time;

4) Undertaking authorized disposition of the records;

5) Establishing and maintaining the procedures that shall be used for administration and maintenance of records systems including maintaining the adequacy of these systems in relation to business processes.

5.6.1 Areas of uncertainty: Records design

☐All business activities adequately appraised to identify records requirements;
☐Gathering records requirements comprehensively for each business process, including needs of all interested parties;
☐Adequacy of design (of the structure and form) of the records to meet the records requirements;
☐Naming, controlling and attributing metadata adequate for their purpose;
☐Point of capture of records appropriate (timely, integrated) for the business process and records system(s).

5.6.2 Areas of uncertainty: Records creation and records system implementation

☐Integration of records creation and control with the business processes;
☐Responsibilities — relationship between the record creators and the actors in the business transactions;
☐Metadata management over time;
☐Access management.

5.6.3 Areas of uncertainty: Metadata

☐Metadata technical specification for records systems;
☐On-going maintenance for a metadata technical specification for records systems;
☐Records metadata backed up by an IT backup;
☐ Searchable metadata.

5.6.4 Areas of uncertainty: Use of records and records systems

The process encompasses:
☐Business use of records by staff;
☐Use by external users and/or data subjects;
☐Security classification / access permissions for records;
☐ Security to control access;
☐Security to control modification of records;
☐Controls embedded in metadata for access classification, security classification;
☐Consistency in retrieving and using records as required;
☐Information on who has accessed, used records;
☐Being able to retrieve, use and interpret records in context;
☐Adequacy of training for the staff/users;
☐Staff compliance with the procedures.

5.6.5 Areas of uncertainty: Maintaining useability

The process encompasses:
☐Authenticity, reliability, integrity and useability of records;
☐Use of encryption methods on records;
☐Version/event history of documents and records;
☐Maintenance of metadata over time;
☐Software and hardware obsolescence issues both related to the records and the records system.

5.6.6 Areas of uncertainty: Disposition of records

The process encompasses:
☐Disposal of records implemented as designed and authorised;
☐Disposal documented;

☐Destruction appropriately authorised;
☐Testing whether forensic recovery is possible from the discarded hardware and/or storage device.

6 Analysing identified risks

6.1 General

Risk is analysed by determining its potential consequences and the likelihood of the risk's being realised. In the case of records processes and systems, the consequences are identified according to the area of uncertainty and scaled according to the risk criteria established for the organization as outlined in Clause 4. Existing controls and their effectiveness and efficiency should also be taken into account.

6.2 Likelihood analysis and probability estimation

Likelihood is the probability (or frequency) that the risk event will occur. The likelihood of the identified risks' being realized is analysed according to the nature of the area of uncertainty and the data available over a reasonable period of time sufficient to support a credible estimate.

Each risk has to be assessed in respect of the combination of the likelihood of something happening, and the consequences which arise if it does actually happen. The factors to take into account when assessing probability are outlined in the order of areas of uncertainty in Clause 5.

Probabilities can be expressed in different ways, but normally are related with the level of risk. Qualitative methods can combine consequence, probability and level of risk by significance levels such as "high", "medium" and "low".

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship; formulae used can also vary.

Purely quantitative methods, which use numerical values for consequences and their probabilities, can be used where (statistical) performance data for records processes and systems are available for a substantial period of time.

Scaling the frequency of the event along the time axis can be appropriate for records processes and systems. An example of how probability may be scaled is shown in Table 1.

Table 1 — Example of scaling probability Probability Score	**Interpretation**
1	Rare probability, occurs once every 10 years or less
2	Low probability, occurs once every 3 years or less
3	Medium probability, occurs once a year
4	High probability, occurs more than once every month