УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА “НАЦИОНАЛНА СИГУРНОСТ”
СПЕЦИАЛНОСТ “ИНФОРМАЦИОННА СИГУРНОСТ”

ДИПЛОМНА РАБОТА

НА ТЕМА:

Политики за управление на информационните системи и защита на информацията в организациите

Дипломант:
Никола Господинов
Редовно обучение
Ф.№ 235-ср

Научен ръководител:
(Доц. Н. Митев)

София
2017

Резюме

Целта на дипломната работа е да представи актуалния проблем пред информационната сигурност и нуждата от политики за нейната сигурност и защита.

Разглежда се какво представляват политиките, нуждата от тях и проблемите, с които те са разработени да се справят.

Подробно се разглеждат изискванията, за сертификация по ISO/IEC-20000, пред организациите желаещи да бъдат сертифицирани.

Последната глава от дипломната работа представя прилагането на ISO/IEC- 20000 и за разработване и прилагане на политика за ефективно използване на информационните системи, постигане и поддържане на високо ниво на информационна сигурност, както и отговорностите на ръководството на организациите за разработване и прилагане на тази политика.

Съдържание

1. Увод……..4
2. Въведение……7
3. ISO/IEC-20 000……13
   3.1 Общи изисквания относно системата за управление на услуги…17
   3.2 Разработка и преход към нови или изменени услуги…….25
   3.3 Процеси за предоставяне на услуги…….27
   3.4 Процеси, свързани с взаимоотношенията……...33
4. Ръководство за прилагане на ISO/IEC 20 000……...40
   4.1 Отговорност на ръководството……40
   4.2 Ръководене на процесите, обслужвани от други страни……53
   4.3 Управление на документацията……...56
   4.4 Управление на ресурси…….59
5. Заключение……..69
6. Използвани съкращения
7. Източници

Увод

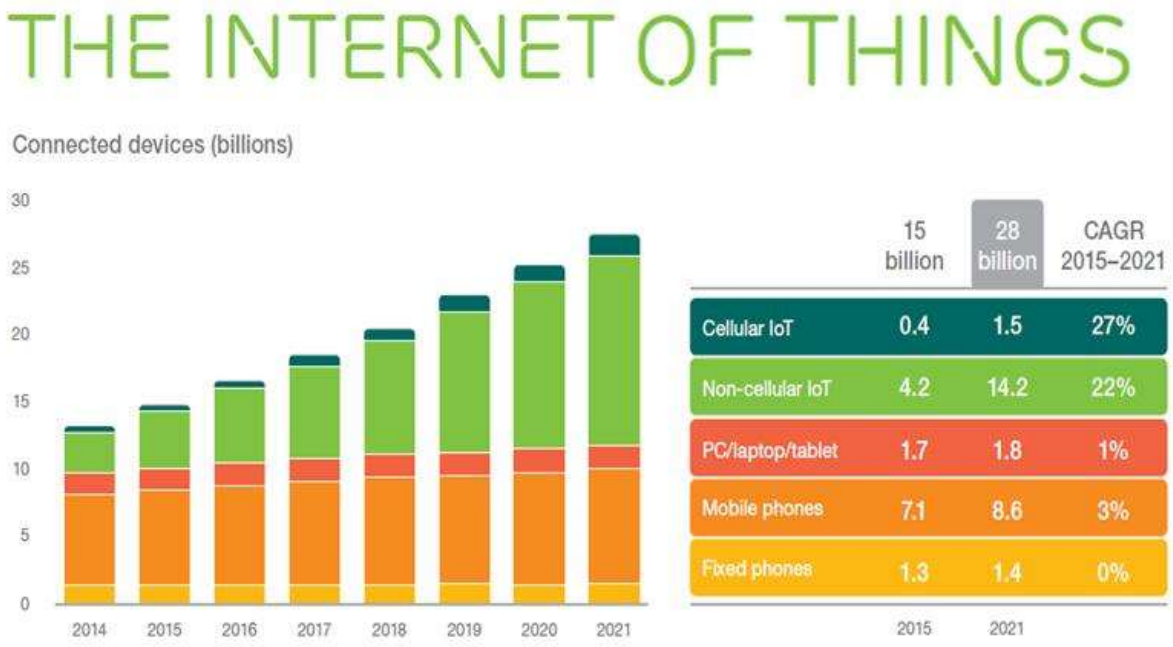
Политика е умението да се управлява полисът и действието по управлението, осъществява се организиран контрол над населението. Този процес може да се изразява в начина на получаване или поддържане на подкрепа за общи или обществени действия. Макар че обикновено терминът се прилага за правителствата, политиката се наблюдава при всички човешки групови взаимодействия, включително корпоративни, академични или религиозни. Разнообразни методи се използват в политиката, които включват рекламиране на собствените политически възгледи сред хората, преговори с други политически групировки, създаване на закони и упражняване на сила, включително война срещу противниците. Политиката се упражнява върху широк кръг социални нива, от кланове и племена на традиционните общества, минавайки през модерните местни власти, фирми и институции и се стигне до суверенни държави и до международно ниво.

Фокусът на тази дипломна работа е върху изграждането и утвърждаването на политика, защитаваща интересите на организациите и техните ресурси чрез конкретни методологии построени спрямо проблемите на света, в който живеем, бързо нарастващите на брой заплахи и нуждата от конструктивни решения за справяне с тях. Тази тема е актуална в целия свят и всеки ден има новини касаещи проблематиката на факта, че все повече информация бива заплашена от нерегламентиран и недобронамерен достъп. Всяка година финансите влети в развиването на информационната сигурност биват увеличавани в пъти спрямо предходната година, специалистите в сферата са високо платени и търсени кадри. Фирмите, сертифицирани по изискванията на стандартите, които ще разгледаме подробно по-нататък, гарантират стремежа към сигурност и утвърждават значимостта на политиките за информационна сигурност и защита.

През последните години технологии като “Internet of things” и “Cloud computing” носят големи печалби на многобройни компании. Възможностите и ползите от тези технологии са огромни и голяма част от населението ги използва без да знаят какво представляват, как работят и дори без да разбират, че те използват нещо, което до преди десетилетие все още е било едва в тестов период.

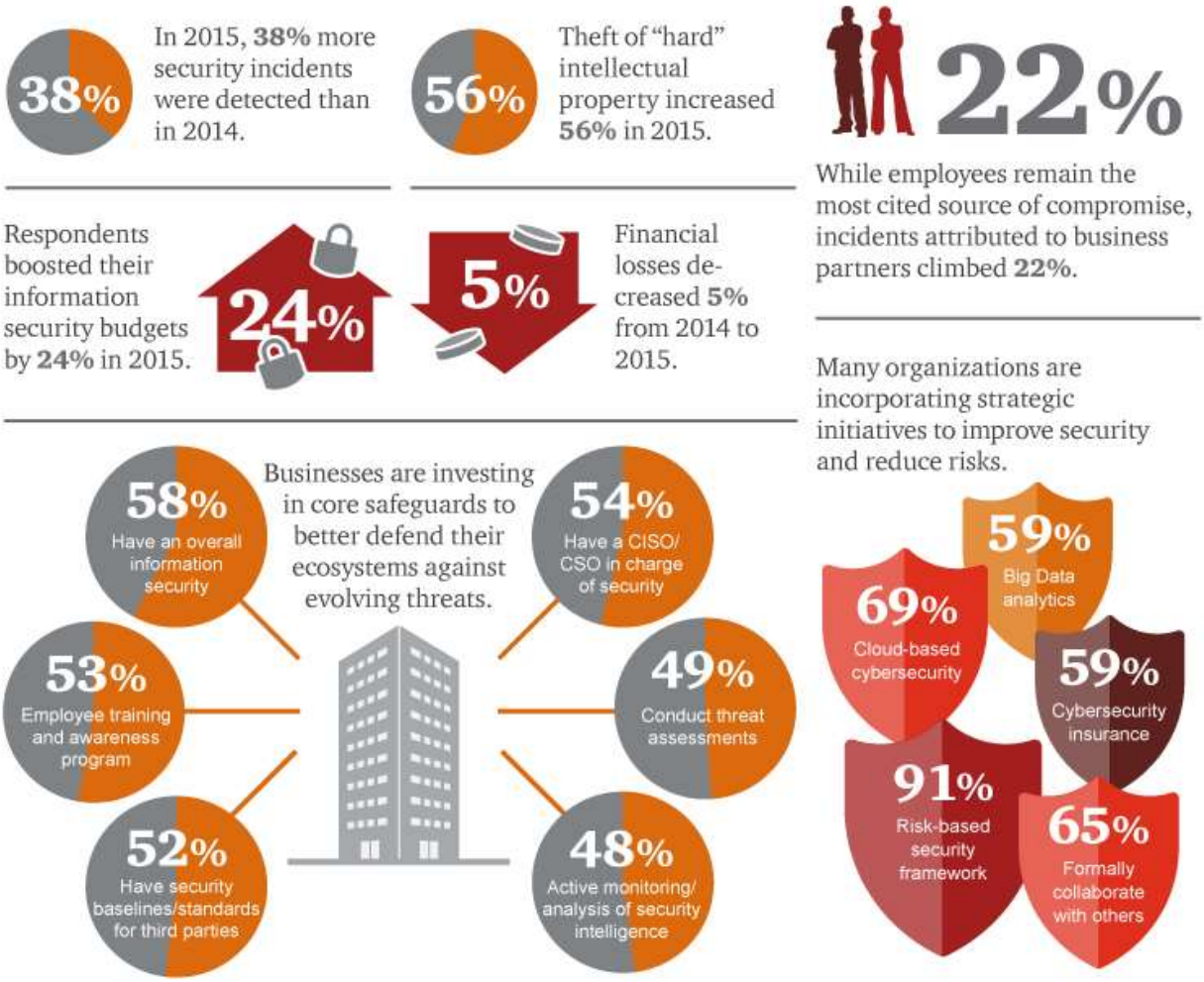
Независимо от това горепосочените и много други подобни или коренно различни технологии боравят с много чувствителна информация. Основата се гради от личната ни информация – снимки, чатове, посещавани сайтове, местоположение добито от GPS модулите в телефоните ни и всевъзможни други. Фирмите и големите корпорации също са част от потребителите на тези технологии, но за разлика от един потребител те могат да имат

информация за милиони хора и незаконното извличане и недобронамереното използване на тази информация може да има последици на световно ниво.
Таблиците по-долу показват огромният брой устройства, в различни сектори, които изграждат “Internet of things” както и прогресивното увеличаване на броят атаки срещу IoT и други технологии.



Фиг. 1.1 Брой устройства в IoT

От фигура 1.1 можем да проследим постоянното нарастване на броят устройства включени в глобална мрежа, обменящи всевъзможна информация постоянно. Очакванията за растеж на броя устройства всяка година се увеличава и с прогресът в различни направления на технологичното развитие все повече устройства ще намерят мястото си в тази постоянно нарастваща мрежа.



Фиг. 1.2 Инцидети и кражба на информация. Нарастване на ангажирания персонал

Фигура 1.2 показва, че заедно с процентното покачване на проблемите за сигурността се покача и наемането на професионалисти в сигурността както и обучаване на персонала за рисковете от различните видове атаки.

Удобствата и продуктивността на технологиите носят и рискове които трябва да бъдат оценени, навременно регистрирани и методично отстранени като за целта се използват политики за сигурност и защита.

Политиката за информационна сигурност е инструмента, който посочва необходимостта от влагане на средства за защита. Тя е официален документ за управленската стратегия за сигурността. Представлява рамка за дефиниране на уместно поведение, определяне базата за необходимите средства, избор на подходящи контроли и създаване на необходимите процедури. Акцентира върху ключовите аспекти наличност, цялостност, поверителност. Отнася се до всеки служител, външен изпълнител и ръководител в организацията.

За да е успешна реализацията на политиката за сигурност целите и дейностите, залегнали в нея, трябва да се базират на целите и изискванията на бизнеса. Задължителни са яснотата относно рисковете и ангажираност на ръководството.

Цели на политиката за информационна сигурност

Целите на политиката за сигурност могат да се разглеждат в два аспекта - човешки и практически. От човешка гледна точка тя определя какво е допустимо и какво не в рамките на организацията, дефинира на кого, какво и при какви обстоятелства е разрешено, информира всички за задълженията им по отношение на сигурността или с други думи въвежда ред.

От практическа гледна точка указва мястото си в контекста на мисията и целите на организацията, предоставя рамка за разработка и внедряване на процедури, установява общи за всички правила за поведение и действие при нарушаване на сигурността.

Структурата на политиката за сигурност

Политиката за информационна сигурност трябва да следва общия стил на подготвяне на документите в организацията. Нейни задължителни характеристики са конкретност, измеримост, приемливост, реалистичност и навременност.

Структурата й включва увод, корпоративна и мрежова политика, политики за информационна сигурност, системно администриране и по отношение на персонала, както и други.

В корпоративната политика се описва общата рамка по отношение на всички политики, действащи в организацията. Дефинират се правилата на разработката, приемането, одобряването и прилагането им. Основната цел на политиката за информационна сигурност е да се гарантира, че информацията е адекватно защитена от промяна и разкриване. Всички информационни активи трябва да имат собственик, който класифицира данните, определя кой има право на достъп до тях, как да се съхраняват,

предават и унищожават и на кои системи какво може да се съхранява и обработва. И всичко това като се отчита местното законодателство. Политиката по отношение на персонала определя подходящата употреба на изчислителните системи - политики за паролите, за ползване на софтуера, електронната поща и преносимите компютри, за достъп до корпоративната мрежа и Интернет.

Документът за системно администриране касае физическата сигурност, контрола на достъпа, политиката за Log on, мерките за гарантиране спазването на политиките, отговорности и одит, сигурност и надеждност на услугите - политики за архивиране и възстановяване, за управление на промените.

Мрежовата политика включва дейностите за разпределени компютърни системи, за отдалечен достъп, за настройка на Интернет защитна стена, маршрутизатори, системи за откриване на проникване, политика за ползване на телефонни мрежи.

Една примерна структура на политика за сигурност би могла да изглежда така:

- Увод;
- Необходимост от политиката и условия за успешното и разработване и прилагане;
- Корпоративна политика;
- Политика за информационна сигурност;
- Политика по отношение на персонала;
- Политика за системно администриране;
- Мрежова политика;
- Други политики;

Реализацията на политиката за информационна сигурност

Реализацията на политиката за информационна сигурност е на базата на дефиниране на процедури, които определят “как” да се защитават източниците, както и механизмите за прилагане на политиките. Те посочват подробно действията, които трябва да се извършат при специфични събития и осигуряват възможност за бърза справка в случай на криза. На практика представляват готови сценарии, помагащи да бъдат елиминирани проблеми.

Разработването на политиката за информационна сигурност минава през няколко етапа:

- Предварителна подготовка;
- Събиране на информация (запознаване с текущото състояние, определяне на рисковете и необходимите мерки за защита, дефиниране на роли и отговорности, запознаване на ръководството и подготовка на първа чернова в свободен текст);
- Писане на политиката - разработка, приемане;
- Привеждане в действие;
- Контрол и периодични прегледи;

Разработване на информационна сигурност са обособени основните моменти, на които трябва да се обърне внимание:

- Осигуряване на одобрението и приемането от ръководството на организацията;
- Установяване на баланс между привилегии и отговорности;
- Постигане на консенсус относно въвеждане и прилагане на политиката на управленско и изпълнителско ниво;
- Начинът, по който политиката за сигурност се привежда в действие;
- Как се реализират предвидените мерки;
- Обучение по въпросите на сигурността;

Процедурата за действие при инциденти например обхваща откриването/засичането им (бърза оценка) и незабавни действия (ограничаване на щетите), подробен анализ на ситуацията, възстановяване на данни, услуги и системи.

След като веднъж е разработена политиката за сигурност е необходимо да се осъществява контрол на изпълнението и периодични прегледи на всеки един от нейните компоненти.

Разработка на политики на сигурност

Постоянно се появяват нови технологии за сигурност. За да разработите добър план на сигурността за мрежата, трябва да знаете с какво разполагате. Също така трябва да можете да определите нивото на сигурност, което е необходимо или желателно за вашата ситуация. Политиките на сигурност трябва да бъдат продукт на общите усилия на целия екип. При тяхното разработване трябва да бъде потърсено съдействието на техническия персонал, ръководството и на представителен брой потребители. За да бъде успешна, една политика на сигурност трябва има поддръжката на мениджърите на организацията и на потребителите. Бюджетните и философските съображения трябва да бъдат балансирани добре с конфиденциалността на данните в мрежата и с отклоненията, ако бъде допуснато компрометиране.

Политиките на сигурност трябва постоянно да се променят и да бъдат преразглеждани и преоценявани периодично при промяна на обстоятелствата. Първата стъпка от създаването на политики е извършването на подробен анализ на сигурността. Трябва да определите какви мерки за сигурност се прилагат в момента, дали те постигат тяхната цел и кои от тях трябва да бъдат премахнати, запазени или заменени.

Съществуват няколко важни елемента, които трябва да се вземем пред вид, когато разработваме политики за сигурност:

- Политики на приемливо използване – Политиката за информационна сигурност в мрежата трябва да включва приемлива политика на използване, която дефинира по какъв начин потребителите могат законно да осъществяват достъп и да използват ресурсите на мрежата. Тя трябва да включва такива елементи, като криптирането на съобщения и файлове, достъпът до Web сайтове, свалянето на файлове от Интернет, използването на пропускателната способност, инсталирането на програми и игри, политиките за електронна поща и други въпроси на крайния потребител.

- Политики на контрол на достъпа - Политиката на сигурност трябва да обхваща процедурите за осигуряване на непрекъсната цялост на данните в мрежата, когато даден служител - особено такъв на техническа позиция - напусне организацията по свое желание или след дисциплинарно уволнение. Особено важно е такива служители да предадат цялата собственост на компанията, която се е намирала под тяхно разпореждане, и да върнат смарт картите и другите устройства за достъп, които са използвали от свое име. Акаунтите на уволнените служители трябва да бъдат незабавно изключени. Ако служителят е имал достъп до конфиденциални данни, не трябва да му се разрешава да взима със себе си дискети, zip устройства или други

носители за съхраняване на данни, без тези носители да бъдат проверени, за да се гарантира, че на тях няма не - оторизирани копия на конфиденциални файлове на организацията.

- Одит на сигурността и откриване на нарушения - Едно изискване за рейтинга на сигурност C2 е възможността за одитиране на събитията на сигурността и действията, извършвани от отделните потребители. Одитът е процес на проследяване на действията на потребителите и на системата. Например одитът включва наблюдение на достъпа до файловете, определяне кога и от кого е осъществен този достъп. Одитът може да включва информация за това, кой е влязъл или излязъл от системата, кой е осъществявал достъп до обекти и кой е упражнявал потребителски права.

Операционни системи като Windows 2000 имат вградено одитиране, който може да бъде конфигуриран за всеки ресурс или потребител поотделно. Събитията на сигурността не само че биват проследявани, но също се записват във файл-дневник за по-лесното им преглеждане. До дневниците на сигурността трябва да имат достъп само администраторите.

Одитиране на сигурността се означава като пасивна форма на откриване на нарушители. Макар че събитията, засягащи сигурността, се записват във файл-дневник, администраторът първо трябва да се усъмни, че има нарушение, и след това да провери файла-дневник, за да определи точния характер на пробива.

В работна среда на мрежа с конфиденциални данни не трябва да се разчита само на пасивното отриване на нарушения. Планът на сигурността трябва да включва една или повече форми на активно откриване. При активното откриване се използва софтуер, който непрекъснато сканира мрежата за признаци на нарушения, а някои програми предупреждават администратора и изключват връзката на подозрителната секция.

COBIT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library) и ISO/IEC-20000 предоставят възможността за разработване и прилагане на политики за изпълнение на описаните по-горе принципи. В рамките на тази дипломна работа ще се спрем подробно на ISO/IEC-20000.

ITIL, COBIT и ISO/IEC-20000 имат какво да предложат и имат различни слаби и силни страни. Изборът на комбинация от най-добрите практики, рамка или стандарт могат да подобрят ефективността и продуктивността на ИТ отдела в организация.

ITIL предлага детайлни напътствия как да имплементираме ИТ процеси и операции, но е слаб при управление и интеграция с рамки или стандарти

като ISO/IEC 20000. От друга страна COBIT 5 е силен в управление и интегриране с други рамки и индустриални стандарти, но не предоставя напътствия за имплементирането им. ISO/IEC-20000 е комбинация от ITIL и COBIT и сертифицирането по ИСО 200000 се прави с цел за организациите да докажат, че те са спазили изискванията на стандарта (Фиг. 2.1). Освен доказателство за качеството на услугите стандартизирането по ISO/IEC 20000 предоставя на организацията конкурентни предимства:

- Позволява да се покаже на партньорите, потребителите, конкурентите, инвеститорите и държавните органи, че има ефективно управление на услугите.
- Своевременно да се разкриват слабости в бизнес-процесите, свързани с управлението на услугите.
- Появява се възможност за изработване на препоръки, насочени към повишаване на нивото на зрелост на процесите в организацията при реализацията на услугите.
- Намалява се риска от преки загуби от предоставянето на нискокачествени услуги.
- Позволява да се осигури високо ниво на защита и да се гарантира сигурността на информацията, обработвана и съхраняване в информационните системи на организациите.

В следващите страници ще се запознаем подробно с изискванията на ISO/IEC-20000 и след това с методологията за прилагане на стандарта.

TÜV NORD

CERTIFICATE

Management system as per
ISO/IEC 20000-1 : 2011

In accordance with TÜV NORD CERT procedures, it is hereby certified that

O2 Czech Republic a.s.
Za Brumlovkou 266/2
140 22 Praha 4
Czech Republic

with the locations according to the annex

applies a management system in line with the above standard for the following scope

Service management system supporting the provision of all kinds of ICT services for communication networks within the technical and organisational structures of O2 Czech Republic a.s., for internal and external customers worldwide.

Certificate Registration No. 44 736 990680
Audit Report No. 3518 2661

Valid until 2019-08-06
Initial certification 2010

Certification Body
at TÜV NORD CERT GmbH

Essen, 2016-09-15

This certification was conducted in accordance with the TÜV NORD CERT auditing and certification procedures and is subject to regular surveillance audits.

TÜV NORD CERT GmbH Langemarckstraße 20 45141 Essen www.tuev-nord-cert.com

itSMF ISO/IEC 20000

APMG International™ ISO/IEC 20000

Фиг. 2 1 Сертификат в съответствие с изискванията на стандарт ISO/IEC 20000

ISO/IEC-20 000

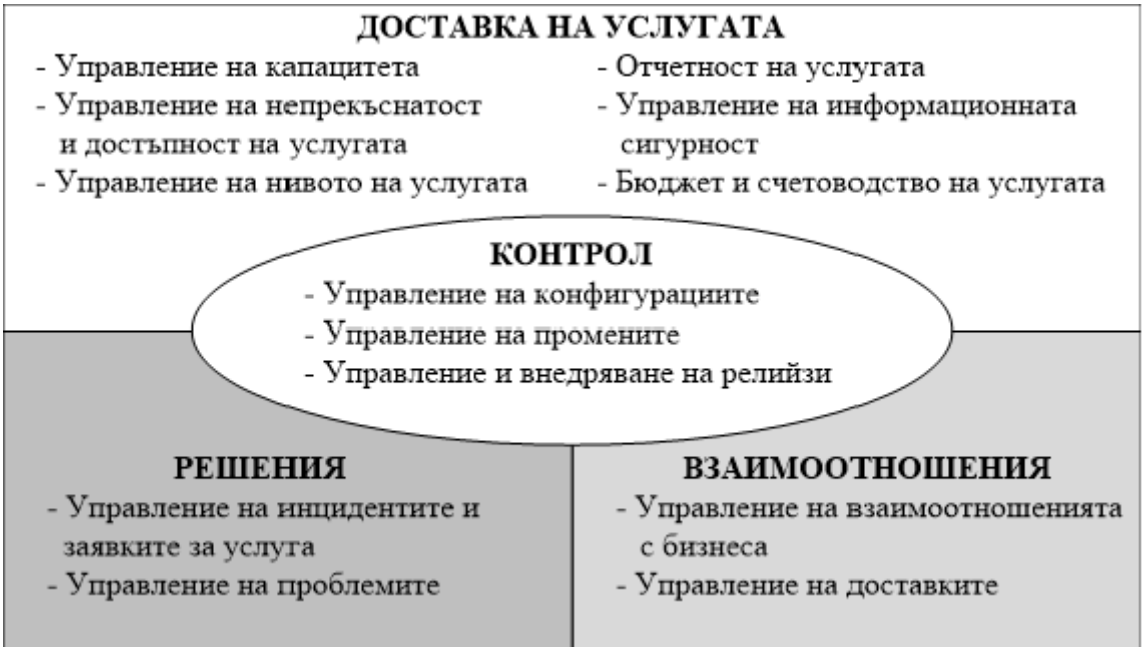
Международната организация за стандартизация (ISO) и Международната електротехническа комисия (IEC) образуват специализирана система за световна стандартизация. Националните органи, които са членове на ISO или IEC, участват в разработването на международни стандарти чрез технически комитети, създадени от съответната организация за отделни области на техническата дейност. Техническите комитети на ISO и IEC си сътрудничат в области от взаимен интерес. В работата участват също така и други международни организации, правителствени и неправителствени, свързани с ISO и IEC. В областта на информационните технологии ISO и IEC създадоха обединен технически комитет ISO/IEC JTC 1.

Международните стандарти се разработват в съответствие с правилата, дадени в Директивите на ISO/IEC, част 2.

Основна задача на обединения технически комитет е да разработва международни стандарти. Проектите на международни стандарти, приети от обединения технически комитет, се разпращат до националните органи - членове за гласуване. Публикуването на международен стандарт изисква одобрението най-малко на 75% от участвалите в гласуването.

Стандартът ISO/IEC 20000-1, който подробно ще разгледаме по-долу е подготвен от обединения технически комитет ISO/IEC JTC 1 Information technology [Информационни технологии], подкомитет SC 7 Софтуер и системен инженеринг.

Изискванията в тази част от ISO/IEC 20000 включват проектиране, преходен период, доставка и усъвършенстване на услугите, които удовлетворяват изискванията относно услугата и придават стойност както за клиента, така и за доставчика на услуги. Тази част на ISO/IEC 20000 изисква интегриран подход към процеса, когато доставчикът на услуги планира, създава, внедрява, поддържа, наблюдава, преразглежда и подобрява системата за управление на услуги (СУУ – Фиг. 2.2).



Фиг. 2 2 Структура на ISO/IEC 20 000. Процеси на управление на ИТ услугата

Координираното интегриране и внедряване на СУУ обезпечава непрекъснат контрол и възможности за непрекъснато подобряване, по-голяма ефективност и ефикасност. Привеждането в действие на процесите, както са определени в тази част на ISO/IEC 20000, изисква персоналът да бъде добре организиран и координиран. Могат да бъдат използвани подходящи инструменти, които да дадат възможност процесите да бъдат ефикасни и ефективни.

Повечето ефикасни доставчици на услуги разглеждат въздействието на СУУ през всички етапи на жизнения цикъл на услугата, от стратегия, през разработване, преходен период и експлоатация/работа, включително и непрекъснато подобряване.

Тази част на ISO/IEC 20000 изисква прилагане на методологията, известна като "Планиране-Изпълнение- Проверка-Действие" (ПИПД) (Plan-Do-Check-Act - PDCA), към всички части на СУУ и на услугите. Методологията ПИПД, приложена към тази част на ISO/IEC 20000, може накратко да бъде описана по следния начин:

- Планиране: създаване, документиране и приемане на СУУ. СУУ включва политиките, целите, плановете и процесите, за да се отговори на изискванията на услугата.

- Изпълнение: внедряване и функциониране на СУУ през разработване, преходен период, доставка и усъвършенстване на услугите.
- Проверка: мониторинг, измерване и преглед на СУУ и на услугите в съответствие с политиките, целите, плановете и изискванията и отчитане на резултатите;
- Действие: предприемане на действия за постоянно подобряване на характеристиките на СУУ и на услугите.

Когато са използвани в рамките на една СУУ, най-важните аспекти на интегрирания подход към процесите и методологията ПИПД са както следва:

- разбиране и изпълнение на изискванията относно услугите за постигане на удовлетвореност на клиента;
- разработване на политика и определяне на цели по управлението на услуги;
- разработване и предоставяне на услуги, основаващи се на СУУ, които придават стойност за потребителя;
- мониторинг, измерване и преглед на характеристиките на СУУ и на услугите;
- непрекъснато подобряване на СУУ и на услугите, основавано на обективни измервания.

Тази част на ISO/IEC 20000 дава възможност на доставчика на услуги да интегрира своята СУУ с други системи за управление в организацията на доставчика на услуги. Възприемането на интегриран подход към процесите и методологията ПИПД дава възможност на доставчика на услуги да съвмести или напълно да интегрира различни стандарти за системи за управление. Така например, системата за управление на услуги може да бъде интегрирана със система за управление на качеството, основаваща се на ISO 9001, или със система за управление на сигурността на информацията, основаваща се на ISO/IEC 27001.

Съзнателно ISO/IEC 20000 е разработен така, че да е независим от специфично ръководство. Доставчикът на услуги може да използва комбинация от общоприети ръководства и своя собствен опит.

Потребителите на даден международен стандарт са отговорни за неговото правилно прилагане. Международният стандарт не претендира да включва всички необходими законови и регулаторни изисквания и договорни задължения на доставчика на услуги. Съответствието с международен стандарт само по себе си не освобождава от законови и

регулаторни изисквания.

Общи приложения

Тази част от ISO/IEC 20000 е стандарт за система за управление на услуги (СУУ). Тя определя изискванията към доставчика на услуги при планиране, създаване, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на една СУУ. Изискванията включват разработка, преходен период, предоставяне и усъвършенстване на услугата, за да се изпълнят изискванията. Тази част на ISO/IEC 20000 може да се използва от:

- организация, която търси услуги от доставчици на услуги и се нуждае от увереност, че нейните изисквания по отношение на услугите ще бъдат удовлетворени;
- организация, която изисква последователен подход от всички свои доставчици на услуги, включително и тези по веригата за доставка;
- доставчик на услуги, който желае да докаже своята способност да разработва, пренася, доставя и подобрява услуги, които отговарят на изискванията;
- доставчик на услуги - за целите на мониторинг, измерване и преглед на своите процеси за управление на услуги и услугите;
- доставчик на услуги, за да подобрява разработката, прехода и доставката на услуги чрез ефикасно внедряване и функциониране на СУУ;

оценител или одитор като критерии за оценяване на съответствието на СУУ на доставчик на услуги с изискванията от тази част на ISO/IEC 20000.

1. Общи изисквания относно системата за управление на услуги

Ангажименти на ръководството

Висшето ръководство трябва да предостави доказателства за своя ангажимент по отношение на планиране, създаване, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на СУУ и на услугите, като:

- създаде и оповести обхвата, политиката и целите по управление на услугите;
- осигури създаването, реализирането и поддържането на план за управление на услугите, който да обезпечи придържане към политиката, постигане на целите за управление на услугите и изпълнение на изискванията към услугите;
- оповести важността от изпълнение на изискванията относно услугите;
- оповести важността от изпълнението на законовите и регулаторни

изисквания и договорните задължения;

- осигури снабдяването с ресурси;
- провежда прегледи от ръководството през планирани интервали;
- осигури рисковете за услугите да са оценени и управлявани.

Политика по управление на услуги

Висшето ръководство трябва да осигури политиката по управление на услуги да:

- е подходяща за целите на доставчика на услуги;
- включва ангажимент за изпълнение на изискванията относно услугите;
- включва ангажимент за непрекъснато подобряване на ефикасността на СУУ и на услугите чрез политиката за продължаващо подобряване;
- осигурява рамка за въвеждане и преглед на целите при управление на услугите;
- е разгласена сред персонала на доставчика на услуги и разбрана от него;
- е преразглеждана с цел непрекъсната пригодност.

Правомощия, отговорности и комуникация

Висшето ръководство трябва да осигури, че:

- правомощията и отговорностите за управление на услугите са дефинирани и се поддържат;
- са създадени и се прилагат документирани процедури за комуникация.

Представител на ръководството

Висшето ръководство трябва да определи член от ръководството на доставчика на услуги, който независимо от останалите си отговорности, да има правомощия и отговорности, включващи:

- осигуряване извършването на дейности за идентифициране, документиране и изпълнение на изискванията относно услугите;
- определяне на правомощия и отговорности, за да се осигури процесите за управление на услугите да са разработени, приложени и подобрявани в съответствие с политиката и целите по управление на услугите;

- осигуряване процесите за управление на услугите да са интегрирани с другите компоненти на СУУ;
- осигуряване, че активите, включително лицензии, използвани за предоставяне на услугите, се управляват съгласно законовите и регулаторни изисквания и договорните задължения;
- докладване пред висшето ръководство за функционирането и възможностите за подобряване на СУУ и на услугите.

Ръководене на процесите, извършвани от други страни

За процесите в точки от 5 до 9 доставчикът на услуги трябва да идентифицира всички процеси или части от процеси, които се извършват от други страни. Другите страни могат да бъдат вътрешна група, клиент или поддоставчик. Доставчикът на услуги трябва да покаже нагледно управляването на процесите, извършвани от други страни, като:

- демонстрира отчетност за процесите и правомощията да изисква придържане към процесите;
- контролира дефинирането на процесите и интерфейсите към други процеси;
- определя изпълнението на процесите и съответствието с изискванията за процесите;
- контролира планирането и определянето на приоритети за подобряване на процесите.

Когато поддоставчик извършва част от процесите, доставчикът на услуги трябва да управлява поддоставчика чрез процес за управление на поддоставчиците. Когато вътрешна група или клиент извършват част от процесите, доставчикът на услуги трябва да управлява вътрешната група или клиента чрез процеса за управление на нивото на услугата.

Управление на документацията

Създаване и поддържане на документи

Доставчикът на услуги трябва да създаде и поддържа документи, включително записи, за осигуряване на ефикасно планиране, функциониране и управление на СУУ. Документите трябва да включват:

- документирана политика и цели по управление на услугите;
- документиран план за управление на услугите;
- документирани политики и планове, създадени за конкретни процеси, както се изисква от тази част на ISO/IEC 20000;
- документиран каталог на услугите;
- документирани споразумения за нивото на услугата;

- документирани процеси за управление на услугите;
- документирани процедури и записи, изисквани от тази част на ISO/IEC 20000;
- допълнителни документи, включително такива от външен произход, определени от доставчика на услуги като необходими за осигуряване на ефикасна работа на СУУ и предоставяне на услугите.

Контрол на документите

Изискваните от СУУ документи трябва да бъдат контролирани. Записите са специален вид документи и трябва да бъдат контролирани според изискванията.

Трябва да бъде създадена документирана процедура, включваща правомощия и отговорности за дефиниране на механизмите за контрол, необходими за:

- създаване и одобряване на документите преди оповестяването им;
- съобщаване на заинтересованите страни за нови или изменени документи;
- преразглеждане и поддържане на документи при необходимост
- осигуряване промените и статута на текущата версия на документите да са идентифицирани;
- осигуряване подходящите версии на приложими документи да са на разположение там, където ще се използват;
- осигуряване документите да са лесно разпознаваеми и четливи;
- осигуряване документите от външен източник да са идентифицирани и тяхното разпространение да е контролирано;
- предотвратяване на неволно използване на излезли от употреба документи и прилагане на подходяща идентификация върху тях, ако те са запазени.

Контрол на записите

Записите трябва да бъдат съхранявани за доказване на съответствие с изискванията за ефикасно функциониране на СУУ.

Трябва да бъде създадена документирана процедура за дефиниране на механизмите за контрол, необходими за идентифициране, съхраняване, защита, запаметяване и изхвърляне на записи. Записите трябва да бъдат четливи и да позволяват лесно идентифициране и възстановяване.

Управление на ресурси

Осигуряване на ресурси

Доставчикът на услуги трябва да определи и осигури човешки, технически, информационни и финансови ресурси, необходими за:

- създаване, внедряване и поддържане на СУУ и на услугите, и непрестанно да подобрява тяхната ефикасност;
- повишаване на удовлетвореността на клиента чрез предоставяне на услуги, които отговарят на изискванията относно услугите.

Човешки ресурси

Персоналът на доставчика на услуги, извършващ дейности, които влияят върху съответствието с изискванията относно услугите, трябва да бъде компетентен въз основа на подходящо образование, обучение, умения и опит. Доставчикът на услуги трябва да:

- определи необходимата компетентност на персонала;
- осигури обучение или предприеме други действия за постигане на необходимата компетентност, когато е подходящо;
- оцени ефикасността на предприетите действия;
- осигури персоналът да е информиран как той допринася за постигане на целите по управление на услугите и изпълнението на изискванията относно услугите;
- поддържа подходящи записи за образованието, обучението, уменията и опита.

Създаване и подобряване на СУУ

Дефиниране на обхвата

Доставчикът на услуги трябва да дефинира и включи обхвата на СУУ в плана за управление на услуги. Обхватът трябва да бъде дефиниран чрез наименованието на организационната единица, предоставяща услугите, и услугите, които трябва да се предоставят.

Доставчикът на услуги трябва също да вземе предвид и други фактори, влияещи върху услугите, които трябва да се предоставят, включително:

- географското местоположение(я), откъдето доставчикът на услуги предоставя услугите;
- клиентите и тяхното местоположение(я);
- използваната технология за предоставяне на услугите.

Планиране на СУУ

Доставчикът на услуги трябва да създаде, внедри и поддържа план за управление на услугите. При планирането трябва да се вземе предвид политиката по управление на услугите, изискванията относно услугите и изискванията в тази част на ISO/IEC 20000.

Планът за управление на услугите трябва да съдържа или да включва указания най-малко за следното:

- целите по управление на услугите, които трябва да бъдат постигнати от доставчика на услуги;
- изисквания относно услугите;
- известните ограничения, които могат да повлияят върху СУУ;
- политиките, стандартите, законовите и регулаторни изисквания и договорните задължения;
- рамките на правомощията, отговорностите и ролите в процеса;
- правомощията и отговорностите за планове, процеси за управление на услуги и услуги;
- човешките, техническите, информационните и финансови ресурси, необходими за постигане на целите по управление на услугите;
- подхода, който трябва да бъде възприет за работа с други страни, включени в разработката и прехода към нов или изменен процес на услуги;
- подхода, който трябва да бъде възприет за интерфейсите между процесите за управление на услуги и тяхното интегриране с други компоненти на СУУ;
- подхода, който трябва да бъде възприет за управление на рискове и критерии за поемане на рискове;
- използваната технология за поддържане на СУУ;
- начина, по който ще бъде измервана, оценявана, отчитана и подобрявана ефикасността на СУУ и на услугите.

Плановете, създадени за конкретни процеси, трябва да бъдат съгласувани с плана за управление на услугите. Планът за управление на услугите и плановете, създадени за конкретни процеси, трябва да бъдат преразглеждани през планирани интервали, и ако е необходимо - актуализирани.

Внедряване и функциониране на СУУ (изпълнение)

Доставчикът на услуги трябва да внедри и експлоатира СУУ за разработване, преход, доставяне и подобряване на услуги съгласно плана за управление на услугите чрез дейности, които включват най-малко следното:

- отпускане и управление на парични средства и бюджети;
- определяне/възлагане на правомощия, отговорности и роли в процесите;
- управление на човешки, технически и информационни ресурси;
- идентифициране, оценяване и управление на рисковете за услугите;
- ръководене на процесите за управление на услуги;

- мониторинг и докладване на характеристиките на дейностите по управление на услугите.

Мониторинг и преглед на СУУ (проверка)

Доставчикът на услуги трябва да използва подходящи методи за мониторинг и измерване на СУУ и на услугите. Тези методи трябва да включват вътрешни одити и прегледи от ръководството.

Целите на всички вътрешни одити и прегледи от ръководството трябва да бъдат документирани. Вътрешните одити и прегледите от ръководството трябва да покажат способността на СУУ и на услугите да постигнат целите по управление на услугите и да отговарят на изискванията относно услугите. Несъответствията трябва да бъдат идентифицирани спрямо изискванията в тази част на ISO/IEC 20000, установените от доставчика на услуги изисквания на СУУ или изискванията към услугите.

Резултатите от вътрешните одити и от прегледите от ръководството, включително идентифицираните несъответствия, безпокойства и действия, трябва да бъдат записани. Резултатите и действията трябва да бъдат съобщени на заинтересованите страни.

Вътрешен одит

Доставчикът на услуги трябва да провежда вътрешни одити през планирани интервали, за да определи дали СУУ и услугите:

- отговарят на изискванията на тази част на ISO/IEC 20000;
- отговарят на изискванията относно услугите и СУУ, идентифицирани от доставчика на услуги;
- са реализирани и се поддържат ефикасно.

Трябва да има документирана процедура, включваща правомощията и отговорностите за планиране и провеждане на одити, отчитане на резултатите и поддържане на записи от одитите.

Трябва да бъде планирана програма за одит. Тя трябва да вземе предвид състоянието и важността на процесите и областите, подлежащи на проверка, както и резултатите от предишни одити. Критериите, обхватът, честотата и методите на провеждане трябва да бъдат документирани.

Изборът на одитори и провеждането на одити трябва да осигурят обективност и безпристрастност на процеса на одит. Одиторите не трябва да извършват одит на своята собствена работа.

Несъответствията трябва да бъдат съобщени, подредени по приоритет и трябва да бъдат определени отговорности за действията. Ръководството, което отговаря за одитираната област, трябва да осигури всички корекции и коригиращи действия да са предприети без ненужно забавяне, за да бъдат премахнати несъответствията и причините за тях. Последващите действия трябва да включват верификация на предприетите действия и отчитане на резултатите.

Преглед от ръководството

Висшето ръководство трябва да извършва преглед на СУУ и на услугите през планирани интервали, за да осигури тяхното непрекъснато съответствие и ефикасност. Този преглед трябва да включва оценка на възможностите за подобряване и необходимостта от промени в СУУ, включително на политиката и целите по управление на услугите.

Входните елементи за прегледите от ръководството трябва да включват най-малко информация относно:

- обратна връзка от клиентите;
- характеристики и съответствие на услугите и процесите;
- нива на текущи и прогнозни човешки, технически, информационни и финансови ресурси;
- текущи и прогнозни човешки и технически възможности;
- рискове;
- резултати от одити и последващи действия;
- резултати и последващи действия от предишни прегледи от ръководството;
- състояние на превантивните и коригиращи действия;
- промени, които могат да повлияят върху СУУ и услугите;
- възможности за подобряване.

Записите от прегледите от ръководството трябва да бъдат съхранявани.

Записите от прегледа от ръководството трябва да включват най-малко решения и действия по отношение на ресурсите, подобряване на ефикасността на СУУ и подобряване на услугите.

Поддържане и подобряване на СУУ (действие)

Общи положения

Трябва да има политика за непрекъснато подобряване на СУУ и на услугите. Политиката трябва да включва критерии за оценка на възможностите за подобряване.

Трябва да има документирана процедура, включваща правомощията и отговорностите за идентифициране, документиране, оценяване, одобряване, определяне на приоритети, измерване и отчитане на подобренията. Трябва да бъдат документирани възможностите за подобряване, включително коригиращите и превантивните действия.

Трябва да бъдат коригирани причините за идентифицираните несъответствия. За да се предотвратят повторения, трябва да бъдат предприети коригиращи действия за елиминиране на причината за идентифицираните несъответствия. Трябва да бъдат предприети превантивни действия, за да се премахне причината за потенциални несъответствия, така че те да бъдат предотвратени.

Управление на подобренията

Трябва да бъдат определени приоритети на възможностите за подобрение. Когато взима решения относно възможностите за подобряване, доставчикът на услуги трябва да използва критерии за оценка в политиката за непрекъснато подобряване.

Одобрените подобрения трябва да бъдат планирани.

Доставчикът на услуги трябва да управлява дейностите по подобряване, които включват най-малко:

- поставяне на цели за подобряване в едно или повече от следното: качество, стойност, способност, цена, продуктивност, използване на ресурсите и намаляване на риска;
- осигуряване, че одобрените подобрения да бъдат осъществени;
- преразглеждане на политиките, плановете, процесите и процедурите за управление на услугите, където е необходимо;
- измерване на осъществените подобрения по отношение на поставените цели, и когато целите не са постигнати, предприемане на необходими действия;
- отчитане на осъществените подобрения.

2. Разработка и преход към нови или изменени услуги

Доставчикът на услуги трябва да използва този процес за всички нови услуги и изменения в услуги с възможности за сериозно въздействие върху услугите или клиента. Измененията, които попадат в обсега на точка 5, трябва да бъдат определени в политиката по управление на измененията, съгласувана като част от процеса за управление на изменения.

Оценяването, одобряването, включването в плана и преразглеждането на нови или изменени услуги в обсега на точка 5 трябва да бъдат контролирани от процеса за управление на изменения. Елементите на конфигурацията, повлияни от нови или изменени услуги в обсега на точка 5, трябва да бъдат контролирани чрез процеса за управление на конфигурацията.

Доставчикът на услуги трябва да преразглежда изходните елементи от дейностите по планиране и разработка на нови или изменени услуги съобразно договорените изисквания относно услугите и свързаните с това изисквания. Въз основа на този преглед доставчикът на услуги трябва да приеме или отхвърли изходите. Доставчикът на услуги трябва да предприеме необходимите действия, за да осигури разработката и преходът към нови или изменени услуги да може да бъде извършено ефикасно, като се използват приетите изходи.

Планиране на нови или изменени услуги

Доставчикът на услуги трябва да идентифицира изискванията относно нови или изменени услуги. Новите или изменени услуги трябва да

бъдат планирани, за да изпълнят изискванията относно услугите. Планирането на нови или изменени услуги трябва да бъде съгласувано с клиента или със заинтересованите страни.

Като входни елементи за планирането доставчикът на услуги трябва да вземе под внимание потенциалното финансово, организационно и техническо въздействие от предоставянето на нови или изменени услуги. Доставчикът на услуги трябва също така да вземе под внимание потенциалното въздействие на новите или изменени услуги върху СУУ.

Планирането на нови или изменени услуги трябва да съдържа или да включва посочване най-малко на следното:

- правомощия и отговорности за дейностите по разработване, развитие и преход;
- дейности, които трябва да бъдат извършени от доставчика на услуги и други страни, включително дейности през интерфейсите от доставчика на услуги към другите страни;
- връзка със заинтересованите страни;
- човешки, технически, информационни и финансови ресурси;
- графици за планираните дейности;
- идентифициране, оценяване и управление на рискове;
- зависимости от други услуги;
- необходими изпитвания за новите или изменени услуги;
- критерии за приемане на услугите;
- очаквани резултати от предоставянето на новите или изменени услуги, изразени в измерими показатели.

За услуги, които трябва да бъдат прекратени, доставчикът на услуги трябва да планира прекратяването на услугата (ите). Планирането трябва да включва датата(ите) за преустановяване, архивиране, изхвърляне или прехвърляне на данни, документация и компоненти на услугата. Компонентите на услугата може да включват инфраструктура и приложения със свързани лицензи.

Доставчикът на услуги трябва да идентифицира други страни, които ще допринесат за предоставянето на компоненти за нови или изменени услуги. Доставчикът трябва да оцени тяхната способност за изпълняване на изискванията относно услугите. Резултатите от оценяването трябва да бъдат записани и трябва да бъдат предприети съответни действия.

Разработване и развитие на нови или изменени услуги

Новите или изменени услуги трябва да бъдат разработени и документирани, така че да включват най- малко:

- правомощия и отговорности за предоставяне на нови или изменени услуги;

- дейности, които трябва да бъдат извършени от доставчика на услуги, клиента и от други страни за доставка на новите или изменени услуги;
- нови или изменени изисквания към човешките ресурси, включително изисквания за подходящо образование, обучение, умения и опит;
- изисквания към финансовите ресурси за предоставяне на нови или изменени услуги;
- нова или изменена технология за поддържане на доставката на новите или изменени услуги;
- нови или изменени планове и политики, изисквани от тази част на ISO/IEC 20000;
- нови или изменени договори и други документирани споразумения за съгласуване с измененията в изискванията относно услугите;
- промени в СУУ;
- нови или изменени СНУ;
- актуализации в каталога на услугите;
- процедури, мерки и информация, които да бъдат използвани за предоставяне на новите или изменени услуги.

Доставчикът на услуги трябва да осигури разработването да позволява новите или изменени услуги да изпълнят изискванията относно услугите. Новите или изменени услуги трябва да бъдат разработени в съответствие с документиран проект.

Преход към нови или изменени услуги

Новите или изменени услуги трябва да бъдат изпитани, за да се верифицира, че те изпълняват изискванията относно услугите и документирания проект. Новите или изменени услуги трябва да бъдат верифицирани спрямо критериите за приемане на услуги, предварително съгласувани между доставчика на услуги и заинтересованите страни. Ако критериите за приемане на услугата не се спазени, доставчикът на услуги и заинтересованите страни ще вземат решение относно необходимите действия.

Процесът за управление пускането и разгръщането на услугата трябва да бъде използван за разгръщане в естествената среда на одобрена нова или изменена услуга.

След завършване на преходните дейности доставчикът на услуги трябва да докладва на заинтересованите страни за постигнатите резултати, сравнени с очакваните резултати.

3. Процеси за предоставяне на услуги

Управление на нивото на услуга

Доставчикът на услуги трябва да съгласува с клиента услугите, които

ще бъдат предоставяни.

Доставчикът на услуги трябва да съгласува с клиента каталог на услугите. Каталогът на услугите трябва да включва зависимостите между услугите и компонентите на услуги.

За всяка предоставена услуга с клиента трябва да бъде договорено едно или повече споразумения за нивото на услугата (СНУ). При създаването на СНУ доставчикът на услуги трябва да вземе предвид изискванията относно услугата. В СНУ трябва да се включват договорените цели на услугата, работни характеристики и изключения.

Доставчикът на услуги трябва да преразглежда услугите и СНУ с клиента през планирани интервали.

Измененията в документираните изисквания към услугите, каталогът на услуги, СНУ и други документирани споразумения трябва да бъдат контролирани чрез процеса за управление на изменения. Каталогът на услуги трябва да бъде поддържан, следвайки измененията на услугите и СНУ, за да се осигури съгласуваност между тях.

През планирани интервали доставчикът на услуги трябва да прави мониторинг на тенденциите и работата, сравнени с целите на услугите. Резултатите трябва да бъдат записвани и разглеждани, за да бъдат идентифицирани причините за несъответствия и възможностите за подобряване.

За компонентите на услугата, предоставяни от вътрешна група или от клиента, доставчикът на услуги трябва да разработи, съгласува, прегледа и поддържа документирано споразумение за дефиниране на дейностите и интерфейсите между двете страни. Доставчикът на услуги трябва да наблюдава през планирани интервали работата на вътрешната група или на клиента по отношение на договорените цели по услугата и други договорени ангажименти. Резултатите трябва да бъдат записвани и разглеждани, за да бъдат идентифицирани причините за несъответствия и възможностите за подобряване.

Отчитане на услуга

Описанието на всеки доклад за услуга трябва да бъде документирано и съгласувано между доставчика на услуги и заинтересованите страни, включително неговата идентичност, цел, предназначение, честота и подробности за източника(ците) на данни.

Отчети за услуги трябва да се изработват за услуги, като се използва информация от предоставянето на услугата и дейностите на СУУ, включително процесите за управление на услугите. Отчитането на услуга трябва да включва най-малко:

- достигнати характеристики спрямо целите на услугата;
- съответна информация относно съществени събития, включващи най-малко значителните произшествия, които предизвикват разгръщане

на нови или изменени услуги и позоваване на плана за непрекъснатост на услугите;

- характеристики на работно натоварване, включително обеми и периодични промени в работното натоварване;
- открити несъответствия спрямо изискванията на тази част на ISO/IEC 20000, изискванията на СУУ или изискванията относно услугите и идентифицираните причини;
- информация относно тенденциите;
- измервания на удовлетвореността на клиента, оплаквания от услуги и резултати от анализа на измерванията на удовлетвореността и на оплакванията;

Доставчикът на услуги трябва да вземе решения и да предприеме действия, основаващи се на заключенията в докладите за услуги. Съгласуваните действия трябва да бъдат съобщени на заинтересованите страни.

Управление на наличността и непрекъснатостта на услугата

Изисквания за наличност и непрекъснатост на услугата

Доставчикът на услуги трябва да оцени и документира рисковете за непрекъснатост на услуга и наличността на услугата. Доставчикът на услуги трябва да идентифицира и съгласува с клиента и със заинтересованите страни изискванията за непрекъснатост и достъпност. Съгласуваните изисквания трябва да отчитат приложимите бизнес планове, изискванията относно услугите, СНУ и рисковете.

Съгласуваните изисквания за непрекъснатост и наличност на услуга трябва да включват най-малко:

- права за достъп до услугите;
- време за реакция на услугите;
- наличие на услугата от край до край.

Планове за наличност и непрекъснатост на услугата

Доставчикът на услуги трябва да създаде, внедри и поддържа план(ове) за непрекъснатост и план(ове) за наличност на услугите.

Промените в тези планове трябва да бъдат контролирани чрез процеса за управление на измененията. Планът(овете) за непрекъснатост на услугите трябва да включва най-малко:

- процедури, които трябва да се приложат в случай на значителна загуба на услуга, или позоваване на тях;
- цели по отношение на наличността, когато планът се задейства;
- изисквания за възстановяване;
- подход за връщане към нормални работни условия.

Планът(овете) за непрекъснатост на услугите, списъците с контакти и БДУК трябва да бъдат достъпни, когато е възпрепятстван достъпа до нормалните местоположения на услугата.

Планът(овете) за налиност трябва да включва най-малко изискванията за наличие и целите.

Доставчикът на услуги трябва да оцени въздействието на заявките за изменения върху плана(овете) за непрекъснатост и плана(овете) за наличност на услугите.

Наблюдение и изпитване на непрекъснатостта и наличността на услугата

Наличността на услугата трябва да бъде наблюдавана, а резултатите да бъдат записвани и сравнени с договорените цели. Непланираната липса на наличност трябва да бъде разследвана и да бъдат предприети необходимите действия.

Плановете за непрекъснатост на услугата трябва да бъдат изпитани спрямо изискванията за непрекъснатост на услугата. Плановете за наличност трябва да бъдат изпитани спрямо изискванията за наличност. Плановете за непрекъснатост и наличност на услугата трябва да бъдат отново изпитани след основни изменения в обкръжаващата среда, в която работи доставчикът на услуги.

Резултатите от изпитванията трябва да бъдат записвани. След всяко изпитване и след задействане на плана за непрекъснатост на услугата трябва да бъдат провеждани прегледи. Там където се открият различия, доставчикът на услуги трябва да предприеме необходимите действия и да докладва за предприетите действия.

Бюджет и счетоводство за услугите

Трябва да има дефиниран интерфейс между процеса по определяне на бюджет и счетоводство за услугите и другите процеси на финансовото управление.

Трябва да има политики и документирани процедури за:

- определяне на бюджет и счетоводство за компонентите на услугите, включващо най-малко:
  1. активите, използвани за предоставяне на услугите, включително и лицензии,
  2. споделени ресурси,
  3. начисления,
  4. капиталови разходи и разходи за експлоатация,
  5. външно доставени услуги,
  6. персонал,
  7. технически и други средства;
- разпределяне на непреките разходи и прехвърляне на преките разходи към услугите, за да се осигурят общите разходи за всяка услуга;
- ефикасен финансов контрол и одобряване.

Разходите трябва да бъдат включени в бюджета, за да се осигури ефикасен финансов контрол и да се вземат решения за предоставените услуги.

Доставчикът на услуги трябва да наблюдава и отчита разходите спрямо бюджета, да преразглежда финансовите прогнози и да управлява разходите.

При процеса за управление на измененията трябва да бъде предоставена информация за поддържане остойностяването на заявките за изменения.

Управление на капацитета

Доставчикът на услуги трябва да идентифицира и съгласува изискванията за капацитет и работни характеристики с клиента и със заинтересованите страни.

Доставчикът на услуги трябва да създаде, внедри и поддържа план за капацитета, който взема под внимание човешки, технически, информационни и финансови ресурси. Измененията в плана за капацитета трябва да бъдат контролирани от процеса за управление на измененията.

Планът за капацитета трябва да включва най-малко:

- текущо и прогнозно търсене на услуги;
- очаквано въздействие на съгласуваните изисквания за наличност, непрекъснатост на услугата и нива на услугата;
- графици, прагове и разходи за достигане капацитета на услугата;
- потенциално въздействие на законови, регулаторни, договорни или организационни промени;
- потенциално въздействие на нови технологии и методи;
- процедури за даване на възможност за прогнозен анализ или позоваване на тях.

Доставчикът на услуги трябва да наблюдава използването на капацитета, да анализира данните за капацитета и да привежда в съответствие работните характеристики. Доставчикът на услуги трябва да осигури достатъчен капацитет, за да изпълни договорените изисквания за капацитет и производителност.

Управление на сигурността на информацията

Политика по сигурност на информацията

Ръководство с подходящи правомощия трябва да одобри политика по сигурност на информацията, като вземе под внимание изискванията относно услугите, законовите и регулаторните изисквания и договорните задължения. Ръководството трябва:

- да съобщи на персонала на доставчика на услуги, на клиента и на външните доставчици политиката по сигурност на информацията и важността от съобразяването с политиката;
- да осигури задачите на управлението на сигурността да са установени;

- да дефинира подход, който трябва да бъде възприет за управление на рисковете за сигурността на информацията и критериите за приемане на рискове;
- да осигури провеждането на оценяване на рисковете за сигурността на информацията през планирани интервали;
- да осигури провеждането на вътрешни одити на сигурността на информацията;
- да осигури разглеждане на резултатите от одит, за да се определят възможностите за подобряване.

Механизми за контрол на сигурността на информацията

Доставчикът на услуги трябва да внедри и използва физически, административни и технически механизми за контрол на сигурността на информацията, за да:

- запази конфиденциалността, интегритета и достъпността на информационните активи;
- изпълни изискванията на политиката по сигурност на информацията;
- постигне целите по управление на сигурността на информацията;
- управлява рисковете, свързани със сигурността на информацията.

Тези механизми за контрол на сигурността на информацията трябва да бъдат документирани и трябва да описват рисковете, за които се отнасят механизмите за контрол, тяхното функциониране и поддържане.

Доставчикът на услуги трябва да преразглежда ефикасността на механизмите за контрол на сигурността на информацията. Доставчикът на услуги трябва да предприеме необходимите действия и да докладва за предприетите действия.

Доставчикът на услуги трябва да идентифицира външни организации, които имат необходимост от достъп, използване или управляване на информация или услуги от доставчика на услуги. Доставчикът на услуги трябва да документира, съгласува и прилага механизмите за контрол на сигурността на информацията с тези външни организации.

Изменения в сигурността на информацията и инциденти

Заявките за изменения трябва да бъдат оценени, за да се идентифицират:

- нови или изменени рискове за сигурността на информацията;
- потенциално въздействие върху съществуващите политика за информационна сигурност и механизми за контрол.

Инцидентите по отношение на сигурността на информацията трябва да бъдат управлявани, като се прилагат процедурите за управление на инциденти с подходящ за рисковете в сигурността на информацията приоритет. Доставчикът на услуги трябва да анализира видовете, обемите и

въздействията от инцидентите със сигурността на информацията. Инцидентите по отношение на сигурността на информацията трябва да бъдат докладвани и разглеждани, за да се идентифицират възможностите за подобряване.

4. Процеси, свързани с взаимоотношенията

Управление на бизнес взаимоотношения

Доставчикът на услуги трябва да идентифицира и документира клиентите, потребителите и заинтересованите от услугите страни.

За всеки клиент доставчикът на услуги трябва да има определено лице, което отговаря за управлението на взаимоотношенията с клиента и неговата удовлетвореност.

Доставчикът на услуги трябва да установи механизъм за комуникациця с клиента. Механизмът за комуникация трябва да спомага за разбирането на средата, в която се извършват услугите, и на изискванията за нови или изменени услуги. Тази информация трябва да позволи на доставчика на услуги да отговори на тези изисквания.

Съвместно с клиента доставчикът на услуги трябва през планирани интервали да извършва преглед на изпълнението на услугите.

Измененията в документираните изисквания относно услугите трябва да бъдат контролирани чрез процеса за управление на измененията. Измененията в СНУ трябва да бъдат координирани чрез процеса за управление нивото на услугите.

Дефиницията за оплакване от услуга трябва да бъде съгласувана с клиента. Трябва да има документирана процедура за управление на оплакванията от услуга от страна на клиента. Доставчикът на услуги трябва да записва, разследва, действа, докладва и приключва оплаквания от услуга. Когато оплакване от услуга не е разрешено чрез нормалните канали, на клиента трябва да бъде осигурено разглеждане от по-високо ниво.

Доставчикът на услуги трябва да измерва удовлетвореността на клиента през планирани интервали въз основа на представителна извадка от клиенти и потребители на услугите. Резултатите трябва да бъдат анализирани и прегледани, за да се идентифицират възможностите за подобряване.

Управление на поддоставчици

Доставчикът на услуги може да използва поддоставчици за внедряване и експлоатация на някои части от процеса за управление на услугите.

За всеки поддоставчик доставчикът на услуги трябва да има определено лице, което да отговаря за управлението на взаимоотношенията, договора и работата на поддоставчика.

Доставчикът на услуги и поддоставчикът трябва да одобрят писмен

договор. Договорът трябва да съдържа или да включва следното:

- обхват на услугите, които ще се предоставят от поддоставчика;
- взаимовръзка между услуги, процеси и страни;
- изисквания, които трябва да бъдат изпълнени от поддоставчика;
- цели на услугите;
- интерфейси между процесите за управление на услугите, извършвани от поддоставчика и останалите страни;
- интегриране на дейностите на поддоставчика в рамките на СУУ;
- работни характеристики;
- изключения от договора и как те ще се борави с тях;
- правомощия и отговорности на доставчика на услуги и поддоставчика;
- отчети и информация, които трябва да бъдат предоставяни от поддоставчика;
- основи за таксуването;
- дейности и отговорности при очаквано или ранно прекратяване на договора и прехвърлянето на услугите на друга страна.

Доставчикът на услуги трябва да съгласува с поддоставчика нивата на услугите, така че да поддържат и да са изравнени със СНУ между доставчика на услуги и клиента.

Доставчикът на услуги трябва да осигури, че ролите и взаимоотношенията между водещи доставчици и доставчици - подизпълнители са документирани. Доставчикът на услуги трябва да верифицира, че водещите поддоставчици управляват своите подизпълнители за спазване на договорните задължения.

Доставчикът на услуги трябва да наблюдава работата на поддоставчика през планирани интервали. Работните характеристики трябва да бъдат измервани спрямо целите на услугата и други договорни задължения. Резултатите трябва да бъдат записвани и прегледани, за да се идентифицират причините за несъответствия и възможностите за подобряване. Прегледът трябва също да осигури договорът да отразява текущите изисквания.

Измененията в договора трябва да бъдат контролирани чрез процеса за управление на изменения.

Трябва да има документирана процедура за управление на споровете по договора между доставчика на услуги и поддоставчика.

Процеси, свързани с вземането на решения

Управление на инциденти и заявки за услуга

Трябва да има документирана процедура за всички инциденти, която да дефинира:

- регистриране;
- определяне на приоритет;
- категоризиране;
- актуализиране на записите;
- отнасяне на въпроса на по-високо управленско ниво;
- разрешаване;
- приключване.

Трябва да има документирана процедура за управляване изпълнението на заявките за услуги, от регистриране до приключване. Инцидентите и заявките за услуги трябва да бъдат управлявани съгласно процедурите.

Когато се определят приоритетите на инциденти и на заявки за услуги доставчикът на услуги трябва вземе предвид въздействието и неотложността на инцидента или на заявката за услуги.

Доставчикът на услуги трябва да осигури персоналът, включен в процеса за управление на инциденти и заявки за услуги, да има достъп и да може да използва съответната информация. Тази информация трябва да включва процедурите за управление на заявки за услуги, известни грешки, разрешаване на проблеми и базата данни за управление на конфигурацията. В процеса за управление на инциденти и заявки за услуги трябва да бъде използвана информацията от процеса за управление на версията и разгръщане на услугата относно успешното или неуспешното въвеждане на версиите и датите на следващата версия.

Доставчикът на услуги трябва да информира клиента относно напредъка по техния регистриран инцидент или заявка за услуга. Ако не могат да бъдат постигнати целите по услугата, доставчикът на услуги трябва да информира клиента и заинтересованите страни и да постави въпроса пред ръководство на по-високо ниво съгласно процедурата.

Доставчикът на услуги трябва да документира и съгласува с клиента дефиницията за голям инцидент. Големите инциденти трябва да бъдат категоризирани и управлявани съгласно документирана процедура. Висшето ръководство трябва да бъде информирано за големи инциденти. Висшето ръководство трябва да осигури назначаването на определено лице, отговорно за управлението на големи инциденти. След възстановяване на приетата услуга големите инциденти трябва да бъдат разгледани с оглед идентифициране на възможностите за подобряване.

Управление на проблеми

Трябва да има документирана процедура за идентифициране на проблемите и намаляване или избягване на въздействието на инцидентите и проблемите. Процедурата за управление на проблеми трябва да дефинира:

- идентификация;
- регистриране;

- определяне на приоритет;
- категоризиране;
- актуализиране на записите;
- повдигане на въпроса на по-високо управленско ниво;
- разрешаване;
- приключване.

Проблемите трябва да бъдат управлявани съгласно процедурата.

Доставчикът на услуги трябва да анализира данните и тенденциите за инциденти и проблеми, за да идентифицира основните причини и потенциалните превантивни действия.

Проблеми, които изискват промени в ЕК, трябва да бъдат решавани чрез подаване на заявка за изменение.

Когато основната причина е идентифицирана, обаче проблемът не е решен за постоянно, доставчикът на услуги трябва да определи действия за намаляване или елиминиране на въздействието на проблема върху услугите. Известните грешки трябва да бъдат записвани.

Ефикасността на решаването на проблеми трябва да бъде наблюдавана, преглеждана и отчитана.

Актуална информация относно известни грешки и решения на проблеми трябва да бъде предоставена в процеса за управление на инциденти и заявки за услуги.

Процеси на управление

Управление на конфигурация

Трябва да има документирана дефиниция за всеки вид от елементите на конфигурацията (ЕК). Записаната информация за всеки ЕК трябва да осигурява ефикасен контрол и да включва най-малко:

- описание на ЕК;
- взаимовръзка(и) между ЕК и други ЕК;
- взаимовръзка(и) между ЕК и компонентите на услугата;
- статут;
- версия;
- местоположение;
- свързани заявки за изменение;
- свързани проблеми и известни грешки.

Елементите на конфигурацията трябва да бъдат идентифицирани по единствен за рода си начин в БДУК. БДУК трябва да бъда управлявана, за да се осигури нейната надеждност и точност, включително и контрол върху достъпа за обновяване.

Трябва да има документирана процедура за записване, контрол и проследяване на версиите на ЕК. Степента на контрол трябва да поддържа

целостта на услугите и компонентите на услугите, отчитайки изискванията относно услугите и свързаните с ЕК рискове.

Доставчикът на услуги трябва да проверява през планирани интервали натрупаните в БДУК записи. Когато се открият недостатъци, доставчикът на услуги трябва да предприеме необходимите действия и да докладва за предприетите действия.

Информация от БДУК трябва да бъде предоставена в процеса за управление на измененията в подкрепа на оценяването на заявките за изменение.

Измененията в ЕК трябва да бъдат проследими и проверяеми, за да се осигури цялост на ЕК и на данните в БДУК.

Преди разгръщане на версия в реална среда трябва да бъде взета основата на конфигурацията на засегнатите ЕК.

Първите оригинали от ЕК, записани в БДУК, трябва да бъдат съхранявани в сигурни физически или електронни библиотеки, към които да има позоваване в записите на конфигурацията. Това трябва да включва най-малко документация, информация за лицензи, софтуер и, когато са налични, изображения на хардуерната конфигурация.

Трябва да има дефиниран интерфейс между процеса за управление на конфигурацията и процеса за управление на финансовите активи.

Управление на изменения

Трябва да бъде установена политика за управление на измененията, която да дефинира:

- a) онези ЕК, които са под контрола на управлението на измененията;
- b) критерии за определяне на изменения, които може да имат сериозно въздействие върху услугите или клиента.

Прекратяване на услуга трябва да бъде класифицирано като изменение с потенциал за сериозно въздействие. Прехвърлянето на услуга от доставчик на услуги към клиента или друга страна трябва да бъде класифицирано като изменение с потенциал за сериозно въздействие.

Трябва да има документирана процедура за регистриране, категоризиране, оценяване и одобряване на заявките за промени.

Доставчикът на услуги трябва да документира и съгласува с клиента дефиницията за спешно изменение. Трябва да има документирана процедура за управление на спешни изменения.

Всички изменения в услуга или в компонент на услуга трябва да бъдат предизвикани от заявка за изменение. Заявките за изменение трябва да имат дефиниран обхват.

Всички заявки за изменение трябва да бъдат регистрирани и категоризирани. Заявки за изменение, категоризирани като имащи потенциал за сериозно въздействие върху услугите или клиента, трябва да бъдат управлявани чрез процеса за разработка и преход към нови или

изменени услуги. Всички други заявки за изменение на ЕК, дефинирани в политиката за управление на измененията, трябва да бъдат управлявани, като се използва процесът за управление на измененията.

Заявките за изменение трябва да бъдат оценявани, като се използва информация от процеса за управление на изменения и другите процеси.

Доставчикът на услуги и заинтересованите страни трябва да взимат решения за приемане на заявки за изменение. При вземането на решение трябва да се вземат предвид рисковете, потенциалните въздействия върху услугите и клиента, изискванията относно услугите, ползите за организацията, техническата осъществимост и финансовото въздействие.

Одобрените изменения трябва да бъдат разработени и проверени.

Трябва да бъде създаден и съобщен на заинтересованите страни график за измененията, съдържащ одобрените промени и предложените за тяхното разгръщане дати. Графикът за измененията трябва да бъде използван като основа за планиране и разгръщане на версии.

Действията, необходими за отмяна или поправка на неуспешно изменение, трябва да бъдат планирани и, където е възможно, проверени.

Изменението трябва да бъде отменено или поправено, ако е неуспешно. Неуспешните изменения трябва да бъдат разследвани и трябва да бъдат предприети съгласувани действия.

Записите в БДУК трябва да бъдат актуализирани след успешно разгръщане на изменение.

Доставчикът на услуги трябва да извършва преглед на измененията по отношение тяхната ефикасност и да предприема съгласувани със заинтересованите страни действия.

Заявките за изменения трябва да бъдат анализирани през планирани интервали, за да бъдат открити тенденциите. Резултатите и направените заключения от анализа трябва да бъдат записвани и разгледани за да се идентифицират възможностите за подобряване.

Управление на версията и разгръщането на услугата

Доставчикът на услуги трябва да установи и съгласува с клиента политика за версиите, излагаща честотата и вида на версиите.

Доставчикът на услуги трябва да планира с клиента и със заинтересованите страни разгръщането в естествена среда на нови или изменени услуги и компоненти на услуги. Планирането трябва да бъде координирано чрез процеса за управление на изменения и да включва връзка със свързаните заявки за изменение, известни грешки и проблеми, които се приключват чрез версията. Планирането трябва да включва датите за разгръщане на всяка версия, доставките и методите за разгръщане.

Доставчикът на услуги трябва да документира и договори с клиента дефиницията на спешна версия. Спешните версии трябва да бъдат управлявани съобразно документирана процедира, която има отношение към процедурата за спешни промени.

Версиите трябва да бъдат проверени преди разгръщането. За изграждане и проверка на версиите трябва да бъде използвана контролирана среда за приемане на версиите.

Критериите за приемане на версиите трябва да бъдат съгласувани с клиента и със заинтересованите страни. Версията трябва да бъде верифицирана спрямо съгласуваните критерии за приемане и одобрена преди разгръщането. Ако критериите за приемане не са спазени, доставчикът на услуги трябва да вземе решение със заинтересованите страни относно необходимите действия и разгръщане.

Версията трябва да бъде разгърната в естествена среда, така че да се запази целостта на хардуера, софтуера и на другите компоненти на услугата по време на разгръщането на версията.

Действията, необходими за отмяна или поправяне на неуспешно разгръщане на версия трябва да бъдат планирани, и където е възможно, подложени на изпитване. Ако е неуспешно, разгръщането на версията трябва да бъде отменено и поправено. Неуспешните версии трябва да бъдат разследвани и да бъдат предприети съгласувани действия.

Успешното или неуспешното въвеждане на версиите трябва да бъде наблюдавано и анализирано. Измерванията трябва да включват инциденти, свързани с версията, за период след разгръщане на версията. Анализът трябва да включва оценка на въздействието на версията върху клиента. Резултатите и заключенията от анализа трябва да бъдат записвани и прегледани, за да се идентифицират възможности за подобряване.

При процеса на управление на изменения и управление на инциденти и при заявки за услуги трябва да бъде предоставена информация относно успеха или неуспеха на версиите и за датите на бъдещи версии.

В процеса за управление на измененията трябва да бъде предоставена информация, за да се подпомогне при оценяването на въздействието на заявките за изменения върху версиите и плановете за разгръщане.

Следващите страници ще предоставим указания за прилагането на система за управление на услугата (СУУ). В тях не се добавят изисквания към по-рано споменатите, целта е да позволи на организациите и отделни лица да тълкуват ISO/IEC 20000 по-точно и по този начин да го ползват по-ефикасно.

Ръководство за прилагане на ISO/IEC 20 000

Общи изисквания за системата за управление на услугите

Отговорност на ръководството

Ангажираност на ръководството - Отговорности на висшето ръководство

Висшето ръководство трябва да бъде ръководството, което направлява, наблюдава и контролира доставчика на услуги на най-високо ниво, то трябва да бъде наясно, че удовлетворяването на изискванията на ISO/IEC 20000-1 включва:

a) Демонстриране на неговата ангажираност да участва на всички етапи на СУУ, започвайки с планирането и създаването на СУУ и продължавайки с експлоатирането, наблюдението, измерването, прегледа, поддържането и непрекъснатото подобряване на СУУ;

b) Демонстриране на неговите правни и други отговорности за СУУ;

c) Осигуряване на увереност, че изискванията към услугата, обхвата на СУУ, политиката и целите на управление на услугата са разбрани и приети от всички заинтересувани страни на СУУ;

d) Осигуряване на увереност, че планът за управление на услугите е създаден, внедрен, поддържан и е в съответствие с целите на дейността;

e) Осигуряване на предоставянето на адекватни ресурси за изпълнение на целите на управление на услугите и за съответствие с политиката за управление на услугите;

f) Осигуряване на увереност, че характеристиките/резултатността на СУУ се докладват на нивото на висшето ръководство;

g) Постигане на целите на управлението на услугите, включително когато те се изменят поради изменение на потребностите на дейността или на изискванията към услугата;

h) Осигуряване на увереност, че рисковете за услугите са сведени до минимум, т.е. чрез оценяване на рисковете, свързани с изменения и предприемане на действия.

Висшето ръководство трябва и да гарантира, че всички етапи от жизнения цикъл на услугата са доставени на договорените нива, както е определено в изискванията към услугата. Жизненият цикъл на услугата включва планиране, внедряване, експлоатация, наблюдение, измерване, преглед, поддържане и непрекъснато подобряване. Жизненият цикъл включва и прехвърляне на услугата към клиент или различна страна или в крайна сметка прекратяване на услугата.

Висшето ръководство трябва да осъзнава, че носи правна отговорност за осигуряване на увереност, че СУУ и услугите, доставени от СУУ, са

оценени и прегледани. Оценките трябва да включват собствените прегледи и вътрешните одити на доставчика на услуги, както и външните одити.

Доказателства за ангажимента на висшето ръководство

Без ангажимент на ръководството е възможно взетите от ръководството решения да влязат в конфликт с изискванията за ефикасна СУУ. Примерите може да включват преразпределяне на ресурси към други проекти, липса на комуникация за СУУ и неразрешени конфликти при разработването на процеси.

Трябва да съществуват доказателства за ангажимента и отговорността на ръководството, които да са налични за преглед от оценител. Висшето ръководство трябва да бъде в състояние да предостави доказателства, основани на записи на участието си в:

a) Редовни срещи за СУУ, например председателство на планираните срещи, така че СУУ да остава в съответствие с потребностите на дейността и новите или изменени изисквания към услугата;

b) Осигуряването на това СУУ да включва определение на обхвата, политиката за управление на услугата, целите на управление на услугата и плана за управление на услугата;

c) Одобряването на политиката за управление на услугата, целите на управление на услугата и плана за управление на услугата;

d) Одобряването на процеси и процедури, които са в съответствие с политиките на СУУ и ги подкрепят.

Одобрението на висшето ръководство на плана за управление на услугата е важно, защото планът може да има влияние върху ангажимента към клиента, планирането на дейностите за поддоставчиците и разпределението на ресурсите за подобрения и други изменения.

Съответствието между политиките, процесите и процедурите позволява насоките на висшето ръководство да достигат до целия персонал на доставчика на услуги. Това осигурява съгласуваност на решенията на ръководството с начина, по който персоналът на доставчика работи всеки ден.

Комуникация на висшето ръководство

Висшето ръководство трябва да участва активно в текущата програма за комуникация. Съобщенията трябва да бъдат насочвани чрез одобрени процедури за комуникация.

Висшето ръководство трябва да участва активно в текущата програма за комуникация, за да обяснява как създадената СУУ се съгласува с целите на дейността и очакванията на клиента. Това е важно за успеха на СУУ, защото персоналът, който разбира целта и важността на СУУ, е по-малко вероятно да се противопоставя на промени поради страх или липса на познания. Съобщенията на висшето ръководство за СУУ могат да бъдат възможност за доставчика на услуги да мотивира своята собствена организация. В допълнение, оценяването на важността на СУУ от страна и на

ръководството, и на персонала трябва да намали риска или вероятността да бъдат вземани решения или да бъдат разрешавани въпроси, които са в противоречие със СУУ.

Програмата за комуникация трябва да обяснява следното:

a) Организационните изменения, политиките, стандартите, вижданията и мисията, както и целите на дейността;

b) Потребностите на дейността, например отношението между СУУ и доставяните услуги, както и как тези услуги подпомагат определените цели и насоки на организацията;

c) Как създадената СУУ се съгласува с целите на дейността и очакванията на клиента;

d) Как политиката за управление на услугата, целите на управление на услугата и планът за управление на услугата подпомагат изпълнението на изискванията към услугата;

e) Изискванията на клиента, например целите на услугата, предвидения капацитет въз основа на предвижданите потребности, сигурността на информацията и непрекъснатостта на услугата, за да подкрепят непрекъснатостта на дейността;

f) Законовите изисквания, като например работно време, здраве и безопасност и защита на данните, които са различни в различните държави;

g) Нормативните изисквания, например записите да бъдат поддържани за определен период от време;

h) Договорните изисквания, например изискване за подписване на споразумение за не разкриване преди правото на достъп до информацията на доставчика на услуги;

i) Документираните споразумения с клиента;

j) Редовния анализ на данните, събрани чрез измерване на СУУ и компонентите й, например измервания на процеси.

В допълнение, комуникациите могат да бъдат възможност за доставчика на услуги да мотивира собствената си организация.

Програмата за комуникация е важна за успеха на СУУ, защото персоналът, който разбира целта и важността на СУУ, е по-малко вероятно да се противопоставя на промени поради страх или липса на познания. Комуникациите трябва да генерират оценяване на важността на СУУ както от ръководството, така и от персонала и да намалят риска или вероятността да бъдат вземани решения или да бъдат разрешавани проблеми, които са в противоречие със СУУ.

Резултатът от тези дейности за комуникация трябва да бъде, че хората разбират своите роли в управлението на услугата и това, как те допринасят за изпълняването на изискванията към услугата и постигането на целите на управлението на услугата.

Цели на управлението на услугата

Висшето ръководство трябва да определи съгласуваните цели за

управление на услугата. Целите трябва да бъдат в съответствие с целите на дейността и с политиката за управление на услугата.
Например основните цели на управление на услугата могат да включват следното:

a) Да позволяват повишена бързина/подвижност на дейността чрез по-бързо доставяне на нови или изменени услуги;

b) Да намаляват непланираната неналичност на критични за дейността услуги;

c) Да оптимизират цената на доставяните услуги чрез ефективност на функционирането;

d) Да увеличават качеството на услугите и намаляването на риска.

Действителните цели на управлението на услугите трябва да бъдат определени така, че да бъдат измервани точно постиженията спрямо целите. Измерването трябва също да позволява възможностите за подобряване да бъдат подреждани по приоритет.
Целите трябва да бъдат ключови входни данни за плана за управление на услугите. Планът трябва да идентифицира действията за постигане на целите и съгласуване с други компоненти на СУУ.
Целите на управление на услугите трябва да бъдат подлагани на преглед на редовни периоди от време, за да може висшето ръководство да реши как и кога те да бъдат преработени.
Доставчикът на услуги трябва да гарантира, че ефикасността на всеки компонент на СУУ е измерена, за да се оцени ефикасността на подкрепата за целите на управление на услугите. Например измерването на ефикасността на подкрепата за целите от конкретен процес. Измерванията трябва да демонстрират и стойността на СУУ в подпомагането на целите на дейността.
Доставчикът на услуги може да сметне за полезно да измерва приносите на отделните лица за постигане на целите. Това ще улесни персонала в подпомагането на СУУ да работи по интегриран начин за същите цели.
План за управление на услугите

Планът за управление на услугите трябва да улеснява координирането на всички начинания на СУУ, за да осигури постигането на целите на управление на услугите. Планът и политиките също трябва да бъдат в съответствие.
Планът може да бъде мощен механизъм за видимост и контрол от край до край. Той трябва и да предотвратява одобряването или прилагането на несъвместими начинания. Планът трябва да позволява оползотворяването на ресурси и способности, за да бъдат възможно най-ефикасни и ефективни.
Планът трябва да бъде съобщен на всички заинтересувани страни. Това трябва да осигури общо разбиране на обхвата на начинанията, задачите, сроковете и разпределените отговорности. Разпределените отговорности трябва да бъдат включени в измерванията на резултатността на всеки

участник в СУУ, включително тези, които участват в начинания по плана за управление на услугите.
Планът не трябва да се смята за изпълнен, когато бъде внедрена СУУ. Той трябва да съществува неограничено, като се променя така, че да отговаря на променящите се потребности на дейността, изискванията на клиента или приоритетите на доставчика на услуги.
Планът за управление на услугите може да се състои от един-единствен план или програма от координирани промени, управлявани централно, с някои локално прилагани промени.
Доставчикът на услуги трябва винаги да бъде информиран за необходимостта да поддържа всички промени да бъдат локално приложени под общото ръководство на плана за управление на услугите. Например подобряването на процес може да бъде извършено локално, под локалния контрол на собственика на процеса, но той е включен в централно управляваната обща програма.
Плановете за определена цел, например за непрекъснатост на услугата и процеса за управление на наличността, могат да бъдат позовавани по-скоро от общия план за управление на услугите, отколкото да бъдат включени в него. Плановете за специалисти и тяхното съгласуване с общия план трябва да бъдат подлагани на преглед с честота, която е подходяща за темпа на измененията. Това трябва да бъде поне веднъж годишно.
Всички промени, произтичащи от прегледите или от промяната на изискванията към услугата, или индивидуалните планове, трябва да бъдат документирани в общия план за управление на услугите. Например промяна на работното време към работа на пълни 24 часа, технология на замяна или промени в уменията.
Съдържанието на плана за управление на услугите трябва да включва:

a) Въведение;
b) Описание на функциите на организацията на доставчика на услуги;
c) Приоритети на начинанията;
d) Очаквани резултати в съответствие с целите на дейността;
e) Мерки за характеристиките/резултатността;
f) Цели на услугата;
g) Проектни планове;
h) Задачи и зависимости;
i) Реализация на ползите, постигнати като резултат от предишни приложени подобрения;
j) Срокове и лица, отговорни за провеждането на начинанията от плана;
k) Рискове и възможности за смекчаване на рисковете.

Рисковете за плана за управление на услугите трябва да бъдат идентифицирани, оценени и управлявани както първоначално, така и като част от методологията ПИПД. Оценяването на риска трябва да обхваща

входните данни, изходните резултати, дейностите и отговорността и отчетността за смекчаване на рисковете. Планът трябва да бъде направен така, че да осигурява постигането на договорените цели и изисквания към услугата.

Ресурси, които подпомагат плана за управление на услугите

Ресурсите, необходими за постигане на целите на управлението на услугите, трябва да бъдат документирани в плана за управление на услугите. Трябва да бъде взето предвид следното:

a) Управлението на човешките ресурси трябва да взема под внимание уменията и опита на лицата, а не просто да се основава само на броя на хората;

b) Техническите ресурси, например инфраструктурата и капацитета за постигане на изискваните характеристики/резултатност;

c) Инструменти, които подпомагат процесите в СУУ;

d) Настаняването в офисите, други съоръжения и съоръжения за непрекъснатост на услугата;

e) Данните и информацията, например подробности за изискванията на клиента, плановете за дейността на клиента, потребностите на дейността на доставчика на услуги, политиките за управление на услугите, измерванията на характеристиките/резултатността и други доклади;

f) Финансовите ресурси, бюджетирани на ниво на подробностите, подходящо за управление на планирането, внедряването, функционирането и подобряването на СУУ;

g) Количеството и наличността на персонала на доставчика на услуги и изработени от него часове;

h) Процесите, процедурите и разполагането във времето за планиране на въвеждането, запазването и последователността на подходящия по умения персонал.

Съдържание на изискванията за услугата

Висшето ръководство трябва да носи отговорност за осигуряване на изпълнението на договорените изисквания за услугата в доставяната услуга. И изискванията на клиента, и потребностите на дейността трябва да бъдат документирани, наблюдавани, преглеждани и управлявани, за да се осигури непрекъснато съответствие с новите или изменени услуги, както и с услугите в естествената среда.

Изискванията за услугата трябва да включват изискваните цели на услугата и очакванията за качеството й. Потребностите на доставчика на услуги трябва да включват подробности за изискванията към ресурсите и способностите. Изискванията за услугата са входни данни за СУУ.

Примерите за изисквания за услугата могат да включват:

a) Услуга в процес на използване, включително изисквания към нивото на услугата;

b) Критерии за качество за разработването на нови или изменени

услуги;

c) Приоритети за критичността за дейността на услугите;

d) Изисквания за наличност;

e) Нормативни изисквания;

f) Изисквания за сигурността на информацията.

Роля на висшето ръководство при съгласуване и изпълняване на изискванията за услугата

Висшето ръководство трябва да гарантира, че изискванията за услугата са определени от гледна точка на:

a) Желаните резултати, които клиентите очакват, например подобрена ефикасност, ефективност, удовлетвореност;

b) Ограниченията, които услугата ще премахне;

c) Функционалността на услугата от гледна точка на клиента, включително потребностите на потребителите на услугата, често определяни като „подходящ за целта";

d) Модели на дейността и потребност, която услугата трябва да поддържа;

e) Гарантиране, че услугата и продуктите ще бъдат доставени или ще отговарят на определени договорени спецификации, често определяни като гаранция.

Типична характеристика на гаранцията е, че тя е дефинирана от гледна точка на непрекъснатостта на услугата, наличността, капацитета и сигурността. Например гаранцията гарантира, че услугата ще остане съответна на целта дори при намалени нива на услугата, дължащи се на големи прекъсвания или бедствия. Гаранцията трябва да осигури и сигурност за услугите.

Потребностите на потребителите на услугите трябва да бъдат определени в контекста на потребностите на клиента - това трябва да описва ползата, която ще има потребителят от използването на услугата като част от изпълнението на служебните си дейности. По-долу са дадени примери.

ПРИМЕР 1: Премахване на ограниченията. Желано изменение на услугата може да позволи на потребителите да имат достъп до услугата от разстояние, вместо само от определени места.

ПРИМЕР 2: Функционалност. Желано подобрение във времето за обработване за бизнес транзакциите.

ПРИМЕР 3: Характеристики/резултатност. Може да е необходимо потребителят да обработи една транзакция за доставка в минута и 50 транзакции за час.

Потребности на доставчика на услуги

От гледна точка на доставчика на услуги изискванията към услугата трябва да включват тези, изброени по- долу.

a) Изисквания, които осигуряват удовлетворяването на потребностите на дейността и по-широки интереси на организацията, която

притежава организацията на доставчика на услуги. Например изискванията да се изпълняват политиките, стандартите, законовите и нормативните изисквания и договорните задължения.

b) Обхват на СУУ да ръководи, наблюдава и контролира интегриран набор от процеси и дейности за управление на услугите. Това включва изискванията за активите, способностите и ресурсите, изисквани за разработването, прехода, доставянето и подобряването на услугите. Например организационни звена, хора, процеси, информация и технологии, изискващи се за поддържането на СУУ.

c) Известни ограничения на СУУ, например човешки, технически, информационни ограничения и ограничения на финансовите ресурси.

d) Изисквания за измерване, одитиране, докладване и подобряване на доставяната услуга спрямо определените цели на дейността.

e) Изисквания за измерване, одитиране, докладване и подобряване на ефикасността на СУУ.

Противоречиви изисквания

Ако доставчикът на услуги установи, че е възникнало противоречие в изискванията, трябва да бъде предприето действие. Примерите за противоречия в изискванията включват следното.

a) Ако съществуват противоречия между изискванията на клиента и потребностите на дейността на клиента, противоречието трябва да бъде разрешено от клиента, например изискване на клиента, което е в противоречие със стратегическата насока на дейността. Обратно, доставчикът на услуги може да анализира разликите и да предложи преразгледани изисквания към услугата.

b) Могат да възникнат противоречия между изискванията на клиента и собствените потребности на дейността на доставчика на услуги, когато изискванията на клиента са нереалистични от гледна точка на приоритетите, цените и наличните средства. Същността на противоречието и защо изискванията са нереалистични трябва да бъдат ясно съобщени на клиента.

c) Трябва да бъдат разрешени, противоречията на законови или нормативни изисквания, или договорни задължения в изискванията за услугата. Например разпространението на софтуера може да бъде ограничено чрез лицензионно споразумение по начин, който е несъвместим с изискванията на клиента за достъп до нови версии на софтуера.

Доставчикът на услуги трябва да гарантира, че всякакви рискове, възникващи от противоречията, са оценени и количествено определени, така че да се идентифицират методите за минимизиране на рисковете. Оценката трябва да включва риска за удовлетвореността на клиента и способността да се удовлетворят изискванията и целите на клиента.

Противоречията и тяхното потенциално въздействие трябва да бъдат документирани и обсъдени с клиента, така че да може да бъдат разрешени.

Ако дадено противоречие е идентифицирано, след като бъде съгласувано разработването на услугата, противоречието трябва да бъде разрешено като коригиращо действие или като възможност за подобряване.

Рискове за услугата

Висшето ръководство трябва да гарантира, че рисковете за СУУ и услугите са идентифицирани, документирани и оценени. Рисковете за услугата може да включват неспособност да се изпълнят законови и нормативни изисквания или договорни задължения. Например неспособност да се изпълнят лицензионните изисквания за софтуера или неспособност да се предостави доказателство за финансова почтеност.

Висшето ръководство трябва да гарантира също, че всички идентифицирани рискове са управлявани, включително гарантирайки, че:

a) Са разработени и документирани възможности за управление на идентифицираните рискове;

b) Предпочитаните възможности са съгласувани с клиента;

c) Договорените възможности за смекчаване на риска са приложени, когато това е необходимо.

Политика за управление на услуги - Указания за политиката за управление на услуги

Политиката за управление на услуги трябва да бъде конкретна за условията на доставчика на услуги и да е насочена към клиента. Политиката не трябва да бъде общо, широко приложимо изявление. Вместо това политиката трябва да отразява положението и целите на доставчика на услуги.

Политиката трябва да представлява насоката и ангажимента на висшето ръководство да изпълнява изискванията към услугата.

Политиката трябва да дава ясно направление на висшето ръководство към ръководителите и персонала на доставчика на услуги.

ПРИМЕР 1: Услугите са в съответствие с целите на дейността на клиента.

ПРИМЕР 2: Измененията на процесите или процедурите се правят само чрез процеса на управление на промените.

ПРИМЕР 3: Ролите и отговорностите за процесите на управление на услуги са определени и документирани по последователен начин и резултатността на персонала се измерва спрямо постигането на тези отговорности.

Политиката за управление на услуги трябва да бъде структурирана така, че да може да бъде използвана за оценяване дали целите на управление на услугата на доставчика на услуги се изпълняват. Например трябва да бъде възможно да се демонстрира връзка между политиката за управление на услуги и това, което е направено за постигане на целите на управление на услугата на доставчика на услуги. Политиката за управление на услуги трябва да бъде структурирана така, че да осигурява измерване на спазването на политиката.

Доставчикът на услуги трябва да бъде в състояние и да демонстрира, че тази

връзка между целите на доставчика на услуги и политиката за управление на услуги е ефикасна, така както политиката за управление на услуги е съгласувана първоначално.
Политиката за управление на услуги трябва ясно да определя нивата на пълномощия, например да прави възможно определянето на това, дали начинание за подобряване трябва да бъде одобрено от собственик на отделен процес или от висшето ръководство.
Политиката за управление на услуги трябва да бъде съобщена и разбрана в организацията на доставчика на услуги. Политиката за управление на услуги може да бъде направена достъпна и за клиента, и поддоставчиците, ако се изисква. Позоваванията на политиката, която се обсъжда, разбира и използва по подходящ начин, може да бъдат използвани като доказателство за изпълнение на това изискване. Например протоколи от срещите, прегледи на персонала, договори с доставчика, споразумения с поддоставчик, заявки за изменение в политиката или заявки за пояснение, въздействие на политиката върху процеси, процедури и поведение по време на стандартни и непланирани операции, прегледи на клиента, прегледи на доставчика.
Висшето ръководство трябва да бъде отговорно и за осигуряване на прегледи на политиката за управление на услуги на подходящи интервали, поне веднъж годишно. Това трябва да идентифицира всякакви недостатъци и да осигури непрекъснато съгласуване с потребностите на дейността и изискванията на клиента. В критериите за качество, приложени по време на прегледа на политиката за управление на услуги, трябва да се вземе под внимание следното:

a) Валидността на политиката спрямо изискванията към услугата;

b) Адекватността на честотата на прегледа;

c) Съответствието между политиката и целите на управление на услугите;

d) Съответствието между политиката и плана за управление на услугите;

e) Съответствието между политиката и процесите за управление на услугите;

f) Дали прегледът е документиран, одобрен, проследен, подходящ и практичен;

g) Адекватността на рамката за създаване, внедряване, експлоатация, наблюдение, преглед, поддържане и подобряване на СУУ;

h) Действията за коригиране и подобряване, идентифицирани при предишни прегледи и одити на СУУ.

Подобрения и други изменения на политиката

Ако бъде открит недостатък след преглед на политиката за

управление на услуги, висшето ръководство трябва да гарантира, че той е коригиран. Недостатъците трябва да бъдат коригирани или като изменение на политиката, целите на управление на услугите, плана, процесите, или изменение на процедурите.

Политиката трябва и да бъде актуализирана, за да отразява всяко изменение на целите на управление на услугите или на обхвата на СУУ.

Пълномощия, отговорност и комуникация - Пълномощия и отговорности

Доставчикът на услуги трябва да гарантира, че пълномощията и отговорностите за всички аспекти на СУУ са определени. Описанията на ролите трябва да бъдат съгласувани, разпределени на отделните лица, съобщени на целия персонал и поддържани в актуално състояние чрез процедура за управление на документите. Доставчикът на услуги трябва да гарантира, че целият персонал е насърчен да създава и поддържа информираност за това, как неговите дейности допринасят за постигането на целите на управление на услугите.

Процедури за комуникация

Висшето ръководство трябва да бъде отговорно за гарантиране, че са разработени, прехвърлени, внедрени и използвани процедури за комуникация. Висшето ръководство може да делегира действителното разработване на процедурите. То обаче трябва да ги одобрява, преди да бъдат приложени, и да налага тяхното използване. Висшето ръководство трябва да участва активно в процедурите за комуникация.

Висшето ръководство трябва да разбира ценността на информираността, мотивацията и участието на персонала в ефикасното управление на услугите и непрекъснатото им подобряване. Процедурите за комуникация трябва да насърчават мотивацията на персонала. Например съобщаването на успешни резултати от участието на персонала в дейностите за подобряване може да има значителен мотивиращ ефект.

Процедурите за комуникация трябва да обхващат най-малко метода за доставка, времето и/или честотата и аудиторията. Процедурите трябва да обхващат и механизмите за отнасяне до по-горно управленско ниво, подробности за контакт, поддържане на списък за разпространение, методи за комуникация, достъп до инструменти и информация, графици и отговорности.

Процедурите за комуникация трябва да включват следното:

a) Метода за доставка;

b) Времето и честотата;

c) Аудиторията за определени комуникации;

d) Механизми за отнасяне до по-горно управленско ниво;

e) Подробности за контакт за аудиторията на комуникацията;

f) Поддържане на списък за разпространение;

g) Методи за комуникация;

h) Достъп до инструменти и информация;

i) Графици и отговорности.

Комуникацията може да приеме различни форми и зависи от културата или от организацията, лицето, с което се комуникира, и ролята на това лице в организацията.

Методите за комуникация на висшето ръководство може да включват материал за ориентацията на персонала, кратки пресконференции и работни конференции, вътрешни публикации на персонала, електронна поща, обществени средства за информация или форуми за обратна връзка с персонала.

Представител на ръководството - Разбиране на отговорностите

Представителят на ръководството трябва да бъде член на управляващия екип на доставчика на услуги, който има правомощие да гарантира, че СУУ е създадена, използвана, подобрявана във времето и е в съответствие с променящите се потребности на дейността. Правомощието трябва да включва гарантиране, че процесите за управление на услугите имат подходящи интерфейси помежду си и че са интегрирани с останалата част от СУУ.

Доставчикът на услуги трябва да гарантира, че е ясно кое лице е представител на ръководството и че отговорностите на представителя на ръководството и нивата на правомощие се разбират от:

a) Собствениците на процеси, които имат правомощие и отговорност за гарантиране, че процесът, неговите интерфейси към други процеси и интегрирането им в СУУ са документирани, спазвани, измервани и подобрявани;

b) Собствениците на услуги, които имат правомощие и отговорност за дадена услуга през нейния жизнен цикъл, включително разработване, прехвърляне, внедряване, подобряване и прекратяване;

c) Друг персонал на доставчика на услуги;

d) Вътрешните групи;

e) Поддоставчиците, включително водещи поддоставчици;

f) Клиента.

Отговорности

Представителят на ръководството трябва да отговаря за гарантиране, че е постигнато следното:

a) Изпълняват се всички аспекти на отговорностите на ръководството, определени в ISO/IEC 20000-1, включително тези, изисквани от висшето ръководство;

b) Документирани са изискванията към услугата;

c) СУУ и определянето на обхвата удовлетворяват собствените потребности на доставчика на услуги, потребностите на клиента и потребителите на услугите;

d) Обхватът и подробностите на СУУ се проверяват на подходящи интервали, за да се гарантира, че изискванията към услугите продължават

да се изпълняват, например ако потребностите на клиента се променят, е възможно СУУ или обхватът на СУУ също да имат нужда от промяна;

e) Политиката и целите на управление на услугите се използват като основа за вземане на решения по време на първоначалното планиране на процесите до разработването на процесите и функционирането и подобряването на процесите;

f) Разработването на процесите започва с идентифициране на входните данни и изходните резултати и на всички дейности, изпълнявани като част от процесите;

g) Политиката и целите диктуват критериите за подреждане по приоритет на подобренията на процесите за управление на услугите;

h) Процесите за управление на услуги имат подходящи и ефикасни интерфейси помежду си и са интегрирани с останалата част на СУУ;

i) Методологията ПИПД е внедрена и се използва за непрекъснато подобряване на СУУ и услугите;

j) Провеждат се вътрешни одити и оценки на СУУ на редовни интервали, за да се измерва способността на СУУ да постига целите на управление на услугите и да изпълнява изискванията към услугата.

Управление на активи

Висшето ръководство трябва да бъде наясно, че ISO/IEC 20000-1 изисква всички активи, които се използват за доставяне на услуги, да се управляват според съответните законови, нормативни и финансови изисквания и договорни задължения. Активите трябва да бъдат управлявани от ефикасни процедури.

Примерите за активи, които трябва да бъдат управлявани, включват софтуерни лицензи, мобилни устройства, компоненти на инфраструктурата, хора, договори, процедури и други документи. Доставчиците на услуги трябва да са в състояние точно да идентифицират местоположението, състоянието и други съответни подробности за активите.

Висшето ръководство трябва да бъде наясно, че управлението на активи изисква да бъде създадена и ефикасно използвана точна база данни за управление на конфигурацията (БДУК) или еквивалентни средства за поддържане на записи. Информацията в БДУК трябва да бъде поддържана в актуално състояние чрез ефикасни процеси за управление на услугите, например измененията на БДУК да бъдат одобрявани чрез процес за управление на измененията.

Законовите изисквания може да включват закони за защита на личната информация и данни, както и закони за защита на интелектуалната собственост и авторските права. Други законови изисквания може да се отнасят към защитата на информационните активи на клиента или защитата на финансова информация.

Нормативните изисквания и договорните задължения може да включват

гарантиране, че активите съответстват на лицензионните изисквания към дейността и стандартите, например стандарти за сигурност за кодиране на чувствителна информация на преносими компютри.
Докладване от представителя на ръководството

Докладите трябва да идентифицират възможностите за непрекъснато подобряване, постигани с използването на методологията ПИПД. Това трябва да се основава на доклади за характеристиките/резултатността на СУУ и услугите.
Честотата и нивото на подробност на докладите трябва да бъдат съответни на нивото на дейността, категориите на изменение и сериозността на всеки проблем и риск, идентифицирани от представителя на ръководството. Трябва да бъдат предоставени възможности за изменения за коригиране на недостатъците, за да се подпомогне подреждането по приоритети на действията и последващото взето решение от висшето ръководство.
Докладите до висшето ръководство трябва ясно да описват доставяната от СУУ стойност в подкрепа на целите на дейността.

Ръководене на процесите, обслужвани от други страни - Указания за процесите, обслужвани от други страни

Доставчикът на услуги трябва да бъде наясно, че може да изпълнява изискванията на ISO/IEC 20000-1 чрез демонстриране на ръководене на процесите, обслужвани от друга страна, за малка част от процесите.
Доставчикът на услуги трябва да бъде в състояние да идентифицира всички процеси или част от процесите за управление на услуги, които се обслужват от други страни. Доставчикът на услуги трябва да има видимост от край до край за резултатността на другите страни.
Доставчикът на услуги трябва да бъде в състояние да демонстрира контрол върху всички страни, обслужващи процеси в СУУ, и това трябва да бъде подкрепено от всички договори и други документирани споразумения.
Други страни, другите страни включват:

a) Вътрешни групи, които са организационни звена в същата организация като тази на доставчика на услуги, но не са под прекия контрол на доставчика на услуги, например екип на център за данни или специалисти по сигурност;

b) Клиент, действащ като поддоставчик, например клиентът изпълнява някои от дейностите при управление на инцидент и заявка за услуга;

c) Поддоставчици, например прехвърляне към външен изпълнител на изпитването, извършвано като част от процеса за управление на пускането и разгръщането на услуга.

Поддоставчиците могат да бъдат и водещи поддоставчици с отговорности за управлението на поддоставчици.
Демонстриране на отговорност и пълномощия

Доставчикът на услуги трябва да демонстрира отговорност и пълномощия за процесите, като предоставя доказателства като описаните по-долу:

a) Отговорността на доставчика на услуги за ефикасността на процесите за управление на услуги, обслужвани от доставчика на услуги или друга страна, например матрицата на лицата, които вземат решения, доказателство за нивата на упълномощаване в собствената организация на доставчика на услуги.

b) Доказателство, че доставчикът на услуги има властта да изисква съответствие с даден процес. Например, като създава политика за сигурност на информацията, като използва механизми за контрол, като открива нарушения и започва коригиращи действия. Друг пример включва предоставяне на доказателства, че практиките се променят при заявка от страна на доставчика на услуги.

c) Анализ на записите на процеси, включително измервания от страна на доставчика на услуги. Например разглеждане на пълен набор от записи на инциденти или на доклад за инцидент и вземане на решения въз основа на съдържанието дори когато записите на инциденти са предоставени от друга страна, която обслужва процеса за управление на инциденти.

d) Контролиране на определението на всички процеси в СУУ, обслужвани от други страни. Това включва интерфейсите между всички процеси. Например документиране, съгласуване и експлоатиране на интерфейсите и зависимостите на процеса на управление на промените с процеса на управление на конфигурацията.

e) Контролиране на планирането и поставянето на приоритети за подобренията на всички процеси в точки от 4 до 9 на ISO/IEC 20000-1:2011. Например оценяване и подреждане по приоритет на подобрението в процеса на управление на капацитета дори ако процесът е обслужван от друга страна.

Доставчикът на услуги може да изисква други страни да обслужват процесите, разработени и документирани от доставчика на услуги. Обратно, доставчикът на услуги може да одобри процесите, които другите страни разработват, документират и обслужват.

Доставчикът на услуги трябва да бъде наясно, че ако разчита на други страни за обслужването на повечето от своите процеси, не е вероятно да е възможно той да демонстрира адекватно ръководене на процесите.

Резултатност и съответствие на процеси

Ръководенето на процеси, обслужвани от други страни, трябва да включва определение на процеса, включително:

a) Идентифициране на собствеността на процес, например коя група или ръководител в организацията на доставчика на услуги е отговорна за процеса;

b) Отговорност за функционирането, например коя група или

ръководител е отговорен за функционирането на процеса;

c) Целта на процеса, резултатите от процеса и приноса към изискванията за услугата и постиганите цели на управлението на услуги;

d) Входни данни и изходни резултати на процеса и коя страна ги генерира;

e) Определение на интерфейсите към други процеси, включително процеси на управление на услуги, например данни, предавани между процесите или прехвърляне на дейности или информация от една страна на друга;

f) Определение на интерфейсите между процесите и други компоненти на СУУ, например между процесите и политиката и целите на управление на услуги;

g) Честотата и метода, чрез които информацията преминава към и от всеки процес;

h) Документите и записите, които се изискват от доставчика на услуги за ръководене на процесите, обслужвани от други страни, и кой ги генерира;

i) Ясна отчетност и отговорности за всички изисквани дейности.

Определението на интерфейсите между компонентите на СУУ трябва да включва методите, чрез които се създават и непрекъснато подобряват процесите за управление на услуги, за да подпомагат политиката и целите на управление на услуги и променящите се потребности на дейността. Например как трябва да бъдат измервани компонентите на СУУ, включително процесите, спрямо тяхното съответствие на политиката за управление на услуги и нейното подпомагане.

Определяне на резултатността и съответствието на процесите

Доставчикът на услуги трябва да гарантира, че всички процеси са ефикасни чрез:

a) Документиране и споразумяване с другите страни за честотата и формата на документите и записите, които ще бъдат достъпни за доставчика на услуги и за другите страни;

b) Създаване на цикъл и критерии за преглед за оценките на процеси;

c) Провеждане на оценяване на процесите спрямо изискванията на ISO/IEC 20000-1;

d) Определяне на задълженията на другите страни в рамките на дейността за преглед на процесите;

e) Анализ на резултатността/характеристиките на процесите;

f) Анализ на интерфейсите между процесите или частите на процеси, обслужвани от други страни и други процеси, както и политиките и плановете;

g) Анализ и съгласуване между процесите или частите на процеси, обслужвани от други страни, и целите на управление на услуги;

h) Поставяне на приоритети и планиране на дейностите за подобряване или корекции за оптимизиране на процесите.

Контролиране на планирането и подреждане по приоритет на подобренията на процеси

Доставчикът на услуги трябва да бъде в състояние да демонстрира, че контролира приоритета, даден на подобренията на всички процеси, включително тези, обслужвани от други страни.

ПРИМЕР 1: Предложено подобрение на процеса за управление на промените може да бъде смятано, че има по-голяма полза за организацията от предложено подобрение на процеса за управление на пускането и разгръщането. Подреждането по приоритет на подобренията на процеси трябва да бъде съгласувано с целите на дейността и изискванията към услугата.

ПРИМЕР 2: Подобрение на процеса за управление на инциденти, обслужван от друга страна, трябва да се ръководи от целите на дейността и изискванията към услугата на доставчика на услуги и неговата организация.

Управление на документацията

Създаване и поддържане на документи - Документите като доказателство

Доставчикът на услуги трябва да гарантира, че са налични доказателства за всеки одит на СУУ. Повечето от доказателствата трябва да съществуват под формата на документи. Документите могат да бъдат от всякакъв тип, форма или носител, подходящ за тяхната цел, например хартиени, електронни файлове, в база данни или процесор на думи.

Следните документи може да бъдат смятани за доказателство за одит на СУУ:

a) Политики, цели и планове за управление на услугите;

b) Документи за процес и процедура;

c) Каталог на услугите;

d) Документи на услугите, включително разработки, спецификации на изискванията, споразумения за нивото на услугата (СНУ), критерии за одобряване и прегледи на услугата;

e) Договорни документи, включително спецификация на изискванията и контрол на измененията;

f) Дейности и доклади за планиране на одита;

g) Документи, описващи или свързани с конкретно изменение, като дейности за планиране на измененията.

Доставчикът на услуги трябва да бъде наясно, че някои документи, като политиките, се изискват от ISO/IEC 20000-1, за да се изпълнят изискванията на определени процеси. В допълнение, организацията може да желае да вземе под внимание допълнителни документи, включително политики, за да предоставят допълнителна яснота или да гарантират ефикасна експлоатация или подобрение на СУУ и доставяне на услугите.

Записите са особен тип документи и трябва също да бъдат налични като доказателство.

Издаване на документи, включително записи

Доставчикът на услуги трябва да разбира, че ефикасната процедура е съществена за издаването на документи, включително записи. Това включва използването на система за именуване и номериране, която е в съответствие с целта и историята на преработването на документи. Използването на шаблони и стандартизиран формат може да намали усилието за създаване, оценяване, обновяване и използване на съдържанието.

Трябва да съществуват доказателства на процедура за одобряване на документи в съответствие с ролите и отговорностите за документите , определени в СУУ.

Доставчикът на услуги трябва да разбира, че документи като споразумение за ниво на услуга (СНУ), политики и планове може да бъдат взаимно зависими, например политика за сигурност на информацията, която определя каква информация може да бъде съхранявана на мобилни устройства или сървър, който подпомага доставянето на услугата електронна поща. Тези взаимни зависимости трябва да бъдат разбирани и управлявани, когато се правят изменения на документите.

Записи, които показват какво е направено в действителност или какво се е случило, не винаги изискват процедура за одобряване, например запис на инцидент. Записът на инцидент трябва да бъде обновяван, когато инцидентът се обработва за приключване. Да се обработва процедура за одобряване всеки път, когато се обновява записът на инцидента, причинява недопустими закъснения в разрешаването на инциденти .

Контрол на документите

Контролът на документите трябва да бъде признат като съществен. Контролът на документите трябва да включва периодичен преглед с обновяване или архивиране, ако е необходимо. Прегледът трябва да бъде поне ежегоден. Документите трябва да бъдат защитени от повреждане, например поради лоши условия на обкръжаващата среда и повреда на хардуера.

Контролът може да предостави видимост на въздействията на измененията, например изменение на СНУ, което въздейства върху договорите с други страни или изискванията за наличност.

Доставчикът на услуги трябва да гарантира, че документите са контролирани чрез използването на:

a) Именуване и номериране на версията;

b) Присвоена отговорност за написването, редактирането, прегледа, одобряването, обновяването, унищожаването и архивирането на документи;

c) Записи на измененията, които показват датата, автора, одобрението на изменението и същността на поправките;

d) Оценяване на измененията на идентифицирани документи чрез

процеса на управление на промените преди одобряване;

e) Идентифициране на отношенията между определени документи и други компоненти на СУУ;

f) Механизми за контрол на достъпа до документи и разпространение на документи;

g) Процедура за одобряване на документи за употреба;

h) Процедура за преглед и обновяване, ако е необходимо, и повторно одобряване на документи;

i) Процедура за гарантиране, че документите от външен за доставчика на услуги произход, които ще бъдат необходими за планирането и функционирането на СУУ, са идентифицирани и тяхното разпространение се контролира;

j) Процедура за гарантиране, че документите са унищожени в съответствие с политиката за сигурност на информацията и нормативните и законовите изисквания;

k) Процедура за архивиране на излезли от употреба документи.

За постигане на контрол на документите може да се използват техники от управлението на документи, управлението на знания, управлението на измененията и управлението на конфигурацията, например политика за това, как се показват версиите на документ.

Доставчикът на услуги трябва да идентифицира документите, които са предмет на процедури за контрол на документите. Това може да включва документи от външен произход като стандарти, нормативни документи или документи на клиента. Доставчикът на услуги трябва да разграничи различните видове контрол, които се прилагат към различните видове елементи, например между тези от вътрешен и външен произход или документи, изискващи различна сигурност поради различното си съдържание.

Много документи се категоризират като елементи на конфигурацията (ЕК), които поради това също се контролират чрез процеса на управление на конфигурацията. Там, където контролът на документите се постига чрез електронни средства, трябва да се обърне особено внимание на съответните процедури за одобряване, достъп, разпространение, (избор на) носител и архивиране.

Контрол на записите

Записите, свързани със СУУ, трябва да бъдат в съответствие с изискванията на ISO/IEC 20000-1, законовите и нормативните изисквания и договорните задължения. Например запаметяването на записи, практиките на архивиране и унищожаване. Записите, които трябва да бъдат запаметявани, включват записа на прегледите на документи и проследяването на коментарите от прегледа до решаването. Тези изисквания и задължения трябва да влияят върху разработването на СУУ.

Всякакви противоречия между законовите и нормативните изисквания или

договорните задължения и изискванията на ISO/IEC 20000-1 трябва да бъдат разрешени. Това трябва да се отнася за всички записи, които са създадени и използвани като част от СУУ. Това включва, но не се ограничава с документацията, регистрите/дневниците и записите в бази данни, записите на известни грешки, ЕК, записите на инциденти и заявка за записи на изменения.

Записите, създадени да предоставят доказателство за съвместимост с изискванията и за ефикасната експлоатация на СУУ, трябва да бъдат контролирани. Организацията трябва да създаде документирана процедура за определяне на механизмите за контрол, необходими за идентифициране, съхраняване, защита, запаметяване, запазване и унищожаване на записи. Записите трябва да бъдат четливи и да позволяват лесно идентифициране и възстановяване.

Управление на ресурси

Осигуряване на ресурси - Ресурси за внедряване на СУУ

Доставчикът на услуги трябва да осигури наличието на всички ресурси, съгласувани в плана за създаване, внедряване, поддържане и подобряване на СУУ и съгласуваните услуги. Ресурсите включват поне следното:

a) Човешките ресурси, например хора, които да разработят, внедрят и експлоатират СУУ, висшето ръководство и персонала, участващ в управлението на СУУ и услугите;

b) Техническите ресурси, например инфраструктура и достатъчен капацитет за постигане на изискванията към услугата, инструменти за поддържане на процесите в СУУ, настаняване в офиси и оборудване и средства за непрекъснатост на услугата;

c) Информация, например подробности за изискванията на клиента, потребностите на дейността на клиента и плановете на дейността, потребностите на дейността на доставчика на услуги, политиките за управление на услуги, измерванията и други доклади;

d) Финансовите ресурси, включително фондовете за проекти и фондовете за продължаването на експлоатацията на СУУ.

Одобряване на ресурси

Трябва да съществуват процедури за одобряване на използването на договорените ресурси като хора, инфраструктура, инструменти и фондове. Те включват:

a) Фондове, които да бъдат договорени и бюджетирани преди внедряването на плана за управление на услуги;

b) Разпределение на хората, необходими за проекта за внедряване на плана за управление на услуги и за по-дългосрочни непрекъснати подобрения и ежедневна експлоатация на процесите;

c) Идентифициране и развиване на уменията, одобреното наемане

и/или чрез обучение на наличните хора;

d) Идентифициране, съгласуване и одобряване на нови роли и технологии;

e) Изискваната инфраструктура, която може да включва оборудване за офис и център за данни, телекомуникации, като локални точки на LAN и WAN, сървъри, архиви за данни и разпределение на захранването и охлаждането;

f) Инструменти за управление на услуги, които могат да включват инструменти за мониторинг (наблюдение) или измерване и докладване на услугата, или поддържане на определени процеси.

ПРИМЕР: Процедурите за ресурси може да бъдат подпомогнати от инструменти за моделиране на определен капацитет или от информацията, получена от БДУК. Въпреки че инструментите не са изискване на ISO/IEC 20000-1, те могат да направят процесите по-ефикасни и ефективни. Инструментите могат да помогнат за предоставяне на доказателства за съответствие с изискванията на ISO/IEC 20000-1.

Човешки ресурси - Общи положения

Ангажиментът на доставчика на услуги да предоставя ресурси трябва да включва определянето на това какво допринася всяка роля и лице за СУУ и услугата. Доставчикът на услуги трябва също да определя и договори нивата на пълномощия и отговорност за всеки тип роля. Това включва компетентността, образованието, обучението, уменията и опита, изискващи се за всяка роля. Доставчикът на услуги трябва да определи, договори и съобщи тази информация в организацията на доставчика на услуги. Когато е подходящо, доставчикът на услуги трябва да съобщи тази информация и на другите страни.

Доставчикът на услуги трябва да разбира рисковете, възникващи от несигурността кои роли, а по този начин и кои лица, имат особени нива и типове пълномощия и отговорност. Когато нивото на пълномощия, отчетност и отговорност на всяка роля е определено, тази информация трябва да стане неразделен компонент на СУУ. Доставчикът на услуги може да намери за полезна матрицата на отговорност, например RACI, полезна за документиране на пълномощия, отчетност и отговорност. Когато информацията стане компонент на СУУ, тя трябва след това да бъде включена в цикъла на преглед на СУУ.

Ресурсите трябва да включват висшето ръководство, което има общата отговорност и отчетност за СУУ и услугите, доставяни от СУУ. Това изискване за ресурси ще продължи неограничено време след проекта на внедряване на СУУ.

Пълномощията и отговорностите за всеки процес на управление на услуги в СУУ трябва да включва:

a) Собственик на процеса, отговорен за:

1) Разработването на процеса;

2) Осигуряването на съответствие с процеса;

3) Измерването и подобряването на процеса;

b) Ръководител на процес, отговорен за експлоатацията на процеса и управлението на ресурсите за управление на процеси;

c) Персонал, който изпълнява процедурите на процеса.

Компетентност, умения, обучение и опит

Изискваната за определена роля компетентност трябва да се основава на анализ на определени характеристики и изисквания за тази роля. Това трябва да включва, но не се ограничава с образование, обучение, умения и опит.

Нивото и видът на отговорността и пълномощията за ролята също трябва да бъдат взети под внимание. Това включва ролите на висшето ръководство.

Доставчикът на услуги трябва да вземе под внимание и работната натовареност на всяка роля и как всяка роля ще се променя във времето. При разпределението на ролите и отговорностите на лицата трябва да се вземат предвид тези аспекти на ролята, когато се разпределят ролите и отговорностите.

Доставчикът на услуги трябва да разпредели ролите на лицата, които отговарят на критериите за способност за успешно изпълнение на тази роля. Решението за пригодността на дадено лице за определена роля трябва да се основава на сравнение на действителната и изискваната компетентност за тази роля. Там, където има несъответствие между изискванията на договорената компетентност и компетентността на разглежданото лице или на това, което вече изпълнява ролята, доставчикът на услуги трябва да гарантира, че несъответствието е коригирано.

Несъответствията може да бъдат коригирани по няколко метода, например лицето притежава образование и подготовка да коригира несъответствието. Обратно, доставчикът на услуги може да позволи липсващите умения или опит да бъдат придобити чрез работа на лицето с друг, който вече има правилните умения и опит. След предприемане на това коригиращо действие доставчикът на услуги трябва да оцени отново компетентността на лицето или лицата, за да провери, че предприетите действия са коригирали несъответствието.

Доставчиците на услуги трябва да приведат в съответствие ключовите показатели за резултатност и/или областите на ключовите резултати на персонала с постигането на целите на управление на услугите. По този начин персоналът не само ще бъде наясно със своите задължения, но и по-добре ще разбира как може да допринесе за желаните резултати на услугата.

Доставчикът на услуги трябва да създаде и да поддържа текущи записи на компетентността, включително образование, обучение, умения и опит. Доставчикът на услуги трябва да гарантира, че персоналът е наясно с това, как допринася за постигането на целите на управлението на услуги.

Трябва да съществува документирана процедура, която гарантира, че

записите за персонала се поддържат в актуално състояние.

Създаване и подобряване на СУУ

Определяне на обхвата

Доставчикът на услуги трябва да установи дали ISO/IEC 20000-1 е приложим към неговите условия на ранен етап на планиране. Освен това доставчикът на услуги трябва да определи обхвата на СУУ на ранен етап на планиране. Доставчикът на услуги трябва да бъде наясно, че пренебрегването на която и да е от тези дейности може да доведе до отказала или неефикасна СУУ, която не изпълнява изискванията на ISO/IEC 20000-1.

За да бъде ефикасна СУУ, доставчикът на услуги трябва непрекъснато да подобрява СУУ и услугите, като използва методологията ПИПД. Обхватът на СУУ трябва да бъде разбран, преди да бъде подобрена СУУ.

Когато се определи обхватът на СУУ, трябва да бъдат взети предвид следните параметри:

a) Организационните единици, които предоставят услуги, например само един отдел, група отдели или всички отдели;

b) Предлаганите услуги, например единична услуга, група услуги или всички услуги, финансови услуги, търговски услуги (на дребно), услуги на електронна поща;

c) Географското местоположение, откъдето доставчикът на услуги предоставя услугите, например единичен офис или група офиси, регионални, национални или глобални;

d) Клиентите и тяхното местоположение, например един клиент, много клиенти, външни или вътрешни клиенти;

e) Използваната технология за предоставяне на услугите.

Изявлението за обхвата не трябва да включва имената на други страни, които допринасят за доставянето на услугата.

Доставчикът на услуги трябва да вземе предвид указанията на ISO/IEC TR 20000-3, когато планира как да изпълни изискванията на ISO/IEC 20000-1. Това дава указания за определянето на обхвата на СУУ и проверяването на приложимостта на ISO/IEC 20000-1 в условията на доставчика на услуги.

Планиране на СУУ (планиране) - Важни аспекти на планирането

Планът за СУУ трябва да обхваща всички аспекти на управлението на услуги и доставката на услуги и включва, но не се ограничава с аспектите, посочени по-долу.

a) Целите на управлението на услуги. Подредените по приоритет цели на доставчика на услуги при внедряването на необходимите изменения и подобрения трябва да бъдат недвусмислени.

b) Планът за управление на услуги. Там, където е възможно, планът трябва да бъде подразделен на етапи с идентифицирани ползи за всеки етап.

c) Политиката за управление на услуги на доставчика на услуги.

Например политиките, свързани с всички подпланове, като политики за управление на промените, политики за сигурност на информацията, политики за непрекъснатост на услугата. Определянето на политики на ранен етап на планирането на СУУ позволява верификацията на обхвата на СУУ и прави възможно идентифицирането на важни съображения.

d) Изисквания към услугата. Политиките, стандартите или ключовите за дейността показатели на резултатността/характеристиките трябва да са съвместими с изискванията на услугата и трябва да отговарят на изискванията на клиента и потребностите на дейността. Например изискванията за услугата не трябва да водят до несъответствие с политиката за сигурност на информацията, поставяйки цялата дейност в риск.

e) Известни ограничения, които може да окажат влияние върху СУУ. Например персоналът на доставчика на услуги да има недостатъчни умения за това, как да внедри и управлява СУУ. Планът трябва да идентифицира съответни действия, като предоставяне на обучение и информираност, наемане на нов персонал със съответните умения и опит и използване на експертността на други страни за наставляване на персонала.

Съгласуване на планирането и споразуменията

Планът за управление на услуги трябва да включва споразумението и документацията на изискванията за услугата. Целите на услугата трябва да бъдат документирани както в плана, така и в споразуменията между доставчика на услуги и съответните групи. В споразуменията трябва да се вземат под внимание аспектите, изброени по-долу.

a) Клиентът, например споразумение за ниво на услуга (СНУ), изискванията за нови или изменени услуги. Това трябва да бъде взето предвид дори ако документираното споразумение с клиента не е законово обвързан договор.

b) Вътрешни групи, например споразумения на работно ниво с група по оборудването, група за разработване на системата, група по човешките ресурси или група по финансите. Това не може да бъде законово обвързан договор, защото доставчикът на услуги и вътрешните групи са част от една и съща законова единица. Вътрешните групи обаче може да не бъдат част от пряката линия на управление на доставчика на услуги. Вътрешните групи могат да бъдат важен аспект на определянето на обхвата на СУУ, тъй като те могат да допринесат за значителна част от общата услуга.

c) Поддоставчиците и водещите поддоставчици, например договори с подизпълнители за услуга или ресурси.

d) Други стандарти, нормативни и законови изисквания, например специфични за промишлената сфера, като медицински, автомобилни, телекомуникационни или съвместимост на законите за лицензиране на софтуера с определена държава.

Роли на управление, пълномощия и отговорности

Ролите на управление, пълномощията и отговорностите в обхвата на СУУ

трябва да бъдат документирани и в плана за управление на услуги, в документацията на процесите и съответните споразумения, включително:

a) Всички роли, за които ръководството е индивидуално или колективно отчетно и отговорно;

b) Представител на ръководството, включително всякакви граници на пълномощията на тази роля и взаимоотношението с висшето ръководство, което това лице представлява;

c) Собствениците на услуга или процес.

Пълномощията и отговорностите за ролите в СУУ трябва да бъдат проверени, за да се гарантира, че няма конфликти на интереси, например една и съща роля предлага и одобрява изменение. Рамката на пълномощията, отговорностите и ролите в процесите в плана трябва да включват подробностите за това, коя роля носи отчетност и отговорност за всички компоненти на СУУ.

Интерфейси на процесите

Информацията за интерфейсите между процесите трябва да включва типа, метода и честотата на информацията, предавана от един процес към друг. Доставчикът на услуги трябва да бъде наясно, че това е важна част от неговото определяне на процес и гарантира, че процесите и СУУ ще функционират ефикасно и ефективно.

Изискванията за нови или изменени услуги включват етапа от проекта, на който са определени изискванията за услугите, и кога е разработена и прехвърлена услугата. Доставчикът на услуги трябва да бъде наясно, че ефикасното управление на услуги е важно за управлението на някои интерфейси. Интерфейсът между СУУ и всички проекти трябва да бъде определен, съгласуван и записан в плана.

Интегрираните компоненти на СУУ, включително процесите, политиките, целите и плановете, трябва да бъдат измерени така, че да бъдат идентифицирани, управлявани и подобрявани ефективността и ефикасността на СУУ и услугите.

С цел да се улесни интеграцията и взаимодействието между клиента и доставчика на услуги, доставчикът на услуги може да създаде стандартизирани описания на процесите. Описанията на процесите определят целта, резултатите, дейностите, политиките, ролите и отговорностите, информационните единици и интерфейсите за всеки процес на управление на услуги в СУУ. Всеки процес може да изисква и документирани процедури или инструкции за работа за по-нататъшно определяне как да се предприемат дейностите.

Доставчикът на услуги трябва да бъде наясно, че общото ръководство и координиране на СУУ е особено важно, когато тя бъде подобрявана или изменяна по каквато и да е друга причина. Измененията на процесите, които оформят част от СУУ, трябва да бъдат правени само след като бъде разбрано и сметнато за допустимо въздействието на изменението върху

останалата част от СУУ. Това включва въздействието върху други процеси или способността на организацията да предоставя услуги.
ПРИМЕР: Измененията на параметри или цели, използвани в процеса на управление на инцидент и заявка за услуга, може да имат непреднамерен и вреден ефект върху други процеси, като управление на нивото на услугата (УНУ), процеси на докладване и управление на сигурността на информацията (УСИ).

Разбирането на взаимните зависимости между процесите и между всички компоненти на СУУ може да намали риска и да позволи ефикасно управление на СУУ. Примери за интерфейси между процесите на управление на услуги и за интегриране в СУУ може да бъдат намерени в приложение А на тази част на ISO/IEC 20000.

Внедряване и експлоатация на СУУ (изпълнение)

Доставчикът на услуги трябва да внедри и експлоатира СУУ в съответствие с плана за управление на услуги и като средство за постигане на целите на управлението на услуги.

Доставчикът на услуги трябва да бъде наясно с ползите от гарантирането, че пълномощията и отговорностите както на доставчика на услуги, така и на клиента са документирани и договорени за дейностите, които оказват въздействие и върху двете страни.

Доставчикът на услуги трябва да бъде наясно, че лицето, което е подходящо за планирането и първоначалното внедряване, не винаги е подходящо за експлоатацията на СУУ. Изискват се различни умения за планиране, внедряване и експлоатация.

Наблюдение и преглед на СУУ (проверка) - Общи положения

Доставчикът на услуги трябва да наблюдава, измерва и извършва преглед на целите на управление на услугите и да планира необходимите действия, за да гарантира, че те се постигат. Висшето ръководство трябва да бъде наясно с резултатите от прегледите. Ако бъдат сметнати за необходими изменения в плана и целите на управление на услугите, тези изменения трябва да бъдат одобрени в съответствие с процеса на управление на промените.

В съответствие с методологията ПИПД доставчикът на услуги трябва редовно да идентифицира, събира, анализира и докладва информация за процесите и доставяната услуга. Тези дейности трябва да подпомагат ефикасното управление на СУУ и услугите и трябва да позволяват обективно да се демонстрира качеството и стойността на доставяните услуги.

Вътрешен одит

Доставчикът на услуги трябва да гарантира, че вътрешните одити се изпълняват според документирана процедура, която включва пълномощия и отговорности за одитите. Тези, които са отговорни за провеждането на

вътрешни одити, трябва да бъдат с подходящи познания и да са независими от одитираните зони, например те не трябва да одитират своята собствена работа. Изискваните роли трябва да бъдат документирани. Те може да включват ръководител на проект, спонсор, надзорен съвет, други заинтересувани страни и независимите одитори.

Трябва да съществува съгласувана програма за вътрешен одит, която да идентифицира кога да бъде одитирана всяка услуга и коя точка от ISO/IEC 20000-1. Трябва да съществува обосновка за решенията по планирането, включително защо услуги или точки от ISO/IEC 20000-1 са включени или изключени за всеки вътрешен одит. Факторите, които трябва да бъдат взети предвид, включват степента на риск в даден процес, неговата честота при експлоатация и неговата предистория.

Интервалите, през които се изпълняват вътрешни одити, трябва да бъдат планирани, а не извършвани само когато съществуват известни рискове или други проблеми. При подбиране на интервал трябва да взема под внимание темпът на изменение на:

a) СУУ и услугите;

b) Изискванията на клиента и организацията на клиента;

c) Персонала и организацията на доставчика на услуги;

d) Технологията, използвана за доставяне на услугата;

e) Главните изменения на инструментите за управление на услуги, когато се използват инструменти.

Ръководството трябва да гарантира, че одитите са изпълнени по плана освен ако не са повторно планирани по документирани причини.

Вътрешните одити на СУУ трябва да включват оценяване на обхвата на СУУ и че СУУ все още е ефикасна за доставяне на договорените услуги с клиента. Това трябва да включва проверка дали политиката за управление на услуги все още предоставя правилната насока на управление и дали се изпълняват целите в очакваните срокове от време. Вътрешният одит трябва да извършва преглед на плановете и да докладва спрямо резултатността на СУУ.

Като използват времева рамка, съответстваща на честотата на одита, вътрешните одитори трябва да предоставят подробности за всяко несъответствие. Доставчикът на услуги трябва след това да използва резултатите от вътрешните одити, за да идентифицира и подреди по приоритет действията си.

Всички резултати от предишни одити трябва да бъдат взети под внимание. Например, там където е установен повод за загриженост, плановете трябва да включват гарантиране, че причината за загриженост ще бъде одитирана отново при следващия вътрешен одит. Вътрешният одит трябва да провери дали са приложени според договорените срокове от време всички установени и договорени коригиращи и превантивни действия. Вътрешният одит трябва да провери и дали договорените

действия действително са довели до предвиденото подобрение.
Несъответствията трябва да бъдат анализирани, за да се определят всички основни причини. Действията, възникващи от одита, трябва да включват превантивни действия по отношение на всяка идентифицирана основна причина. Действията трябва да имат ясни и договорени собственици и срокове от време, за да помогнат при гарантирането, че те са изпълнени ефикасно и навреме. Последващите дейности по идентифицираните несъответствия трябва да включват верификация, че са предприети действия. Резултатите от предприетите действия трябва да бъдат докладвани на висшето ръководство.
Преглед от ръководството

Трябва да бъде извършван преглед СУУ на планирани интервали, за да се провери дали СУУ продължава да позволява изпълнението на променящите се потребности на дейността и изисквания за услугата. Това трябва да се изпълнява поне веднъж годишно. Някои доставчици на услуги обаче работят в бързо променяща се среда и прегледите на СУУ трябва да бъдат по-често. Прегледът трябва да включва действителния обхват спрямо определения обхват на СУУ, пригодността на текущите планове в сравнение с текущите потребности на клиента и потребностите на дейността на клиента.
По-точно прегледът може да бъде изпълнен спрямо:

a) Резултатността на СУУ по отношение на политиките, плановете и целите;

b)Измерването на ключовите показатели за резултатност/характеристики за процеса;

c) Резултатите от вътрешни и външни одити;

d) Преглед на дейностите за непрекъснато подобряване в съответствие с целите на дейността;

e) Прегледи на измененията след внедряване;

f) Най-добрите практики в бранша;

g) Резултати от проучването на удовлетвореността на клиента;

h) Желаните резултати от дейността.

Поддържане и подобряване на СУУ (действие) - Общи положения

Трябва да се изгради стратегически подход за подобряване на услугата, като се създаде политика за непрекъснато подобряване на СУУ и услугите. Политиката трябва да включва определение на договорените критерии за оценяване, за да се приемат и подредят по приоритет възможностите за подобряване.
Всички услуги, доставени на клиента, процесите на управление на услуги и СУУ в нейната цялост трябва да бъдат обект на непрекъснато подобряване. За да се улесни това още повече, доставчикът на услуги може да намери за полезно да вгради дейности за непрекъснато подобряване в документацията на процеса на управление на услуги. Доставчикът на услуги може да намери

за полезно и да съгласува измерването на компонентите на СУУ и целите на резултатността на персонала спрямо постиженията на непрекъснатото подобряване.
На всяко несъответствие, установено чрез оценявания, одити или други средства, трябва да бъде обърнато внимание и да бъдат предприети действия за отстраняване на причините за установените и потенциалните несъответствия.

Управление на подобренията

Непрекъснатото подобряване е едно от основните понятия в ISO/IEC 20000. Трябва да бъде използвана документирана процедура, която идентифицира пълномощията и отговорностите за всички дейности. Тази процедура трябва да гарантира, че възможностите за подобряване са ефикасно идентифицирани, оценени, подредени по приоритет, одобрени, внедрени, управлявани и измерени.
Входните данни за управление на непрекъснатото подобряване трябва да включват:

a) Съответни насоки от висшето ръководство;

b) Идентифицираните основни причини като резултат от одити и прегледи както на СУУ, така и на отделните услуги;

c) Предложения от клиента, други страни и от организацията на доставчика на услуги;

d) Записи на проблеми;

e) Изпитвания на плановете, например изпитвания на непрекъснатостта на услугата;

f) Доставка на стойност/изисквания към услугата, например подреждане по приоритет на дейностите за подобряване въз основа на критичността на услугите за дейността;

g) Оптимизирано оползотворяване на ресурсите или намаляване на риска, например възможности за увеличена ефективност или подобрена автоматизация.

След 1990г., когато Интернет набира бясна скорост в разпространение, приложение и възможности светът се променя. Появяват се нови работни позиции, начина на рекламиране на продукти се променя, достъпа до информация и количеството й дават огромни възможности.
В днешно време това не е новина, защото е част от нашата култура и начин на живот. Поради тази причина възниква необходимост от разработване на политики за прилагане на системи за управление на услугите и за осигуряване на защита на информацията в организациите, което им дават възможност да постигнат конкурентно предимство.
Систематизираното поддържане, одитинг и подобряване на ИТ средата в организациите е предпоставка за качество, надеждност, цялост на информацията, отговаряща на международни изисквания продукция.
Методологичните принципи, представени в различни политики предоставят възможност за развитие и поддържане на високо ниво на предоставяните от организация услуги, а сертифицирането е доказателство за изпълнение на тези политики.

Списък на съкращенията

БДУК – База данни за управление на конфигурацията
ЕК - Елементи на конфигурацията
ПИПД - Планиране-Изпълнение- Проверка-Действие
СНУ - Споразумения за нивото на услугата
СУУ - Система за управление на услугите
УНУ - управление на нивото на услугата
УСИ - управление на сигурността на информацията
COBIT – Control objectives for information and related technology
ITIL – Information technology infrastructure library
IoT - Internet of things

Източници

1. www.diksi.bg/bg
2. ISO/IEC 20000-1, Information technology – Service management – Part 1: Service management system requirements
3. ISO/IEC 20000-2, Information technology — Service management — Part 2: Code of practice
4. www.isaca.org
5. https://www.axelos.com/best-practice-solutions/itil