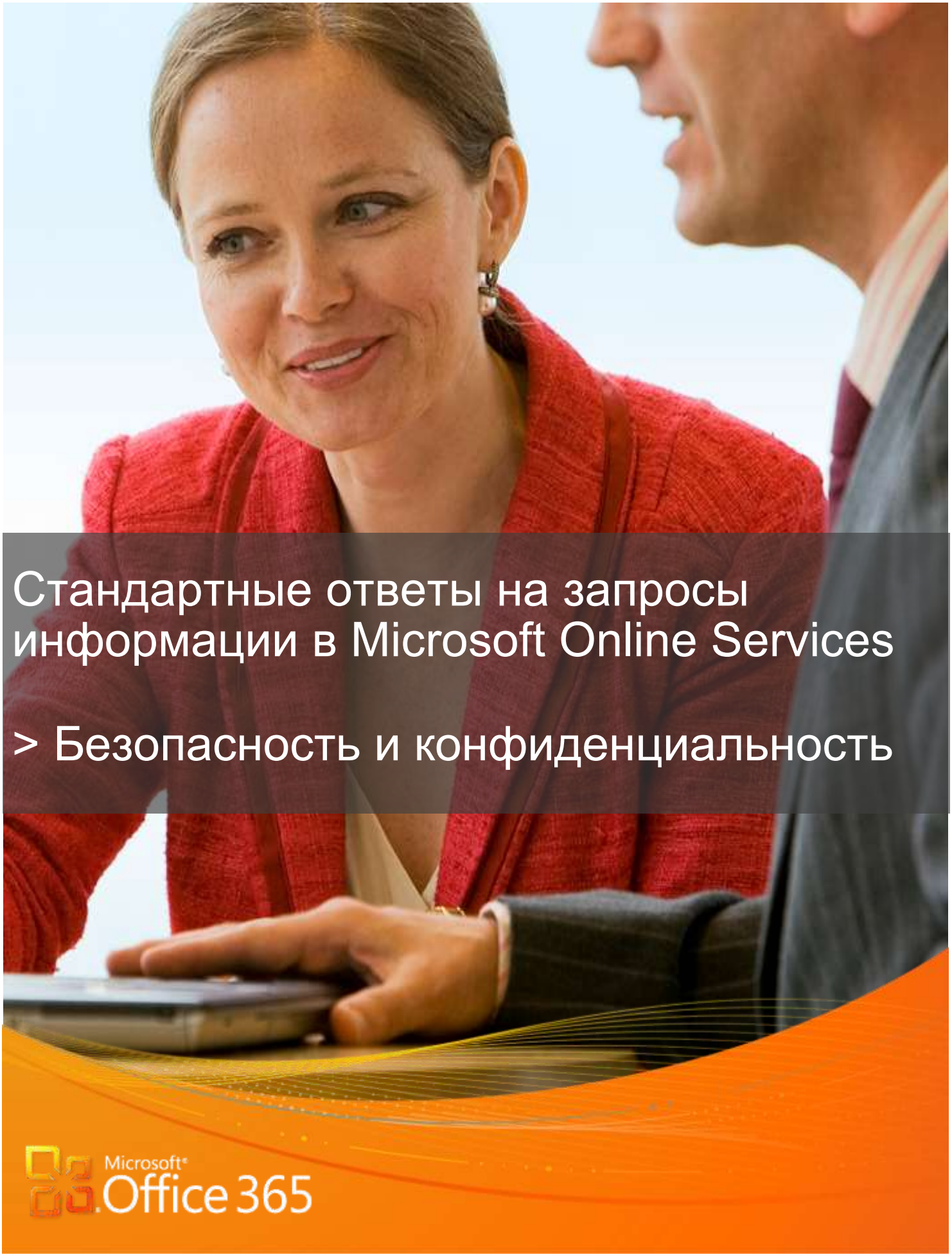

Стандартные ответы на запросы информации в Microsoft Online Services

> Безопасность и конфиденциальность

Microsoft Office 365

Ограничение ответственности

Содержащиеся в документе сведения отражают текущую позицию корпорации Майкрософт в отношении обсуждаемых вопросов на момент публикации. Поскольку корпорация Майкрософт должна реагировать на изменение рыночных условий, данный документ не следует рассматривать как обязательство со стороны корпорации Майкрософт и корпорация Майкрософт не гарантирует точности представленных сведений после даты публикации.

Сведения в данном документе предоставлены исключительно в ознакомительных целях. КОРПОРАЦИЯ МАЙКРОСОФТ НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ, ПОДРАЗУМЕВАЕМЫХ ИЛИ ПРЕДУСМОТРЕННЫХ ЗАКОНОМ, ОТНОСИТЕЛЬНО СОДЕРЖАЩИХСЯ В ДОКУМЕНТЕ СВЕДЕНИЙ.

Пользователь единолично несет ответственность за соблюдение всех применимых законов об авторском праве. Согласно законам об авторском праве, никакие части этого документа нельзя воспроизводить, хранить или использовать в поисковых системах или передавать в любой форме (электронной, механической, в виде фотокопий, записей или иными способами) и в любых целях без письменного разрешения корпорации Майкрософт.

Корпорация Майкрософт может являться правообладателем патентов, заявок на получение патента, товарных знаков, авторских прав и прочих объектов интеллектуальной собственности, которые имеют отношение к содержанию данного документа. Предоставление настоящего документа не означает передачи какой-либо лицензии на использование таких патентов, товарных знаков, авторских прав и других объектов интеллектуальной собственности, за исключением случаев, явно оговоренных в лицензионном соглашении корпорации Майкрософт.

Microsoft и Microsoft Office 365 являются охраняемыми товарными знаками корпорации Майкрософт в США и в других странах.

Использованные в документе названия реальных компаний или продуктов могут быть товарными знаками соответствующих владельцев.

Содержание

Cloud Security Alliance (CSA) — некоммерческая организация, занимающаяся продвижением передовых методов обеспечения безопасности при облачных вычислениях.

Организация Cloud Security Alliance выпустила документ под названием Cloud Controls Matrix, призванный помочь заказчикам в оценке облачных служб и определить круг вопросов, на которые необходимо получить ответы, прежде чем переходить на облачные службы. В ответ на это группа Microsoft Online Services создала данный документ, описывающий, каким образом мы соответствуем предложенным принципам, и сопоставляющий эти принципы с системой сертификации ISO.

Подробнее:
https://cloudsecurityalliance.org

Введение

Работа с облачными вычислениями поднимает вопросы, связанные с безопасностью, защитой данных, конфиденциальностью и правами на данные. Службы Microsoft Online Services работают в центрах обработки данных, управляемых и принадлежащих корпорации Майкрософт, которые физически расположены в разных уголках мира. Службы разработаны так, чтобы их производительность, масштабируемость, безопасность и уровень обслуживания отвечали ожиданиям корпоративных заказчиков. Мы использовали самые современные технологии и процессы, чтобы обеспечить стабильный и надежный доступ, безопасность и конфиденциальность для каждого пользователя. Службы Microsoft Online Services обладают встроенными возможностями, которые позволяют им соответствовать широкому ряду норм и требований к конфиденциальности.

В данном документе мы представляем нашим заказчикам подробный обзор методов, которые позволяют службам Microsoft Online Services соответствовать требованиям к безопасности, конфиденциальности, совместимости и управлению рисками, описанным в документе Cloud Controls Matrix (CCM) организации Cloud Security Alliance (CSA). Обращаем ваше внимание, что целью настоящего документа является предоставление информации о работе служб Microsoft Online Services. На заказчиках лежит ответственность за управление средой и ее поддержку после подготовки службы к работе (т. е. управление доступом пользователей, а также внедрение необходимых политик и процедур в соответствии с нормативными требованиями).

Требования к безопасности для облака: Cloud Controls Matrix

Документ под названием Cloud Controls Matrix (CCM) был опубликован некоммерческой организацией, руководимой ведущими специалистами отрасли и сосредоточенной на помощи заказчикам в принятии правильных решений при переходе на облачные вычисления. Он содержит подробный разбор принципов и концепций безопасности и конфиденциальности, сгруппированных под руководством организации Cloud Security Alliance в 13 частях.
В данном документе корпорация Майкрософт публикует подробный обзор возможностей, позволяющих нам соответствовать требованиям CCM.
С помощью описанного здесь стандартного ответа на запрос информации мы хотим дать заказчикам наглядную и подробную информацию для оценки разнообразных предложений, существующих сегодня на рынке.

Знакомство с Office 365

Корпорация Майкрософт предлагает целый ряд облачных служб, однако здесь наша цель — дать ответы на вопросы, связанные с бизнес-службами Microsoft® Office 365. Продукты Office 365 представляют собой набор приложений для повышения производительности, соединяющий в облаке знакомый вам пакет Microsoft Office профессиональный плюс с нашим ПО для использования электронной почты и совместной работы. Приложения Office 365 работают в облачной инфраструктуре и доступны с разных клиентских устройств. Заказчики не контролируют инфраструктуру облака, не управляют его сетью, серверами, операционными системами, возможностями хранилищ или отдельных приложений, за исключением некоторых возможностей конфигурации. Дополнительные сведения см. на веб-сайте www.office365.com.

Как поставляется Office 365: набор служб

Центр управления безопасностью предлагает дополнительные сведения на такие темы, как географическое расположение данных, доступ администратора, а также расширенную информацию о методах, позволяющих добиться соответствия требованиям.

Дополнительные сведения см. на сайте Trust Center

(http://go.microsoft.com/fwlink/?LinkID=206613&CLCID=0x409)

При оценке среды управления в предложениях, относящихся к типу «программа как служба», важно учитывать весь набор служб поставщика услуг облачных вычислений. Предоставлять инфраструктуру и приложения могут сразу несколько организаций, и добиться согласованной работы при этом может быть нелегко. Сбой в любой части этого комплекса может сорвать поставку облачных услуг и повлечь самые разрушительные последствия. Поэтому заказчики нуждаются в предварительной оценке работы поставщика услуг, чтобы понимать не только принципы функционирования приложений, но и лежащую в их основе инфраструктуру.

Корпорация Майкрософт является поставщиком, владеющим и управляющим всем набором необходимых услуг, от облачных приложений до центров обработки данных, в которых хранятся данные и службы заказчика, включая магистрали оптоволоконного кабеля, по которым передается информация, а также до непосредственной подготовки службы к работе.

В среде Office 365 службы управляются группой *Microsoft Global Foundation Services*, предоставляющей услуги инфраструктуры как для заказчиков Майкрософт, так и для нужд самой корпорации, а также группой *Microsoft Online Services*, которая предоставляет набор приложений и данные (см. рисунок 1).

Рисунок 1. Набор служб для Office 365

Сертификаты ISO 27001, полученные корпорацией Майкрософт, позволяют заказчикам оценить, насколько корпорация отвечает стандартам по поставке и применению услуг или превосходит эти стандарты.

Сертификаты ISO для набора служб Microsoft Online Services

Как Office 365, так и инфраструктура, на которую он опирается (Microsoft Global Foundation Services), применяют системы безопасности на основе семейства стандартов Международной организации по стандартизации (ISO/IEC 27001:2005) и имеют сертификаты ISO 27001 от независимых аудиторов.

Наши сертификаты ISO 27001 позволяют заказчикам оценить, насколько корпорация отвечает стандартам по поставке и применению услуг или превосходит эти стандарты. В стандарте ISO 27001 определены пути внедрения, мониторинга, поддержки и постоянного усовершенствования системы менеджмента информационной безопасности (СМИБ). Кроме того, инфраструктура и службы проходят ежегодный аудит стандарта SAS 70 (или его преемника SSAE16).

Политика защиты информации Microsoft Online Services, применимая к Office 365, также соответствует стандарту ISO 27002, дополненному специальными требованиями для веб-служб. ISO 27002 не является видом сертификации, но предлагает набор положений, подходящих для системы менеджмента информационной безопасности.

Как читать требования CSA и ответ корпорации Майкрософт

Далее приводится сопоставление наших методов обеспечения безопасности с руководством, предложенным организацией CSA. Содержимое первых двух столбцов, озаглавленных «Идентификатор критерия в CCM» и «Описание», взято непосредственно из определений соответствующих положений CCM[1]. Третий столбец с заголовком «Ответ корпорации Майкрософт» содержит:

1) короткое объяснение того, каким образом Microsoft Online Services соответствует данной рекомендации Cloud Security Alliance;
2) ссылку на критерии стандарта ISO 27001 с указанием в соответствующих случаях сертификатов ISO 27001, присвоенных службам Microsoft Global Foundation Services (GFS) и (или) Microsoft Online Services.

Пример:

Критерий IS-O2 документа Cloud Controls Matrix организации Cloud Security Alliance гласит:

«Среднее и высшее руководство предпринимает официальные действия, направленные на защиту информации с помощью ясного письменного распоряжения, обязательства, точно сформулированного задания и проверки его исполнения».

Ответ Майкрософт:

«Каждая утвержденная руководством версия политики защиты информации и все ее последующие обновления рассылаются всем заинтересованным лицам. Политика защиты информации доступна для ознакомления всем новым и существующим сотрудникам группы Microsoft Online Services.

Факт присвоения службам Microsoft Online Services сертификатов ISO 27001 означает, что, по мнению независимого аудитора, наша среда соответствует этим стандартам или превосходит их.

Общедоступная копия сертификации ISO для служб Microsoft Online Services доступна здесь: ISO Certification

(http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/, условие поиска: «Microsoft Online Services»)

(1) Содержимое CCM в первом и втором столбцах принадлежит Cloud Security Alliance (по данным на 2011 г.) и использовано с разрешения правообладателя.

Ответ Майкрософт (продолжение):

Все сотрудники Microsoft Online Services подтверждают, что они ознакомились с принципами, описанными в документах политики защиты информации, и согласны придерживаться этих принципов.

Персонал подрядчиков Microsoft Online Services также соглашается следовать соответствующим принципам политики защиты информации. В случае если одна из сторон по какой-либо причине не имеет доступа к этой политике, надзирающий агент корпорации Майкрософт отвечает за предоставление ей материалов. Предназначенная для заказчиков версия политики защиты информации может быть предоставлена по запросу. Для получения копии политики защиты информации существующие и потенциальные заказчики должны подписать соглашение о неразглашении или равнозначный ему документ.

Документы "Management Commitment to Information Security" (Обязательства руководства по защите информации) и "Management Responsibility" (Обязанности по руководству персоналом) подпадают под действие стандарта ISO 27001, а именно Статьи 5 и Приложения A, части 6.1.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы».

Инструкции для получения дополнительных сведений и руководств

Настоятельно рекомендуем ознакомиться с общедоступными стандартами ISO 27001 и ISO 27002. Стандарты ISO можно приобрести на веб-сайте Международной организации по стандартизации по адресу http://www.iso.org/iso/iso_catalogue. Эти стандарты ISO содержат подробную информацию и инструкции. Повторим, что факт присвоения службам Microsoft Online Services сертификатов ISO 27001 означает, что, по мнению независимого аудитора, наша среда соответствует этим стандартам или превосходит их.

Пример:

При ознакомлении со стандартом можно взять критерий или статью ISO 27001 и прочесть конкретные требования, например критерии статьи 5 «Management Commitment to Information Security» (Обязательства руководства по защите информации) стандарта ISO 27001 или информацию из консультативного положения 6.1.1 стандарта ISO 27002.

ISO27002 (ISO 27002) (загрузить)

Практическое руководство ISO27002 ISO 27001 ISM (PDF).

Стандарт ISO/IEC 27002:2005 определяет правила и общие принципы подготовки, внедрения, обслуживания и усовершенствования системы менеджмента информационной безопасности в организации.

Стандарт ISO/IEC 17799:2005 переименован в ISO/IEC 27002:2005 (Информационные технологии – Технологии безопасности – Практическое руководство по менеджменту информационной безопасности). Стандарты ISO/IEC 17799:2005 и ISO/IEC 27002:2005 идентичны.

Этот стандарт содержит полный набор целей при управлении информационной безопасностью и подборку лучших средств управления.

Примечание. Став дистрибьютором организации ANSI, мы теперь можем вам предложить электронную PDF-версию стандарта по гораздо более низкой цене, чем печатная версия, – см. пресс-релиз.

Издатель: ANSI/INCITS
Формат: документ для электронной загрузки в формате PDF
Условия лицензирования: приобретение и использование этого продукта регулируется данным лицензионным соглашением
Другие форматы: ISMS 3 Standards Kit (загрузить)
Доступность: немедленная загрузка

«Обязанности по руководству персоналом…»

Требования ISO27001 (ISO 27001) ISMS (PDF)

Требования ISO27001 ISO 27001 ISO/IEC 27001 ISMS.

ISO/IEC 27001 (Информационные технологии – Технологии безопасности – Системы менеджмента информационной безопасности – Требования)

ISO/IEC 27001 – международный стандарт системы менеджмента информационной безопасности, по которому можно получить сертификацию системы СМИБ. Он позволяет организациям добиться соблюдения всех нормативных требований, связанных с информационной безопасностью (например, FISMA, GLBA, PIPEDA и т. д.); такое близок по тематике к изданию «Практическое руководство» ISO/IEC 27002 (бывший ISO/IEC 17799).

Система, соответствующая требованиям ISO/IEC 27001, использует систематический подход к обеспечению доступности, конфиденциальности и целостности корпоративной информации. Применяемые критерии направлены на выявление и устранение всех возможных потенциальных рисков, угрожающих информационным активам организации.

Этот стандарт вобрал в себя профессионализм и знания опытнейших специалистов в области информационной безопасности, работающих во множестве известных организаций более чем 40 стран мира, чтобы предложить вам передовые методы защиты информационной безопасности. Все больше фирм применяют этот стандарт и не только демонстрируют соответствие требованиям и эффективное управление рисками, но и успешно готовятся с его помощью к появлению новых регулятивных норм.

Ресурсы

Посетите наш **Центр управления безопасностью**, чтобы получить:

- технические документы;
- вопросы и ответы;
- информацию о сертификации;
- стандарты ISO, доступные для приобретения.

(Ссылка на Центр управления безопасностью: http://go.microsoft.com/fwlink/?LinkID=206613&CLCID=0x409)

Общедоступная копия сертификации ISO для служб Microsoft Online Services доступна здесь: **ISO Certification** *(http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/, условие поиска: «Microsoft Online Services»).*

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с CO-01 по CO-02

Идентификатор критерия в CCM[1]	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
CO-01 **Соответствие требованиям — планирование аудита**	Для минимизации риска прерывания бизнес-процесса планы аудита, действия и согласованные мероприятия должны разрабатываться с упором на проблемы дублирования данных, доступа к данным и сужения границ данных. Действия по аудиту должны быть заранее спланированы и согласованы заинтересованными лицами.	Мы ставим перед собой две цели: сделать безопасность ключевым принципом работы с нашими службами и донести до заказчиков гарантии соблюдения этого принципа. Мы внедрили и намерены поддерживать разумные и эффективные технические и организационные меры, механизмы внутреннего контроля и процедуры защиты информации, направленные на защиту данных заказчика от случайной потери, повреждения или изменения, от несанкционированного доступа или разглашения либо от незаконного уничтожения. Каждый год мы проходим проверку международно признанных внешних аудиторов, чтобы подтвердить независимую оценку того, насколько наши политики и процедуры отвечают стандартам безопасности, конфиденциальности, непрерывности и соответствия требованиям. Подписав соглашение о неразглашении, существующие заказчики могут получить информацию об аудите через Центр управления безопасностью, а потенциальные заказчики — по запросу. Предоставление отчетов и сертификатов независимого аудита служб Microsoft Online Services заменяет заказчикам аудит, который они бы проводили самостоятельно. Эти сертификаты и аттестаты достоверно отражают наши способы достижения целей в сфере безопасности и соответствия требованиям и служат для заказчиков наглядным подтверждением соблюдения нами данных обязательств. В целях безопасности и производительности заказчикам запрещено проводить аудит служб Microsoft Online Services самостоятельно. Документ «Monitor and review the Information Security Management System (ISMS)» (Сбор и анализ данных системы менеджмента информационной безопасности (СМИБ)) подпадает под действие стандарта ISO 27001, а именно Статьи 4.2.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
CO-02 **Соответствие требованиям — независимый аудит**	Независимые проверки и оценки (например, внутренние и внешние проверки, сертификации, проверки на уязвимости и проникновения) должны выполняться не реже чем раз в год либо через запланированные интервалы времени, чтобы гарантировать соответствие организации политикам, процедурам, стандартам и применимым нормативным требованиям.	Для получения дополнительных сведений см. наши текущие сертификации и аттестации независимых сторон, доступные в положении CO-01 или в Центре управления безопасностью.

[1] Содержимое CCM в первом и втором столбцах принадлежит Cloud Security Alliance (по данным на 2011 г.) и использовано с разрешения правообладателя.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с CO-03 по CO-05

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
CO-03 **Соответствие требованиям — аудит третьих сторон**	Сторонние поставщики служб должны демонстрировать соответствие требованиям защиты и конфиденциальности информации, определениям служб и соглашениям об уровне услуг по доставке, включенным в контракты этих поставщиков. Отчеты, записи и службы третьих сторон должны проходить аудит и проверку через запланированные интервалы времени для поддержания соответствия требованиям соглашений о поставках.	В договорах группы Microsoft Online Services с третьими сторонами, поставляющими услуги корпорации Майкрософт, закреплено требование поддерживать соответствие стандартам политики защиты информации служб Microsoft Online Services. Кроме того, одно из требований Microsoft Online Services заключается в том, чтобы эти третьи стороны каждый год проходили аудит отдельно или в рамках ежегодного аудита сторонних поставщиков служб Microsoft Online Services. Office 365 имеет встроенные возможности аудита, указанные в описании веб-службы Office 365 Exchange. Отчеты Office 365 предназначены для внутреннего пользования, любой администратор может конфиденциально их просматривать. Документ «Addressing security in third party agreements and third party service delivery management» (Безопасность адресации в соглашениях третьих сторон и управление поставкой услуг третьих сторон) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 6.2 и 10.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
CO-04 **Соответствие требованиям — взаимодействие с властями**	Связи и точки соприкосновения с местными органами власти должны поддерживаться согласно бизнес-требованиям и требованиям заказчиков, а также соответствовать законодательным, регулятивным и закрепленным в контракте требованиям. Для обеспечения надлежащих точек контакта данные, объекты, приложения, инфраструктура и оборудование считаются областью применения законодательства и подпадают под его юрисдикцию.	Группа Microsoft Online Services поддерживает связи с внешними сторонами, такими как органы власти, поставщики услуг, организации по управлению рисками и отраслевые форумы, для того чтобы в случае необходимости быстро принять меры или получить рекомендации. В корпорации Майкрософт есть специальная группа сотрудников, через которую осуществляется большая часть контактов с правоприменяющими органами. Роли и ответственность за поддержание и управление этими связями четко определены. Документ «Contact with authorities and contact with special interest groups» (Контакт с государственными организациями и группами, представляющими особые интересы) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 6.1.6 и 6.1.7. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
CO-05 **Соответствие требованиям — сопоставление регулятивных норм информационной системы**	Для всех элементов информационной системы должны быть определены регулятивные, нормативные и закрепленные в контракте требования. Подход организации к выполнению известных требований и адаптации к новым предписаниям должен быть ясно определен, задокументирован и актуален для каждого элемента информационной системы в этой организации. Элементы информационной системы могут включать данные, объекты, приложения и оборудование. Для упрощения сопоставления каждый элемент считается областью применения законодательства и подпадает под его юрисдикцию.	Группа Microsoft Online Services предоставляет информацию о применяемых положениях и регулятивных нормах в описаниях контрактов и услуг, в том числе относительно юрисдикции. У служб Microsoft Online Services имеется установленный процесс для определения и внедрения в своих службах изменений в положениях и регулятивных нормах, которые выявляются во время ежегодного аудита ISO 27001. Кроме того, веб-интерфейс Microsoft Online Services ограничивает возможность добавления пользователей в юрисдикции, выходящие за пределы области поддержки Microsoft Online Services. Документ «Establish the ISMS, management review of the ISMS and compliance with legal requirements» (Внедрение СМИБ, анализ управления СМИБ и соответствие юридическим требованиям) подпадает под действие стандарта ISO 27001, а именно Статей 4.2.1 и 7.3, а также Приложения A, части 15.1. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерий CO-06

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
CO-06 **Соответствие требованиям — интеллектуальная собственность**	Должны разрабатываться и применяться политики, процессы и процедуры, направленные на защиту интеллектуальной собственности и использование защищаемого ПО, в соответствии с законодательной юрисдикцией и закрепленными в контракте ограничениями, действующими в организации.	Мы требуем от всех текущих и новых сотрудников соблюдения законов о защите интеллектуальной собственности. Корпорация Майкрософт несет ответственность за использование защищаемого ПО согласно законодательной юрисдикции и закрепленным в контракте ограничениям, действующим в организации. Перед запуском каждой службы в эксплуатацию она сравнивается со всем существующим сторонним ПО для подтверждения наличия необходимого лицензирования. Кроме того, в службах Microsoft Online Services предусмотрены политики и процедуры, обеспечивающие соблюдение требований закона о защите авторских прав в цифровую эпоху и других законодательных норм, распространяющихся на конкретную службу. Данные заказчика используются в службах Microsoft Online Services только для оказания соответствующих услуг и их поддержки. Бизнес-службы корпорации Майкрософт разработаны отдельно от клиентских служб. Хотя некоторые данные могут храниться или обрабатываться в системах, используемых как клиентскими, так и бизнес-службами, данные бизнес-служб недоступны для систем, используемых в рекламных целях. Документ «Establish the ISMS» (Внедрение СМИБ) подпадает под действие стандарта ISO 27001, а именно Статьи 4.2.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с DG-01 по DG-02

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
DG-01 **Управление данными — владение и руководство**	Управлением любыми данными должны заниматься лица, ответственность которых определена, закреплена в письменной форме и объявлена.	Группа Microsoft Online Services внедрила официальную политику, требующую учета активов, используемых для предоставления служб Microsoft Online Services, и назначения этим активам владельца (определение актива включает данные и оборудование). Владельцы активов отвечают за поддержку актуальности информации этих активов. Документ «Allocation of information security responsibilities and ownership of assets» (Распределение ответственности по защите безопасности и владение активами) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 6.1.3 и 7.1.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
DG-02 **Управление данными — классификация**	Данные и содержащие их объекты должны быть классифицированы по типу, юрисдикции происхождения, юрисдикции местонахождения, контексту, правовым ограничениям, ограничениям контракта, значению, конфиденциальности, критичности для организации, а также по обязательствам третьей стороны по их сохранению и предотвращению несанкционированного разглашения или неправильного использования.	Стандарты Microsoft Online Services предоставляют руководство по классификации активов, состоящее из нескольких применимых категорий классификации безопасности, а затем реализуют стандартный набор атрибутов безопасности и конфиденциальности. Документ «Information classification» (Классификация информации) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 7.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с DG-03 по DG-04

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
DG-03 **Управление данными — обработка, маркировка и политика безопасности**	Должны быть внедрены политики и процедуры для маркировки, обработки и защиты данных и содержащих их объектов. Для объектов, служащих сводными контейнерами для данных, должны быть внедрены механизмы наследования меток.	Стандарты Microsoft Online Services предоставляют руководство по классификации активов, состоящее из нескольких применимых категорий классификации безопасности, а затем реализуют стандартный набор атрибутов безопасности и конфиденциальности. Документ «Information classification, labeling and handling» (Класссификация, маркировка и обработка информации) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 7.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
DG-04 **Управление данными — политика хранения**	Для обеспечения соответствия регулятивным, нормативным и закрепленным в контракте требованиям должны существовать политики и процедуры для хранения данных; кроме того, должны применяться механизмы резервного копирования данных. Через запланированные интервалы времени должна проводиться проверка восстановления резервных копий с диска или магнитной ленты.	Заказчикам служб Microsoft Online Services предоставляются возможности применения политик хранения данных, что определено в описаниях отдельных служб. Что касается резервных копий, содержимое реплицируется из основного центра обработки данных во вторичный центр обработки данных. Таким образом, расписания резервного копирования нет, поскольку репликация происходит постоянно. При необходимости заказчики могут самостоятельно выполнять резервное копирование и извлечение данных. Данные заказчиков хранятся в избыточной среде с надежными возможностями по резервному копированию, восстановлению и отработке отказа, чтобы обеспечить доступность, непрерывную работу и быстрое восстановление. Реализовано несколько уровней избыточности данных, от применения резервных дисков для защиты от сбоев локальных дисков до непрерывной полной репликации данных для географически рассредоточенных центров обработки данных. Корпорация Майкрософт ежегодно проходит проверку методов резервного копирования и восстановления. Документ «Information back-up» (Резервное копирование информации) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.5.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерии с DG-05 по DG-06

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
DG-05 **Управление данными — безопасная утилизация**	Должны быть внедрены политики, процедуры и реализованы механизмы, обеспечивающие безопасное выбытие и полное удаление данных со всех носителей и гарантирующие невозможность восстановления этих данных какими-либо методами.	Корпорация Майкрософт использует передовые процедуры и решения для очистки, соответствующие стандарту NIST 800-88. Для жестких дисков, которые нельзя очистить, мы применяем процесс, уничтожающий диск физически и делающий восстановление информации невозможным (это может быть процесс дробления, измельчения, разрезания, сжигания). Информационные активы Microsoft Online Services, предназначенные для выбытия, уничтожаются. Способ уничтожения определяется типом актива. Сведения об уничтожении сохраняются. Все службы Microsoft Online Services используют утвержденные службы хранения носителей и управления выбытием. Бумажные документы уничтожаются утвержденными способами в рамках заранее обозначенного завершающего этапа жизненного цикла. Носители для хранения данных, такие как магнитные ленты, жесткие диски и компакт-диски, очищаются от всех данных и уничтожаются с помощью решения для очистки, соответствующего стандарту NIST 800-88. Документ «Secure disposal or re-use of equipment and disposal of media» (Безопасная утилизация или повторное использование оборудования и утилизация носителей) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 9.2.6 и 10.7.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
DG-06 **Управление данными — непроизводственные данные**	Производственные данные не должны реплицироваться или использоваться в непроизводственных средах.	Корпорация Майкрософт применяет принцип разделения обязанностей, чтобы гарантировать ограничение доступа к средам тестирования и производства в соответствии с политикой. Перемещение или копирование данных заказчика за пределы среды производства в непроизводственную среду категорически запрещено, кроме тех случаев, когда получено согласие заказчика, либо по распоряжению юридического отдела Майкрософт. Документ «Separation of development, test and operation facilities and protection of system test data» (Разделение помещений для разработки, тестирования и эксплуатации и защита данных системных тестов) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 10.1.4 и 12.4.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с DG-07 по DG-08

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
DG-07 **Управление данными — утечка информации**	Для предотвращения утечки данных должны быть внедрены защитные механизмы.	В средах Microsoft Online Services реализованы логические и физические элементы управления (см. описание службы безопасности Office 365, доступное через Центр загрузки); пользователи могут по своему выбору улучшать базовые возможности с помощью поддерживаемых технологий, таких как: 1. Конфигурация правил передачи сообщений. 2. Интеграция с продуктами защиты от утечки данных электронной почты. 3. Поддержка интеграции служб управления правами Active Directory. 4. Exchange Hosted Encryption и другие продукты шифрования. Документ «Information leakage» (Утечка информации) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 12.5.4. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
DG-08 **Управление данными — оценка рисков**	Через запланированные интервалы времени должна проводиться оценка рисков, связанная с требованиями по управлению данными и учитывающая следующее: • сведения о том, где хранятся и как передаются конфиденциальные данные между приложениями, базами данных, серверами и в сетевой инфраструктуре; • соответствие определенным периодам хранения и требованиям утилизации в конце жизненного цикла; • классификацию данных и их защиту от несанкционированного использования, доступа, потери, уничтожения и фальсификации.	Для служб Microsoft Online Services ежегодно проводится анализ влияния на бизнес. Этот анализ включает: • определение угроз, относящихся к бизнес-среде и процессам Microsoft Online Services; • оценку выявленных угроз, включая потенциальное влияние и ожидаемый ущерб; • одобренную руководством стратегию для смягчения значительных угроз и для восстановления критических бизнес-процессов. Документ «Establish the ISMS and Information classification and asset management» (Внедрение СМИБ, классификация информации и управление активами) подпадает под действие стандарта ISO 27001, а именно Статьи 4.2.1 и Приложения A, части 7.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с FS-01 по FS-02

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
FS-01 **Безопасность помещений — политика**	Должны быть внедрены политики и процедуры для поддержания безопасной и защищенной рабочей среды в офисах, кабинетах, помещениях и защищенных областях.	Доступ к зданиям Майкрософт контролируется, и входы в центры обработки данных защищены устройствами чтения карт, срабатывающими на авторизованные идентификационные карты, или биометрией. От персонала отдела регистратуры требуется уверенно узнавать сотрудников, работающих полный рабочий день, и официальных подрядчиков даже без идентификационных карт. Все гости должны носить идентификационные карты и перемещаться в сопровождении сотрудников корпорации Майкрософт. Документ «Securing offices, rooms, and facilities» (Защита офисов, кабинетов и помещений) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 9.1.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
FS-02 **Безопасность помещений — доступ пользователей**	Физический доступ к информационным активам и функциям для пользователей и персонала службы поддержки должен быть запрещен.	Доступ ограничен таким образом, что только основной персонал может получить разрешение на управление приложениями и службами пользователей. При санкционировании физического доступа в центр обработки данных используется несколько защитных процессов проверки подлинности: идентификационная карта и смарт-карта, биометрические сканеры, непрерывное видеонаблюдение, двухфакторная проверка подлинности и ответственные за безопасность на местах сотрудники. В дополнение к дверным элементам управления физическим доступом управляющая организация центров обработки данных Майкрософт внедрила следующие оперативные процедуры для ограничения физического доступа авторизованных сотрудников, подрядчиков и посетителей: • Авторизация для временного или постоянного доступа в центры обработки данных корпорации Майкрософт дается только штатному персоналу. Запросы и решения об авторизации отслеживаются с помощью системы доступа по билетам. • Идентификационные карты для предоставления доступа персоналу выпускаются после проверки идентификационных данных. • Управляющая организация центров обработки данных Майкрософт выполняет проверку списка постоянного доступа. По результатам этого аудита предпринимаются необходимые действия. Документ «Physical and environmental security» (Физическая защита и защита среды) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 9. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с FS-03 по FS-05

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
FS-03 **Безопасность помещений — точки доступа**	Должны быть внедрены периметры физической защиты (заборы, стены, шлагбаумы, ограда, ворота, электронное наблюдение, приборы для физической проверки подлинности, регистрационные стойки и охранные патрули) для защиты конфиденциальных данных и информационных систем.	Здания центров обработки данных не имеют отличительных знаков, на них не указано, что внутри расположены центры обработки данных корпорации Майкрософт. Доступ в помещения центров обработки данных ограничен. Двери по периметру главного помещения или приемной оборудованы устройствами контроля доступа по электронным картам для ограничения доступа к внутренним помещениям. Кабинеты центра обработки данных Майкрософт, в которых находятся критически важные системы (серверы, генераторы, электрические щиты, сетевое оборудование и т. д.), также защищены разнообразными устройствами безопасности, такими как система управления доступом через электронные карты, замки, запирающиеся на ключ, биометрические устройства и (или) устройства для предотвращения прохода нескольких лиц по одному пропуску. Помещения центра обработки данных управляются через GFC. Дополнительные физические барьеры, такие как запертые кабинеты или запертые ящики внутри периметров, могут потребоваться для определенных активов в соответствии с политиками и (или) бизнес-требованиями. Документ «Physical security perimeter and environmental security» (Периметр физической защиты и защита среды) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 9. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
FS-04 **Безопасность помещений — авторизация защищенной зоны**	Входы и выходы из охраняемых зон должны быть ограничены и поставлены под наблюдение с помощью средств контроля физического доступа, чтобы гарантировать доступ только авторизованных сотрудников.	Документ «Public access, delivery, loading area and physical/ environmental security» (Область общего доступа, доставки, погрузки, а также физическая защита и защита среды) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 9. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы. Также см. критерий FS-03.
FS-05 **Безопасность помещений — вход неавторизованных лиц**	Такие точки входа и выхода, как служебные зоны, а также другие точки, в которых неавторизованный персонал может попасть за периметр, должны находиться под наблюдением и контролем и по возможности быть изолированы от помещений для обработки и хранения данных во избежание несанкционированного разглашения, повреждения или утери данных.	Документ «Public access, delivery, loading area and physical/ environmental security» (Область общего доступа, доставки, погрузки, а также физическая защита и защита среды) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 9. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы. Также см. критерий FS-03.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с FS-06 по FS-08

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
FS-06 **Безопасность помещений — авторизация перемещения**	Для перемещения оборудования, ПО или данных во внешние расположения нужна предварительная авторизация.	Процедуры защиты активов и данных в Microsoft Online Services предоставляют руководство по защите логических и физических данных и включают инструкции по перемещению. Документ «Removal of Property and change management» (Удаление имущества и управление изменениями) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 9.2.7 и 10.1.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
FS-07 **Безопасность помещений — удаленное оборудование**	Должны быть внедрены политики и процедуры защиты и управления активами для использования и безопасного удаления оборудования, эксплуатируемого и обслуживаемого за пределами территории организации.	Политика управления активами корпорации Майкрософт была разработана и внедрена с учетом критериев, специфичных для Microsoft Online Services, и служит дополнением к используемым нами стандартам. Данные критерии включают технологические активы, компоненты инфраструктуры и технологии служб Microsoft Online Services. Документ «Security of equipment off-premises» (Защита удаленного оборудования) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 9.2.5. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
FS-08 **Безопасность помещений — управление активами**	Должна проводиться полная инвентаризация критически важных активов, сопровождаемая определением и документированием владения.	Группа Microsoft Online Services внедрила официальную политику, требующую учета активов, используемых для предоставления служб Microsoft Online Services, и назначения этим активам владельца. Инвентаризация основных активов оборудования в среде Microsoft Online Services проводится с помощью средства управления активами, принадлежащего группе Global Foundation Services (GFS). Владельцы активов отвечают за поддержку актуальности информации об этих активах в инвентаризации, включая информацию о владельце или связанном с активом агенте, сведения о расположении и категории безопасности. Владельцы активов также отвечают за классификацию и поддержку защиты этих активов в соответствии с надлежащими стандартами. Документ «Asset management» (Управление активами) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 7. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с HR-01 по HR-03

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
HR-01 **Кадровая безопасность — проверка биографии**	Все соискатели на должности в организации, подрядчики и третьи стороны должны проходить проверку биографии в соответствии с местным законодательством, этическими нормами и закрепленными в контракте ограничениями, которая пропорциональна категории данных, к которой они будут иметь доступ, бизнес-требованиям и приемлемому риску.	Корпорация Майкрософт требует, чтобы все новые штатные сотрудники (ЭПЗ) в США успешно проходили стандартную проверку биографии в рамках процесса приема на работу. Проверки биографии включают среди прочего исследование информации об образовании, опыте работы и возможном криминальном прошлом соискателя. Субподрядчики, имеющие доступ к определенным классам данных заказчиков, прежде чем получить доступ к данным заказчиков, также обязаны пройти проверку биографии. Кроме того, может потребоваться дополнительная информация и проверка биографии при запросе доступа к федеральной среде. Для защиты конфиденциальности сотрудников корпорация Майкрософт не открывает заказчикам результаты проверок биографии. Процесс проверки проводится отделом по работе с персоналом корпорации Майкрософт.
HR-02 **Кадровая безопасность — трудовое соглашение**	Прежде чем получить физический или логический доступ к помещениям, системам или данным, сотрудники, подрядчики, третьи стороны и заказчики должны подписать договор найма или оказания услуг, ясно определяющий ответственность сторон за информационную безопасность.	Сотрудники корпорации Майкрософт участвуют в программе обучения мерам безопасности, спонсируемой группой Microsoft Online Services, и при необходимости получают периодические обновления информации о мерах безопасности. Обучение мерам безопасности представляет собой непрерывный процесс и регулярно проводится в целях минимизации рисков. Кроме того, контракты сотрудников корпорации Майкрософт включают соглашение о неразглашении. Все сотрудники подрядчиков Microsoft Online Services должны проходить обучение, подходящее для их роли и предоставляемых служб. Документы «Roles and responsibilities» (Роли и ответственность) и «Information security awareness, education and training» (Информирование, обучение и тренинг по мерам безопасности) подпадают под действие стандарта ISO 27001, а именно Приложения A, части 8. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
HR-03 **Управление персоналом — увольнение сотрудника**	Роли и ответственность при последующем прекращении работы по найму или изменения в процедурах принятия на работу должны быть определены, задокументированы и объявлены.	Корпоративная политика управления персоналом Майкрософт определяет процессы прекращения работы по найму. Мы не создаем учетных записей заказчиков; заказчик создает учетные записи либо непосредственно в центре управления Microsoft Online, либо в локальной службе Active Directory, где учетные записи можно синхронизировать со службами Microsoft Online Services. Поэтому заказчики самостоятельно несут ответственность за достоверность сведений в созданных ими учетных записях.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-01 по IS-02

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-01 **Защита информации — программа менеджмента**	Должна быть разработана, задокументирована, утверждена и внедрена программа менеджмента информационной безопасности (ПМИБ), включающая административные, технические и физические меры безопасности для защиты активов и данных от утери, неправильного использования, несанкционированного доступа, разглашения, изменения и уничтожения. Эта программа безопасности в зависимости от характеристик конкретного бизнеса должна распространяться среди прочего на следующие области: • Управление рисками. • Политика безопасности. • Организация защиты информации. • Управление активами. • Кадровая безопасность. • Физическая защита и защита среды. • Управление операциями и связями. • Управление доступом. • Приобретение, разработка и обслуживание информационной системы.	Общая система СМИБ служб Microsoft Online Services разработана и внедрена для использования передовых методов отрасли в области безопасности, конфиденциальности и рисков. Документы «Establishing and managing the ISMS» (Внедрение и управление СМИБ) и «Organization of information security» (Организация защиты информации) подпадают под действие стандарта ISO 27001, а именно Статьи 4.2 и Приложения A, части 6. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-02 **Защита информации — поддержка и привлечение руководства**	Среднее и высшее руководство должно предпринимать официальные действия, направленные на защиту информации, с помощью ясных задокументированных распоряжений, обязательств, точно сформулированных заданий и проверки их исполнения.	Каждая утвержденная руководством версия политики защиты информации и все ее последующие обновления рассылаются всем заинтересованным лицам. Политика защиты информации доступна для ознакомления всем новым и существующим сотрудникам группы Microsoft Online Services. Все сотрудники Microsoft Online Services подтверждают, что они ознакомились с принципами, описанными в документах политики защиты информации, и согласны придерживаться этих принципов. Персонал подрядчиков Microsoft Online Services также соглашается следовать соответствующим принципам политики защиты информации. В случае если одна из сторон по какой-либо причине не имеет доступа к этой политике, надзирающий агент корпорации Майкрософт отвечает за предоставление ей материалов. Предназначенная для заказчиков версия политики защиты информации может быть предоставлена по запросу. Для получения копии политики защиты информации существующие и потенциальные заказчики должны подписать соглашение о неразглашении или равнозначный ему документ. Документы «Management Commitment to Information Security» (Обязательства руководства по защите информации) и «Management Responsibility» (Обязанности по руководству персоналом) подпадают под действие стандарта ISO 27001, а именно Статьи 5 и Приложения A, части 6.1.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерий IS-03

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-03 **Защита информации — политика**	Руководство должно утвердить документ официальной политики защиты информации, опубликовать его и ознакомить с ним сотрудников, подрядчиков и других заинтересованных лиц. Политика защиты информации должна задавать направление организации и ориентироваться на передовые методы и нормы, а также на федеральные, местные и международные законы. Политика защиты информации должна быть подкреплена стратегическим планом и программой безопасности с четким распределением ролей и указанием ответственности руководства и исполнителей.	Документ политики защиты информации подпадает под действие стандарта ISO 27001, а именно Приложения A, части 5.1.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы. Для получения дополнительных сведений см. критерий IS-02.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерий с IS-04 по IS-06

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-04 **Защита информации — основные требования**	Должны быть внедрены основные требования безопасности, применяющиеся к проектированию и реализации создаваемых и приобретаемых приложений, баз данных, систем, сетевой инфраструктуры, а также к процессу обработки информации, в соответствии с политиками, стандартами и применимыми нормативными требованиями. Соответствие основным требованиям безопасности должно пересматриваться не реже одного раза в год или при каждом внесении значительных изменений.	Как часть общей платформы СМИБ, основные требования безопасности постоянно проверяются, улучшаются и внедряются. Документ «Information systems acquisition, development maintenance and security requirements of information systems» (Приобретение информационных систем, разработка, обслуживание и требования безопасности информационных систем) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 12. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-05 **Защита информации — проверка политики**	Руководство должно проверять политику защиты информации через запланированные интервалы времени или при изменении организации для обеспечения неизменной эффективности и точности ее работы.	Политика защиты информации Microsoft Online Services регулярно проходит процесс официальной проверки и обновления через запланированные интервалы времени, не превышающие одного года. В случае если необходимо значительное изменение требований безопасности, политика может быть пересмотрена и обновлена независимо от расписания. Документ «Review of the information security policy» (Проверка политики защиты информации) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 5.1.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-06 **Защита информации — применение политики**	Должна быть внедрена официальная дисциплинарная политика или санкции для сотрудников, нарушивших процедуры и политики безопасности. Сотрудники должны быть поставлены в известность о том, какие действия, прописанные в политиках и процедурах, могут последовать в случае нарушения.	В отношении персонала Microsoft Online Services, подозреваемого в совершении нарушений требований безопасности и (или) политики защиты информации Microsoft Online Services, равноценных нарушению правил поведения Майкрософт, должно быть проведено расследование и предприняты надлежащие дисциплинарные действия, включая увольнение. В отношении персонала подрядчиков, подозреваемого в нарушении требований безопасности и (или) политики защиты информации Microsoft Online Services, должно быть проведено официальное расследование и предприняты действия согласно контракту, которые могут включать прекращение действия этого контракта. При установлении нарушения политики персоналом Microsoft Online Services об этом извещается отдел кадров, который впоследствии отвечает за координацию дисциплинарных действий. Документ «Information security awareness, education, training and disciplinary process» (Процесс оповещения, обучения и тренинга по мерам безопасности) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 8.2.2 и 8.2.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-07 по IS-08

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-07 **Защита информации — политика доступа пользователей**	Политики и процедуры доступа пользователей должны быть задокументированы, утверждены и реализованы для предоставления и запрета обычного и привилегированного доступа к приложениям, базам данных и инфраструктуре серверов и сети в соответствии с деловыми требованиями и требованиями безопасности, соответствия и соглашений об уровне обслуживания.	Политика управления доступом является компонентом общей политики и проходит официальный процесс проверки и обновления. Доступ к активам Microsoft Online Services предоставляется на основе бизнес-требований и при авторизации владельца актива. Кроме того: • Доступ к активам предоставляется на основе принципов служебной необходимости и минимальных полномочий. • Где возможно, для распределения логического доступа к конкретной рабочей функции или сфере ответственности используется управление доступом на базе ролей, а не индивидуальное. • Политики управления физическим и логическим доступом соответствуют стандартам. Документ «Access control» (Управление доступом) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-08 **Защита информации — ограничение и авторизация доступа**	Обычный и привилегированный доступ пользователей к приложениям, системам, базам данных, сетевым конфигурациям и конфиденциальным данным и функциям должен быть ограничен и подлежать утверждению руководством.	Политика управления доступом является компонентом общей политики и проходит официальный процесс проверки и обновления. Доступ к активам Microsoft Online Services предоставляется на основе бизнес-требований и при авторизации владельца актива. Кроме того: • Доступ к активам предоставляется на основе принципов служебной необходимости и минимальных полномочий. • Где возможно, для распределения логического доступа к конкретной рабочей функции или сфере ответственности используется управление доступом на базе ролей, а не индивидуальное. • Политики управления физическим и логическим доступом соответствуют стандартам. Документ «User access management and privilege management» (Управление доступом пользователей и привилегиями) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-09 по IS-11

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-09 **Защита информации — запрет доступа пользователей**	Запрет или изменение доступа пользователей к информационным системам, активам и данным должны своевременно осуществляться при каждом изменении статуса сотрудников, подрядчиков, заказчиков, деловых партнеров или третьих сторон. Под изменением статуса понимается в том числе прекращение работы по найму, расторжение контракта или соглашения, смена должности или перевод на другую позицию в организации.	Руководители, владельцы приложений и данных отвечают за контроль лиц, имеющих периодический доступ. Средства проверки доступа хранятся в сети во многих экземплярах. Аудит регулярного доступа выполняется для подтверждения надлежащего предоставления доступа. Документ «Removal of access rights» (Удаление прав доступа) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 8.3.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-10 **Защита информации — анализ доступа пользователей**	Все уровни доступа пользователей должны проверяться руководством через запланированные интервалы времени и документироваться. При обнаружении нарушений доступа должно последовать задокументированное исправление политик и процедур управления доступом.	Руководители и владельцы приложений и данных отвечают за контроль лиц, имеющих периодический доступ. Средства проверки доступа хранятся в сети во многих экземплярах. Microsoft Online предоставляет расширенные возможности, позволяющие заказчикам проверять и предоставлять конечным пользователям доступ в пределах службы. Для получения более подробной информации ознакомьтесь с соответствующими описаниями служб. Документ «User access management and privilege management» (Управление доступом пользователей и привилегиями) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-11 **Защита информации — обучение и оповещение**	Программа оповещения и обучения мерам безопасности должна функционировать для всех подрядчиков, сторонних пользователей и сотрудников организации и являться обязательной в отдельных случаях. Все лица с доступом к данным организации должны получать необходимое обучение и регулярные обновления процедур, процессов и политик организации, относящихся к функциям этих лиц в организации.	Сотрудники корпорации Майкрософт участвуют в программе обучения мерам безопасности, спонсируемой группой Microsoft Online Services, и при необходимости получают периодические обновления информации о мерах безопасности. Обучение мерам безопасности представляет собой непрерывный процесс и регулярно проводится в целях минимизации рисков. Все сотрудники подрядчиков Microsoft Online Services должны проходить обучение, подходящее для их роли и предоставляемых служб. Документ «Information security awareness, education and training» (Информирование, обучение и тренинг по мерам безопасности) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 8.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-12 по IS-14

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-12 **Защита информации — отраслевые знания и сравнение эффективности**	Для поддержки отраслевых знаний о безопасности и оценки эффективности должны организовываться сети и форумы специалистов по безопасности, а также профессиональные сообщества.	Корпорация Майкрософт является членом нескольких отраслевых организаций и посылает на профессиональные мероприятия своих сотрудников не только в качестве слушателей, но и в качестве лекторов. Кроме того, корпорация проводит несколько видов внутреннего обучения. Документ «Contact with special interest groups» (Контакт со специальными группами по интересам) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 6.1.7. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-13 **Защита информации — роли и ответственность**	Роли и ответственность подрядчиков, сотрудников и сторонних пользователей, имеющие отношение к активам и защите информации, должны быть задокументированы.	Одной из функций политики защиты информации Microsoft Online Services является обеспечение персонала Microsoft Online Services и персонала подрядчиков текущим набором ясных и кратких политик защиты информации. Эти политики определяют стратегию защиты в Microsoft Online Services. Политика создавалась как часть общей системы менеджмента информационной безопасности (СМИБ) для Microsoft Online Services. Она проверена, одобрена и утверждена руководством Microsoft Online Services. Документ «Roles and responsibilities of contractors, employees and third party users» (Роли и ответственность подрядчиков, сотрудников и сторонних пользователей) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 8.1. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-14 **Защита информации — надзор со стороны руководства**	Руководители отвечают за объявление и следование политикам, процедурам и стандартам защиты в подконтрольной им области.	Каждая утвержденная руководством версия политики и все ее последующие обновления рассылаются всем заинтересованным лицам. Эта политика доступна для ознакомления всем новым и существующим сотрудникам группы Microsoft Online Services. Все сотрудники Microsoft Online Services подтверждают, что они ознакомились с принципами, описанными в документах политики защиты информации, и согласны придерживаться этих принципов. Персонал подрядчиков Microsoft Online Services также соглашается следовать соответствующим принципам этой политики. В случае если одна из сторон по какой-либо причине не имеет доступа к этой политике, надзирающий агент корпорации Майкрософт отвечает за предоставление ей материалов. Документы «Management responsibility» (Обязанности по руководству персоналом) и «Management commitment to information security and responsibilities» (Обязательства руководства по защите информации и ответственность) подпадают под действие стандарта ISO 27001, а именно Статьи 5 и Приложения A, части 6.1. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-15 по IS-17

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-15 **Защита информации — разделение обязанностей**	Должны применяться политики, процессы и процедуры для обеспечения и усиления разделения обязанностей. Для случаев, когда существует ограничение на конфликт интересов «пользователь — роль», должны применяться технические средства контроля для снижения рисков несанкционированного или ненамеренного изменения или неправильного использования информационных активов организации.	От персонала служб Office 365, разрабатывающего и применяющего отдельные службы внешнего размещения, требуется соблюдение принципа разделения обязанностей. Это выражается в контроле доступа к исходному коду, серверам построения и производственной среде. Например: • Доступ к производственной среде служб Office 365 дается только эксплуатирующему персоналу. Команды разработки и тестирования могут получить доступ к этой информации изнутри производственной среды для участия в устранении неполадок. • Доступ к исходному коду служб Office 365 дается только разработчикам; эксплуатирующий персонал не может вносить изменения в код. Прежде чем сдать серверы в эксплуатацию в многопользовательской среде, персонал Майкрософт выполняет их построение. Когда построение сервера закончено, разрешения выполнившей его команды отменяются. С момента сдачи сервера в эксплуатацию существует ограниченное количество путей получения разрешений на доступ к системе этого сервера. Персонал службы поддержки может получить доступ непосредственно в результате запроса в службу поддержки, требующего входа в систему или ее обновления для установки ПО или разрешения проблемы. В таких случаях журнал аудита показывает, кто и когда входил в систему. Применяемые процессы соответствуют имеющимся у нас сертификациям. Разделение обязанностей внедряется в средах Microsoft Online Services для конфиденциальных и (или) критически важных функций, чтобы минимизировать риск подделки, неправильного использования или ошибки. Документ «Segregation of duties» (Разделение обязанностей) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.1.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-16 **Защита информации — ответственность пользователя**	Пользователям должно быть известно, что они ответственны за: • поддержание осведомленности и соответствия опубликованным политикам, процедурам и стандартам безопасности, а также применимым нормативным требованиям; • обеспечение безопасной и защищенной рабочей среды; • соблюдение требований безопасности при оставлении оборудования без присмотра.	Сотрудники корпорации Майкрософт участвуют в программе обучения мерам безопасности Microsoft Online Services и при необходимости получают периодические обновления информации о мерах безопасности. Обучение мерам безопасности представляет собой непрерывный процесс и проводится как минимум раз в год для минимизации рисков. Все сотрудники подрядчиков Microsoft Online Services должны проходить обучение, подходящее для их роли и предоставляемых служб. Документ «User responsibilities» (Ответственность пользователя) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.3. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

IS-17 **Защита информации — рабочее пространство**	Должны существовать политики и процедуры для очистки видимых документов, содержащих конфиденциальные данные, когда рабочее пространство остается без присмотра, а также для принудительного прекращения сеанса рабочей станции на время ее бездействия.	Политики Майкрософт включают технические и процедурные средства управления, в том числе в таких областях, как требования к времени ожидания сеанса. Документ «User responsibilities» (Ответственность пользователя) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.3. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-18 по IS-19

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-18 **Защита информации — шифрование**	Должны быть внедрены политики и процедуры, а также механизмы их применения для шифрования конфиденциальных данных, находящихся в хранилище (например, на серверах файлов, в базах данных и на рабочих станциях конечного пользователя), и передаваемых данных (например, данных в системных интерфейсах, общедоступных сетях и электронных сообщениях).	Шифрование выполняется на нескольких уровнях, таких как транспортный уровень, шифрование между клиентами и Exchange Online (SSL), обмен мгновенными сообщениями и федерация обмена мгновенными сообщениями. Для получения дополнительных сведений ознакомьтесь с описанием службы безопасности Office 365, доступным в Центре загрузки. Кроме того, мы поддерживаем S/MIME, службу управления правами Active Directory и PGP. Мы не шифруем данные в состоянии покоя, однако заказчик может сделать это через управление правами на доступ к данным или службу управления правами. Документ «Exchange of information» (Обмен информацией) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.8. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-19 **Защита информации — управление ключами шифрования**	Должны существовать и применяться политики, процедуры и механизмы для эффективного управления ключами для поддержки шифрования хранимых и передаваемых данных.	Шифрование выполняется на нескольких уровнях, таких как транспортный уровень, шифрование между клиентами и Exchange Online (SSL), обмен мгновенными сообщениями и федерация обмена мгновенными сообщениями. Для получения дополнительных сведений ознакомьтесь с описанием службы безопасности Office 365, доступным в Центре загрузки. Кроме того, мы поддерживаем S/MIME, службу управления правами Active Directory и PGP. Мы не шифруем данные в состоянии покоя, однако заказчик может сделать это через управление правами на доступ к данным или службу управления правами. Документ «Media Handling» (Обращение с носителями информации) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.7.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерий IS-20

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-20 **Защита информации — контроль уязвимостей и исправлений**	Должны существовать и применяться политики, процедуры и механизмы контроля уязвимостей и исправлений, обеспечивающие оценку уязвимостей приложений, системы и сетевых устройств и своевременное применение исправлений безопасности от подрядчиков на основе оценки рисков при назначении приоритетов критически важным исправлениям.	Группа Microsoft Online Services внедряет технологии проверки среды на уязвимости. Выявленные уязвимости отслеживаются и проверяются для исправления. Кроме того, организация по управлению рисками регулярно выполняет официальную оценку уязвимостей и проникновений для выявления уязвимостей и определения эффективности работы логических средств управления ключами. Результаты доступны в регулярно публикуемых отчетах. Группа Microsoft Online Services имеет подписку на службу Microsoft Security Response и постоянно отслеживает внешние сайты, информирующие об уязвимостях безопасности. В рамках обычного процесса контроля уязвимостей в Microsoft Online Services проводится оценка обнаруженных уязвимостей и при необходимости выполняются действия для снижения рисков. Microsoft Security Response Center (MSRC) выпускает бюллетень безопасности во второй вторник каждого месяца («Вторник исправлений») или при необходимости в нейтрализации эксплойтов нулевого дня. В случае если экспериментальный код общедоступен с точки зрения возможного эксплойта или если выпущено новое критически важное исправление безопасности, группа Microsoft Online Services должна как можно скорее применить исправления затронутых систем Microsoft Online Services для немедленного устранения уязвимости в среде заказчика. В этом окне оперативная группа Microsoft Online Services обновляет или исправляет все применимые устройства Microsoft Online Services, что может вызвать короткий перерыв в работе служб, длящийся, как правило, не больше 10 минут, пока идет перезагрузка серверов или восстановление кластеров. Документ «Control of technical vulnerabilities» (Контроль технических уязвимостей) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 12.6. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-21 по IS-22

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-21 **Защита информации — антивирусное и антивредоносное ПО**	Убедитесь, что антивирусные программы способны выявлять и удалять все известные типы вредоносного и несанкционированного ПО с помощью обновлений антивирусных сигнатур, наличие которых должно проверяться не реже чем раз в 12 часов.	В службах Microsoft Online Services используется несколько уровней антивредоносного ПО, чтобы обеспечить защиту от вредоносных программ. Например, на серверах в среде Microsoft Online работают программы, сканирующие входящие файлы на вирусы. Кроме того, на почтовых серверах Microsoft Exchange работает дополнительное антивирусное ПО, проверяющее сообщения электронной почты на наличие вредоносных программ. Более подробные сведения можно найти в описании соответствующих служб и в соглашении об уровне обслуживания. Корпорация Майкрософт имеет свой центр реагирования на вопросы безопасности, Security Response Center (MSRC), который также предоставляет нашим заказчикам информацию по всему диапазону продуктов Майкрософт. Дополнительные сведения можно найти на веб-сайте http://www.microsoft.com/security/msrc/default.aspx. Документ «Protection against malicious code» (Защита от вредоносного кода) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.4. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-22 **Защита информации — реагирование на инциденты**	Должны существовать политики, процессы и процедуры для рассмотрения событий, связанных с безопасностью, и своевременного, тщательного реагирования на инциденты.	В Microsoft Online был разработан надежный процесс, позволяющий обеспечить скоординированную реакцию на каждый инцидент. Инциденты, связанные с безопасностью, могут включать среди прочего следующие примеры: почтовые вирусы, вредоносное ПО, вирусы-черви, атаки типа «отказ в обслуживании», неавторизованный доступ и любой другой вид несанкционированных или незаконных действий, затрагивающий компьютерные сети или оборудование для обработки данных Microsoft Online. Процесс реагирования состоит из следующих действий: идентификация, ограничение распространения, устранение, восстановление, выводы. Документ «Security incident response plans» (Планы реагирования на инциденты безопасности) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 13.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерий IS-23

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-23 **Защита информации — отчеты об инцидентах**	Подрядчики, сотрудники и сторонние пользователи должны быть оповещены об обязанности своевременно сообщать о любых событиях, связанных с информационной безопасностью. О таких событиях нужно немедленно и любыми возможными способами сообщать через предварительно определенные каналы связи в соответствии с нормативными, регулятивными и закрепленными в контракте требованиями.	Персонал группы Microsoft Online Services и подрядчиков обязан немедленно сообщать обо всех инцидентах, слабых местах и случаях неправильной работы Microsoft Online Services. При создании таких отчетов и обработке событий сотрудники следуют предписанным процедурам в соответствии с существующей политикой. В Microsoft Online был разработан надежный процесс, позволяющий обеспечить скоординированную реакцию на каждый инцидент. Событием, связанным с безопасностью, помимо прочего, может быть незаконный доступ к данным заказчика, хранящимся в нашей среде или в нашем помещении, и несанкционированный доступ, приведший к потере, разглашению или изменению данных заказчика. Процесс реагирования на инциденты безопасности Microsoft Online состоит из следующих этапов: • Идентификация. Сбор, корреляция и анализ системных предупреждений и предупреждений безопасности. События изучаются оперативными организациями и организациями по безопасности Microsoft Online. Если в событии сообщается о проблеме, связанной с безопасностью, ему назначают категорию серьезности и передают уполномоченной группе в корпорации. Эта группа включает специалистов по продукту, безопасности и технике. • Ограничение распространения. Команда специалистов оценивает область, затронутую инцидентом, и его влияние. В первую очередь группа эскалации должна убедиться, что инцидент локализован и данные в безопасности. Группа эскалации определяет реакцию, выполняет необходимое тестирование и вносит изменения. В случаях, требующих более глубокого изучения, содержимое собирают из соответствующих систем с помощью наилучших криминалистических программ и передовых методов отрасли. • Устранение. После того как ситуация локализована, группа эскалации переходит к устранению ущерба, вызванного нарушением безопасности, и определяет коренную причину возникновения проблемы. Если определена уязвимость, группа эскалации сообщает о проблеме разработчикам продукта. • Восстановление. Во время восстановления к системе применяются обновления ПО или конфигурации, а службы возвращаются к нормальному рабочему режиму. • Выводы. Каждый инцидент, связанный с безопасностью, анализируется, чтобы обеспечить необходимые меры, исключающие повторение проблемы в будущем. Документ «Reporting security weaknesses and responsibilities and procedures» (Отчеты об ослаблении безопасности, ответственность и процедуры) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 13.1.2 и 13.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-24 по IS-26

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-24 **Защита информации — юридическая подготовка реакции**	В случае если после инцидента, связанного с информационной безопасностью, в отношении лиц или организаций потребуются дальнейшие действия юридического характера, для сбора, хранения и представления свидетельств должны быть выполнены надлежащие криминалистические процедуры, включая охрану вещественных доказательств, необходимые для поддержки юридических действий согласно законодательству.	В рамках этапа «Ограничение распространения» процесса реагирования на инциденты безопасности группа эскалации должна в первую очередь убедиться, что инцидент локализован и данным ничто не угрожает. Группа эскалации определяет реакцию, выполняет необходимое тестирование и вносит изменения. В случаях, требующих более глубокого изучения, содержимое собирают из соответствующих систем с помощью наилучших криминалистических программ и передовых методов отрасли. Документ «Security incident response plans and collection of evidence» (Планы реагирования на инциденты безопасности и сбор доказательств) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 13.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-25 **Защита информации — показатели реакции на инцидент**	Должны существовать механизмы для отслеживания и подсчета типов инцидентов в сфере информационной безопасности, их объемов и связанных с ними затрат.	На начальном этапе инцидента организация по управлению рисками анализирует инциденты, чтобы оценить их серьезность. Это делается в сотрудничестве с представителями владельцев затронутой инцидентом собственности. Точная оценка серьезности инцидента помогает группе в определении широты его связей и формировании стратегии реагирования. Оценка критичности инцидента может меняться по мере поступления дополнительной информации в процессе расследования. Персонал по управлению инцидентами безопасности отвечает за обновление оценки серьезности и оповещение заинтересованных лиц об изменениях. Документ «Management information security incidents and learning from information security incidents» (Управление инцидентами информационной безопасности и выводы из инцидентов информационной безопасности) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 13.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-26 **Защита информации — допустимое использование**	Должны существовать политики и процедуры для допустимого применения информационных активов.	Политика прав на использование продуктов была разработана и внедрена для дополнения стандарта допустимого использования критериями, специфичными для служб Microsoft Online Services. Данные критерии включают технологические активы, компоненты инфраструктуры и технологии служб Microsoft Online Services. Политика прав на использование продуктов доступна на сайте http://www.microsoft.com/licensing/pur/products.aspx. Документ «Acceptable use» (Допустимое применение) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 7.1.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-27 по IS-29

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-27 **Защита информации — возврат активов**	Сотрудники, подрядчики и сторонние пользователи должны возвращать все активы, принадлежащие организации, в определенные и задокументированные сроки после прекращения действия контракта или договора о найме.	Сотрудники, подрядчики и сторонние пользователи официально уведомляются о требовании уничтожить или вернуть, в зависимости от обстоятельств, любые физические материалы, предоставленные им корпорацией Майкрософт во время действия контракта или договора о найме, и удалить электронные носители данных из инфраструктуры подрядчиков или третьих сторон. Корпорация Майкрософт также может провести аудит, чтобы удостовериться, что данные удалены надлежащим образом. Документ «Return of assets» (Возврат активов) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 8.3.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-28 **Защита информации — электронные транзакции**	Данные об электронной коммерции, передаваемые по общедоступным сетям, должны быть надлежащим образом классифицированы и защищены от мошеннической деятельности, несанкционированного разглашения и изменения, чтобы предотвратить споры по контракту и разглашение данных.	Office 365 не является решением для электронной коммерции. Однако данные все равно шифруются на нескольких уровнях, таких как транспортный уровень, шифрование между клиентами и Exchange Online (SSL), обмен мгновенными сообщениями и федерация обмена мгновенными сообщениями. Для получения дополнительных сведений ознакомьтесь с описанием службы безопасности Office 365, доступным в Центре загрузки. Кроме того, мы поддерживаем S/MIME, службу управления правами Active Directory и PGP.
IS-29 **Защита информации — доступ к средствам аудита**	Доступ к средствам аудита, взаимодействующим с информационными системами организаций, а также использование этих средств должны быть надлежащим образом разграничены и взяты под контроль во избежание раскрытия и неправильного использования данных журнала.	Модель делегированного управления дает администраторам только тот доступ, который им необходим для выполнения специальных задач, что сокращает вероятность совершения ошибки и открывает доступ к системам и функциям только тогда, когда это необходимо. В группе Microsoft Online Services существуют официальные процессы мониторинга, определяющие частоту проверок для стандартных рабочих процедур, а также процессы и процедуры надзора за проверками. Документ «Protection of information systems audit tools and protection of log information» (Средства для аудита защиты информационных систем и защита информации журнала) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 15.3.2 и 10.10.3. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-30 по IS-31

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-30 **Защита информации — доступ к портам диагностики и конфигурации**	Пользовательский доступ к портам диагностики и конфигурации должен предоставляться только авторизованным лицам и приложениям.	Политика управления доступом является компонентом общей политики и проходит официальный процесс проверки и обновления. Доступ к активам Microsoft Online Services предоставляется на основе бизнес-требований и при авторизации владельца актива. Кроме того: • Доступ к активам предоставляется на основе принципов служебной необходимости и минимальных полномочий. • Где возможно, для распределения логического доступа к конкретной рабочей функции или сфере ответственности используется управление доступом на базе ролей, а не индивидуальное. • Политики управления физическим и логическим доступом соответствуют стандартам. Службы Microsoft Online Services контролируют физический доступ к портам диагностики и конфигурации через описанные физические средства управления центра обработки данных и путем поддержки процедур управления физическим доступом к порту. Порты диагностики и конфигурации доступны только по договоренности между владельцем службы или актива и запрашивающим доступ персоналом поддержки ПО или оборудования. Порты, службы и устройства, установленные на компьютере или сетевом устройстве, которые не требуются для выполнения конкретных бизнес-функций, отключаются или удаляются. Документ «Network controls access controls» (Средства управления доступом к управлению сетью) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 10.6.1, 11.1.1 и 11.4.4. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-31 **Защита информации — сетевые и инфраструктурные службы**	Внутренние и внешние соглашения об уровне обслуживания сети и инфраструктуры должны четко документировать средства управления безопасностью, уровни обслуживания и производственной мощности, а также деловые требования и требования заказчика.	Управление мощностями происходит следующим образом. Упреждающий мониторинг непрерывно оценивает производительность ключевых систем платформы служб Office 365 по сравнению с установленными границами допустимой производительности и доступности служб. При достижении порогового значения или возникновении нестандартного события система мониторинга создает предупреждения для оперативного персонала со ссылкой на это значение или событие. Безопасность. Сети в центрах обработки данных Office 365 разработаны для создания нескольких отдельных сетевых сегментов в каждом центре обработки данных. Такое деление на сегменты позволяет физически отделить наиболее важные внутренние серверы и устройства хранения от общедоступных интерфейсов. Документ «Addressing security in third party agreements and security of network services» (Безопасность адресации в соглашениях третьих сторон и безопасность сетевых служб) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 6.2.3 и 10.6.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с IS-32 по LG-01

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
IS-32 **Защита информации — мобильные устройства**	Должны разрабатываться и применяться политики, процедуры и меры, строго ограничивающие доступ к конфиденциальным данным с портативных и мобильных устройств, таких как ноутбуки, сотовые телефоны и КПК, использовать которые, как правило, менее безопасно, чем стационарные устройства (например, настольные компьютеры и оборудование организации).	Не разрешается входить с мобильных устройств (ноутбуков, смартфонов и т. д.) в производственные среды Microsoft Online Services или напрямую подключать такие устройства к этим средам, если только использование устройства не одобрено руководством служб Microsoft Online Services. Office 365 поддерживает доступ заказчиков к службам через ряд мобильных устройств. В таких обстоятельствах заказчик несет ответственность за соблюдение политик и адекватную защиту конечной точки. Документ «Access control to mobile computing and communications» (Управление доступом для мобильных устройств) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.7.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-33 **Защита информации — ограничение доступа к исходному коду**	Доступ к исходному коду приложения, программы или объекта должен предоставляться только авторизованному персоналу исходя из служебной необходимости. При этом должны указываться лицо, предоставившее доступ, причина для доступа и версия исходного кода, к которой был выдан доступ.	Доступ к библиотекам исходного кода Microsoft Online Services дается только авторизованному персоналу и подрядчикам Microsoft Online Services. Когда это возможно, библиотеки исходного кода используют раздельные рабочие области для не связанных между собой проектов. Персонал группы Microsoft Online Services и подрядчиков получает доступ только к тем рабочим областям, которые необходимы для выполнения служебных обязанностей. Ведется журнал аудита, в котором отражаются изменения, вносимые в библиотеку исходного кода. Документ «Access control and access control to program source code» (Управление доступом и контроль доступа к исходному коду) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 11 и 12.4.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
IS-34 **Защита информации — доступ к специальным программам**	Доступ к специальным программам, способным переопределить средства управления системой, объектом, сетью, виртуальной машиной или приложением, должен быть ограничен.	В Active Directory существуют механизмы, которые ограничивают действия, связанные с доступом и ведением журнала. Документ «User authentication for external connections» (Проверка подлинности пользователя для внешних подключений) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.4.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
LG-01 **Юридический отдел — соглашения о неразглашении**	Требования по неразглашению или соглашения о конфиденциальности, отражающие необходимость защиты данных и информации об эксплуатации, должны формулироваться, документироваться и проверяться через запланированные интервалы времени.	Юридический и кадровый отделы корпорации Майкрософт используют политики и процедуры, определяющие внедрение и выполнение соглашений о неразглашении и конфиденциальности. Документ «Confidentiality agreements and non-disclosure agreements» (Соглашения о конфиденциальности и соглашения о неразглашении) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 6.1.5. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с LG-02 по OP-01

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
LG-02 **Юридический отдел — соглашения с третьими сторонами**	Статьи соглашений с третьими сторонами, прямо или косвенно влияющих на информационные активы или данные организаций, должны покрывать все относящиеся к делу требования безопасности. Сюда относятся соглашения, включающие обработку, доступ, обмен, размещение или управление информационными активами организации либо добавление или удаление услуг или продуктов из уже существующей информации. Положения соглашений об активах должны включать средства управления безопасностью (например, шифрование, управление доступом и предотвращение утечек) и целостностью передаваемых данных в целях предотвращения несанкционированного разглашения, изменения или уничтожения.	В стандартах группы Microsoft Online Services указано, что наша организация по управлению рисками санкционирует некоторые виды обмена данными со сторонами, не входящими в Microsoft Online Services. В рамках этого процесса организация по управлению рисками следит за тем, чтобы обмен активами, имеющими высокое и среднее влияние на бизнес, со сторонами, не входящими в корпорацию Майкрософт, производился только в соответствии с официальными процедурами. Документ «Addressing security in third party agreements» (Безопасность адресации в соглашениях третьих сторон) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 6.2.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
OP-01 **Управление операциями — политика**	Политики и процедуры должны разрабатываться и становиться доступными всему персоналу для адекватной поддержки роли операций служб.	В соответствии с политикой корпорации Майкрософт, менеджеры по кадрам, прежде чем заниматься набором персонала, проводить собеседования и нанимать служащих, должны определить требования к рабочим заданиям. Требования к заданиям включают основную ответственность и задачи, относящиеся к рабочим обязанностям, базовые характеристики, необходимые для выполнения работы, и необходимые личные характеристики. Когда требования определены, менеджеры создают описание работы, которое представляет собой ее профиль и используется для определения потенциальных соискателей. Когда подходящие соискатели определены, начинается проведение собеседований для оценки соискателей и принятия оптимального решения о найме. Документ «Information security policy» (Политика защиты информации) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 5.1. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с OP-02 по OP-04

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
OP-02 **Управление операциями — документация**	Документация к информационным системам (например, руководства пользователя и администратора, схемы архитектуры и т. д.) должна быть доступна авторизованному персоналу в целях обеспечения: • настройки, установки и эксплуатации информационной системы; • эффективного использования функций безопасности системы.	Стандартные рабочие процедуры официально задокументированы и утверждены руководством группы Microsoft Online Services. Эти процедуры проверяются как минимум раз в год. Группа Microsoft Online Services обеспечивает доступность подробных материалов руководств, обучения, справки и устранения неполадок в рамках службы Office 365. На портале администрации есть ссылки на многие из доступных ресурсов, включая следующие: • справочные статьи для пользователей и администраторов, которым требуется управлять службой Office 365; • видеоматериалы для администраторов Exchange; • статьи и шаги, необходимые для конфигурации гибридных сред; • форумы и вики-страницы, на которых публикуются справочные статьи и техническая документация; • панель мониторинга работоспособности службы для получения информации о простоях и проблемах. Документ «Documented operating procedures and security of system documentation» (Документированные рабочие процедуры и безопасность документации системы) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 10.1.1 и 10.7.4. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
OP-03 **Управление операциями — планирование мощностей и ресурсов**	Доступность, качество, а также адекватные мощность и ресурсы должны быть спланированы, подготовлены и измерены для обеспечения необходимой производительности системы согласно нормативным, закрепленным в контракте и бизнес-требованиям. Должно выполняться прогнозирование будущих требований к производительности для снижения риска перегрузки системы.	В Майкрософт существуют следующие эксплуатационные процессы: упреждающее управление мощностью на основе определенных пороговых значений или событий, мониторинг подсистем ПО и оборудования для допустимой производительности и доступности служб, использование ЦП, использование служб, использование хранилищ и задержка в сети. Документ «Capacity management» (Управление мощностью) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.3.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
OP-04 **Управление операциями — техническое обслуживание оборудования**	Должны существовать политики и процедуры для технического обслуживания оборудования, обеспечивающие непрерывность и доступность работы.	Для среды служб Microsoft Online Services существует процесс разработки и обслуживания управления непрерывностью служб (SCM). Этот процесс включает стратегию восстановления активов Microsoft Online Services и возобновления ключевых бизнес-процессов Microsoft Online Services. Решение для обеспечения непрерывности отражает требования безопасности, соответствия и конфиденциальности производственной среды службы в другом узле. Документ «Equipment maintenance» (Техническое обслуживание оборудования) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 9.2.4. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с RI-01 по RI-03

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
RI-01 **Управление рисками — программа**	Организации должны разрабатывать и поддерживать инфраструктуру управления рисками предприятия, чтобы управлять рисками на допустимом уровне.	В службах Microsoft Online Services применяется цикл ISO «планирование, выполнение, проверка, управление» (PDCA) для непрерывной поддержки и улучшения инфраструктуры управления рисками. Документ «Establishing the ISMS and risk management framework» (Внедрение СМИБ и инфраструктура управления рисками) подпадает под действие стандарта ISO 27001, а именно части 4.2.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RI-02 **Управление рисками — оценка**	Оценка связана с общей инфраструктурой предприятия. Официальные оценки риска должны выполняться не реже одного раза в год либо через запланированные интервалы времени и определять вероятность и влияние всех выявленных рисков с помощью качественных и количественных методов. Вероятность и влияние, связанные с неотъемлемыми и остаточными рисками, должны определяться независимо, с учетом всех категорий рисков (например, результатов аудита, анализа угроз и уязвимостей, а также соблюдения регулятивных норм).	Инфраструктура оценки рисков организации по управлению рисками Microsoft Online Services основана на стандартах ISO 27001. Интегрированной частью методологии является процесс оценки рисков. Этап оценки потенциальных рисков начинается с выявления риска, определения уровня риска в зависимости от вероятности его возникновения и от его влияния и, наконец, определения мер безопасности и средств контроля, сокращающих влияние риска до допустимого уровня. Существуют также надлежащие меры, рекомендации и средства управления для максимально возможного снижения рисков. Документ «Establishing and managing the ISMS» (Внедрение и управление СМИБ) подпадает под действие стандарта ISO 27001, а именно Статьи 4.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RI-03 **Управление рисками — снижение и принятие**	Риски должны быть снижены до приемлемого уровня. Приемлемые уровни, основанные на критериях рисков, должны быть определены и задокументированы с учетом разумных сроков разрешения и при утверждении руководства.	Инфраструктура оценки рисков организации по управлению рисками Microsoft Online Services основана на стандартах ISO 27001. Интегрированной частью методологии является процесс оценки рисков. Этап оценки потенциальных рисков начинается с выявления риска, определения уровня риска в зависимости от вероятности его возникновения и от его влияния и, наконец, определения мер безопасности и средств контроля, сокращающих влияние риска до допустимого уровня. Существуют также надлежащие меры, рекомендации и средства управления для максимально возможного снижения рисков. Документ «Establishing and managing the ISMS» (Внедрение и управление СМИБ) подпадает под действие стандарта ISO 27001, а именно Статьи 4.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерии с RI-04 по RI-05

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
RI-04 **Управление рисками — влияние изменений бизнеса и политики**	Результаты оценки рисков должны включать обновление политик безопасности, процедур, стандартов и средств управления для поддержки их актуальности и эффективности.	Решения об обновлении политик и процедур принимаются на основе отчетов об оценке рисков. Оценки рисков регулярно пересматриваются на основе заданного расписания и изменений в ситуации с рисками. Документ «Establishing the ISMS and risk management framework» (Внедрение СМИБ и инфраструктура управления рисками) подпадает под действие стандарта ISO 27001, а именно Статьи 4.2.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RI-05 **Управление рисками — доступ третьих сторон**	После идентификации, оценки и присвоения приоритетов рискам, возникающим в бизнес-процессах, требующих доступа третьих сторон к информационным системам и данным организации, должно следовать скоординированное применение ресурсов для минимизации, мониторинга и измерения вероятности и влияния неавторизованного или нецелесообразного доступа. Компенсирующие меры, полученные в результате анализа рисков, должны быть внедрены до открытия доступа.	Политика управления доступом является компонентом общей политики и проходит официальный процесс проверки и обновления. Доступ к активам Microsoft Online Services предоставляется на основе бизнес-требований и при авторизации владельца актива. Кроме того: • Доступ к активам предоставляется на основе принципов служебной необходимости и минимальных полномочий. • Где возможно, для распределения логического доступа к конкретной рабочей функции или сфере ответственности используется управление доступом на базе ролей, а не индивидуальное. • Политики управления физическим и логическим доступом соответствуют стандартам. Документ «Identification of risks related to external parties and access control» (Определение рисков, связанных со внешними сторонами, и управление доступом) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 6.2.1 и 11. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с RM-01 по RM-02

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
RM-01 **Управление выпусками — разработка с нуля и приобретение**	Должны существовать политики и процедуры для получения разрешений от руководства на разработку или приобретение новых приложений, систем, баз данных, инфраструктур, служб, операций и оборудования.	Для изменений в службах Microsoft Online Services и системных изменений существует процедура контроля изменений во время эксплуатации. Эта процедура включает процесс проверки и утверждения руководством группы Microsoft Online Services. С процедурой контроля изменений должны быть ознакомлены все стороны (Microsoft Online Services и третьи стороны), занимающиеся обслуживанием систем в службах Microsoft Online Services. Процедура контроля изменений во время эксплуатации учитывает следующие действия: • определение и документирование запланированного изменения; • процесс оценки возможных последствий изменения; • тестирование изменения в утвержденной непроизводственной среде; • план оповещения об изменении; • процесс утверждения изменения руководством; • план отмены и восстановления изменения (где применимо). Заказчики за год извещаются о кардинальных изменениях и по крайней мере за пять дней — о мероприятиях планового обслуживания; однако из-за специфики многопользовательской службы заказчики не имеют возможности определять, когда будет проведено обновление. Документ «Change management» (Управление изменениями) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.1.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RM-02 **Управление выпусками — производственные изменения**	Изменения в производственной среде должны документироваться, тестироваться и утверждаться перед внедрением. Изменения производственного ПО и оборудования могут затрагивать приложения, системы, базы данных и сетевые устройства, требующие исправлений, пакетов обновлений и других видов обновления и преобразования.	См. критерий RM-01.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с RM-03 по RM-05

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
RM-03 **Управление выпусками — тестирование качества**	Для всего ПО, разрабатываемого организацией, должна действовать программа систематического мониторинга и оценки, чтобы обеспечить соответствие стандартам качества. В целях безопасности должны быть созданы и задокументированы критерии оценки и приемлемости качества для информационных систем, обновлений и новых версий, а также должно проводиться тестирование системы или систем как во время разработки, так и перед приемом в эксплуатацию. Руководство должно иметь четко определенные возможности надзора в процессе тестирования качества, в результате которого конечный продукт перед выпуском сертифицируется как «соответствующий целевому назначению» (продукт пригоден для использования в запланированных целях) и «готовый к отправке» (все ошибки устранены).	Критические контрольные точки проверки и утверждения безопасности включаются в жизненный цикл разработки системы. Определяются деловые, операционные и технические риски в таких областях, как соответствие требованиям, безопасность, конфиденциальность и непрерывность обслуживания. Будучи первопроходцем в области разработки встроенных систем безопасности, методика Security Development Lifecycle лежит в основе служб Microsoft Online Services. Дополнительные сведения см. на веб-сайте http://www.microsoft.com. Документ «Security in development and support processes» (Безопасность в процессе разработки и поддержки) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 12.5. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RM-04 **Управление выпусками — внешняя разработка**	Для всего ПО, разрабатываемого за пределами организации, должна работать программа систематического мониторинга и оценки, чтобы обеспечить соответствие стандартам качества. Внешняя разработка ПО должна происходить под наблюдением и контролем организации и включать выполнение требований безопасности, независимую проверку безопасности внешней среды сертифицированным лицом, сертифицированное обучение мерам безопасности для внешних разработчиков ПО и проверку кода. В качестве сертификации для такого контроля должна быть использована либо сертификация с аккредитацией ISO/IEC 17024, либо юридически признанная лицензия или сертификация в соответствующей законодательной юрисдикции, выбранная организацией, занимающейся внешней разработкой.	Корпорация Майкрософт применяет Security Development Lifecycle, процесс обеспечения безопасности ПО, для проектирования, разработки и внедрения служб Office 365. Методика Security Development Lifecycle помогает гарантировать надежную защиту служб связи и совместной работы даже на самом нижнем уровне. С помощью таких средств управления, как Establish Design Requirements (Разработка конструктивных требований), Analyze Attack Surface (Анализ направлений атаки) и Threat Modeling (Моделирование угроз), продукт Security Development Lifecycle помогает системам Майкрософт определять потенциальные угрозы при использовании службы и уязвимые аспекты службы, открытые для атаки. Если выявлены потенциальные угрозы на этапах проектирования, разработки или внедрения, Майкрософт может снизить вероятность атак, ограничив некоторые службы или убрав функции, без которых можно обойтись. После удаления лишних функций Майкрософт снижает потенциальные угрозы, которые могут возникнуть на этапе проверки, путем полного тестирования средств управления на этапе проектирования. Дополнительные сведения можно найти на веб-сайте http://www.microsoft.com/security/sdl. Документ «Security in development and support processes» (Безопасность в процессе разработки и поддержки) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 12.5. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RM-05 **Управление выпусками — установка ПО**	Должны существовать и применяться политики, процедуры и механизмы для ограничения установки неавторизованного ПО.	Все изменения в производстве проходят через процесс контроля изменений, описанный в положении RM-01. Программы устанавливаются на наших серверах администраторами с помощью процесса контроля изменений.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с RS-01 по RS-02

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
RS-01 **Устойчивость — программа управления**	Должны применяться политики, процессы и процедуры, определяющие непрерывность деятельности и способность к аварийному восстановлению для сокращения влияния реализовавшегося риска на организацию до приемлемого уровня и для упрощения восстановления информационных активов (что может потребоваться в результате реализации риска, например в результате стихийных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий) путем сочетания превентивных и восстановительных средств, в соответствии с регулятивными, нормативными, закрепленными в контракте и бизнес-требованиями, а также отраслевыми стандартами. Эта программа управления устойчивостью должна быть доведена до сведения всего штатного персонала, прежде чем он будет допущен к работе, а также опубликована, размещена, сохранена, записана и распространена в нескольких местах, легко доступных в случае какого-либо происшествия.	Для среды служб Microsoft Online Services существует процесс разработки и обслуживания управления непрерывностью служб (SCM). Этот процесс включает стратегию восстановления активов Microsoft Online Services и возобновления ключевых бизнес-процессов Microsoft Online Services. Решение для обеспечения непрерывности отражает требования безопасности, соответствия и конфиденциальности производственной среды службы в другом узле. Документ «Information security aspects of business continuity management» (Аспекты защиты информации в управлении непрерывностью деятельности) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 14.1. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RS-02 **Устойчивость — анализ влияния**	Должен существовать определенный и задокументированный метод оценки влияния любой остановки в работе на организацию, включающий следующие шаги: • определение критических продуктов и служб; • выявление зависимостей, затрагивающих процессы, приложения, деловых партнеров и сторонних поставщиков услуг; • понимание угроз критическим продуктам и службам; • определение влияния запланированной или незапланированной остановки и его изменения со временем; • определение максимального приемлемого периода простоя; • определение приоритетов для восстановления; • определение целевого срока восстановления для возобновления работы критических продуктов и служб, не превышающего максимального приемлемого периода простоя; • расчет количества ресурсов, необходимых для возобновления.	Анализ влияния на бизнес проводится и пересматривается с заданной периодичностью. Этот анализ включает: • определение угроз, относящихся к бизнес-среде и процессам Microsoft Online Services; • оценку выявленных угроз, включая потенциальное влияние и ожидаемый ущерб; • одобренную руководством стратегию для смягчения значительных угроз и восстановления критических бизнес-процессов. Документ «Information security aspects of business continuity management» (Аспекты защиты информации в управлении непрерывностью деятельности) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 14.1. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с RS-03 по RS-05

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
RS-03 **Устойчивость — планирование непрерывности**	Должна быть разработана, задокументирована и введена в использование единая и последовательная инфраструктура для планирования непрерывности бизнеса и разработки планов, чтобы обеспечить во всех планах по непрерывности бизнеса согласованность приоритетов обращения при тестировании и обслуживании, а также согласованность требований информационной безопасности. Требования для планов непрерывности бизнеса включают следующее: • определенную цель и область применения, учитывающую имеющиеся зависимости; • доступность и понятность для тех, кто будет пользоваться этими планами; • наличие одного или нескольких владельцев, имена которых указаны и которые отвечают за проверку, обновление и утверждение; • указание линий связи, ролей и ответственности; • подробную информацию о процедурах восстановления, описание способов решения проблем вручную и справочную информацию; • метод запуска реализации плана.	Службы Microsoft Online Services поддерживают инфраструктуру, отвечающую как отраслевым, так и корпоративным передовым практикам, что позволяет реализовывать программу непрерывности на всех уровнях. Инфраструктура Microsoft Online Services включает: • назначение ответственности за ключевые ресурсы; • процессы уведомления, эскалации и объявления; • целевой срок восстановления и целевые точки восстановления; • планы непрерывности с задокументированными процедурами; • программу обучения для подготовки всех участников к выполнению плана непрерывности; • процессы тестирования, обслуживания и проверки. Документ «Information security aspects of business continuity management» (Аспекты защиты информации в управлении непрерывностью деятельности) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 14.1. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RS-04 **Устойчивость — тестирование непрерывности**	Для обеспечения эффективности планов непрерывности бизнеса должно проводиться их тестирование через запланированные интервалы времени, а также при значительных организационных изменениях и изменениях среды.	Планы восстановления проверяются на регулярной основе с использованием передовых методов для обеспечения доступности решений при возникновении происшествий. Документ «Testing, maintaining and re-assessing business continuity plans» (Тестирование, обслуживание и пересмотр планов непрерывности бизнеса) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 14.1.5. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RS-05 **Устойчивость — риски, связанные со средой**	Должна быть предусмотрена и спланирована физическая защита от повреждений и меры противодействия при разрушениях, вызванных естественными причинами, а также преднамеренными атаками и катастрофами, включая пожар, наводнение, молнию, магнитную бурю, ураган, землетрясение, цунами, взрыв, ядерную аварию, вулканическую активность, биологическую угрозу, гражданские беспорядки, оползень, тектоническую активность и другие естественные или рукотворные бедствия.	Для защиты центров обработки данных были внедрены следующие меры по контролю за состоянием среды: • температурный контроль; • отопление, вентиляция и кондиционирование; • системы обнаружения и ликвидации пожара; • системы управления питанием. Документ «Protecting against external and environmental threats» (Защита от внешних и природных угроз) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 9.1.4. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с RS-06 по RS-08

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
RS-06 **Устойчивость — расположение оборудования**	Для снижения рисков, связанных с естественными угрозами и возможностями неавторизованного доступа, оборудование должно располагаться в достаточном удалении от мест с высокой вероятностью таких рисков и дублироваться избыточным оборудованием, находящимся на разумном расстоянии от основного.	Оборудование Microsoft Online Services расположено в средах, разработанных с учетом защиты от краж и таких естественных рисков, как огонь, дым, вода, пыль, вибрация, землетрясение и электрическое воздействие. Документ «Protecting against external and environmental threats and equipment siting protection» (Защита от внешних и природных угроз и защита размещения оборудования) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 9.1.4 и 9.2.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RS-07 **Устойчивость — сбои питания оборудования**	Должны применяться резервы и механизмы безопасности для защиты оборудования от остановки коммунального обслуживания (например, сбоев питания, отказа сетей и т. п.).	Центры обработки данных в режиме 24/7 снабжаются от специальных источников бесперебойного питания (ИБП) и оборудованы аварийной системой питания, то есть генераторами. Как для генераторов, так и для ИБП проводится регулярное обслуживание и тестирование. Центры обработки данных подготовлены для аварийной доставки топлива. Существует также специальный центр эксплуатации оборудования, который следит за следующими областями: • системы питания, включая все критические электрические компоненты: генераторы, переключатель питания, главное распределительное устройство, модуль управления питанием и оборудование ИБП; • система отопления, вентиляции и кондиционирования, которая контролирует и отслеживает температуру, влажность, давление и поступление воздуха в центрах обработки данных. Во всех центрах обработки данных установлены системы обнаружения и ликвидации пожара. Кроме того, в каждом центре обработки данных в нескольких местах находятся портативные огнетушители. Для оборудования защиты от естественных угроз и для помещений осуществляется регулярное техническое обслуживание. Документ «Protecting against external and environmental threats and supporting utilities» (Защита от внешних и природных угроз и вспомогательные средства) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 9.1.4 и 9.2.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
RS-08 **Устойчивость — питание и телекоммуникации**	Оборудование для телекоммуникаций, данные о пересечении кабелей и реле или вспомогательные службы должны быть защищены от перехвата или повреждения и спроектированы с учетом резервного оборудования, альтернативных источников питания и изменения маршрутизации.	Документ «Cabling security and supporting utilities» (Защита кабелей и вспомогательное оборудование) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 9.2.3 и 9.2.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы. Дополнительные сведения см. в положении RS-07.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерий SA-01

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
SA-01 **Архитектура системы безопасности — требования для доступа заказчика**	Прежде чем заказчики получат доступ к данным, активам и информационным системам, должны быть проработаны и исправлены существующие регулятивные и закрепленные в контракте требования, а также требования безопасности.	Наши заказчики во всем мире подпадают под действие разнообразных законов и постановлений. Юридические требования в одной стране или отрасли могут не совпадать с требованиями, применяемыми где-либо еще. Как поставщик глобальных услуг по облачному вычислению, мы обязаны в работе наших служб обеспечить одинаковое качество и набор функций для разных заказчиков и в условиях разных законодательств. Чтобы помочь заказчикам добиться соответствия их собственным требованиям, при создании наших служб мы руководствовались общими правилами безопасности и конфиденциальности. Определив, какую работу мы должны будем выполнить для заказчика согласно регулятивным и контрактным требованиям, а также требованиям безопасности, мы проработали и исправили эти требования в режиме тестирования, прежде чем продавать свои услуги, и с тех пор продолжаем следовать этим принципам. Однако заказчик при желании может оценить наши предложения согласно своим собственным требованиям и определить, удовлетворяют ли наши услуги его потребностям. Мы всегда предоставляем заказчикам подробную информацию об облачных службах, чтобы помочь им сформулировать собственную нормативную оценку. Документ «Identification of risks related to external parties and access control policy» (Выявление рисков, связанных со внешними сторонами, и политика управления доступом) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 6.2.1 и 11.1.1. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерий SA-02

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
SA-02 **Архитектура системы безопасности — учетные данные пользователя**	Внедрение и усиление (средствами автоматизации) контроля учетных данных и паролей пользователей для приложений, баз данных, а также сетевой и серверной инфраструктуры требует соблюдения следующих минимальных стандартов: • Проверка удостоверения пользователя перед сбросом пароля. • Если сброс пароля инициирован не пользователем (например, администратором), пользователь должен при первом же использовании изменить пароль. • Своевременный запрет доступа для неактивных пользователей. • Удалять или отключать неактивные учетные записи пользователей следует не реже чем раз в 90 дней. • Уникальные ИД пользователей и запрет на групповые, общие или универсальные учетные записи и пароли. • Срок действия пароля должен составлять не более 90 дней. • Минимальная длина пароля должна составлять семь (7) символов. • Надежные пароли, содержащие как цифровые, так и буквенные символы. • Разрешение на повторное использование старого пароля должно даваться не раньше чем после смены четырех (4) паролей. • Блокирование ИД пользователя после более чем шести (6) попыток входа. • Продолжительность блокирования ИД должна составлять не менее 30 минут или до включения ИД пользователя администратором. • Повторный ввод пароля для активизации терминала, бездействовавшего более 15 минут. • Ведение журналов действий пользователей для привилегированного доступа.	Группа Microsoft Online Services использует службу Active Directory для укрепления политики управления паролями. Системы Microsoft Online Services сконфигурированы так, чтобы побуждать пользователей к использованию сложных паролей. Установлен максимальный возраст пароля и его минимальная длина. Требования по обращению с паролями включают смену предоставленных подрядчиком паролей по умолчанию перед вводом службы или системы в любую среду, принадлежащую или управляемую Microsoft Online Services. Документ «User password management and user registration» (Управление паролями пользователей и регистрация пользователей) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 11.2.1 и 11.2.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с SA-03 по SA-04

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
SA-03 **Архитектура системы безопасности — безопасность и целостность данных**	Должны существовать и применяться в соответствии с юридическими, регулятивными и закрепленными в контракте требованиями политики, процедуры и механизмы для обеспечения безопасности (например, шифрование, управление доступом и предотвращение утечек) и целостности данных, передаваемых через один или несколько системных интерфейсов, юрисдикций либо сторонних поставщиков служб общего доступа, чтобы предотвратить несанкционированное разглашение, замену или уничтожение данных.	Для минимизации риска, связанного с существованием общих для нескольких организаций активов, обмен между внутренними или внешними организациями выполняется в установленном заранее порядке, а доступ к производственным средам Microsoft Online Services персонала организации и ее подрядчиков строго контролируется. Документ «Information exchange policies and procedures and information leakage» (Политики и процедуры обмена информацией и утечка информации) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 10.8.1 и 12.5.4. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
SA-04 **Архитектура системы безопасности — безопасность приложений**	Приложения должны разрабатываться в соответствии с принятыми в отрасли стандартами безопасности (например, OWASP для веб-приложений) и соответствовать применимым регулятивным и бизнес-требованиям.	Для этого существует решение Security Development Lifecycle. Корпорация Майкрософт применяет Security Development Lifecycle, процесс обеспечения безопасности ПО, для проектирования, разработки и внедрения служб Office 365. Методика Security Development Lifecycle помогает гарантировать надежную защиту служб связи и совместной работы даже на самом нижнем уровне. С помощью таких средств управления, как Establish Design Requirements (Разработка конструктивных требований), Analyze Attack Surface (Анализ направлений атаки) и Threat Modeling (Моделирование угроз), продукт Security Development Lifecycle помогает системам Майкрософт определять потенциальные угрозы при использовании службы и уязвимые аспекты службы, открытые для атаки. Если выявлены потенциальные угрозы на этапах проектирования, разработки или внедрения, Майкрософт может снизить вероятность атак, ограничив некоторые службы или убрав функции, без которых можно обойтись. После удаления лишних функций Майкрософт снижает потенциальные угрозы, которые могут возникнуть на этапе проверки, путем полного тестирования средств управления на этапе проектирования. Дополнительные сведения можно найти на веб-сайте http://www.microsoft.com/security/sdl. Кроме того, мы поддерживаем службу, использующую тестирование на проникновение третьих сторон на основе проекта OWASP Top Ten. Документ «Control of technical vulnerabilities» (Контроль технических уязвимостей) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 12.6.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с SA-05 по SA-06

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
SA-05 **Архитектура системы безопасности — целостность данных**	Должны применяться процедуры целостности ввода и вывода данных (например, сверка данных и контрольная правка) для интерфейсов приложений и баз данных во избежание ошибок ручной или системной обработки или повреждения данных.	Группа Microsoft Online Services определяет применимые стандарты, чтобы обеспечить точный и полный ввод данных в системы приложений. Где это применимо, входящие данные должны быть очищены или обработаны до ввода в систему приложений. Управление внутренней обработкой внедрено в среду Microsoft Online Services в целях сокращения риска возникновения ошибок обработки. Внутренний контроль обработки существует как в приложениях, так и в среде обработки. Примеры внутренних элементов контроля обработки включают среди прочего использование контрольных сумм, управление балансировкой нагрузки и ПО для составления графика работы. Документ «Correct processing in applications» (Правильная обработка данных в приложениях) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 12.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
SA-06 **Архитектура системы безопасности — производственные и непроизводственные среды**	Производственные и непроизводственные среды должны быть разделены во избежание неавторизованного доступа или изменения информационных активов.	В Microsoft Online Services поддерживается разделение производственных и непроизводственных сред. Доступ к производственной среде тщательно контролируется и предоставляется только сотрудникам группы Microsoft Online Services и ее подрядчикам, авторизованным для выполнения определенных обязанностей. Поскольку каждая среда может иметь собственные стандарты работы, существует формализованная процедура обмена активами между средами. Эта процедура соответствует всем применимым требованиям конфиденциальности и служебным стандартам. Документ «Separation of development, test and operational facilities» (Разделение оперативных средств, средств разработки и средств тестирования) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.1.4. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с SA-07 по SA-08

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
SA-07 **Архитектура системы безопасности — многофакторная проверка подлинности пользователя**	Во всех случаях удаленного доступа пользователей должна применяться многофакторная проверка подлинности. Какие формы проверки подлинности используются для операций, требующих высокой надежности? К таким операциям может относиться вход в интерфейсы управления, создание ключей, доступ к многопользовательским учетным записям, конфигурация брандмауэра, удаленный доступ и т. д. Используется ли двухфакторная проверка подлинности при управлении критическими компонентами в инфраструктуре, такими как брандмауэры и т. д.?	Доступ персонала и подрядчиков к производственным средам Microsoft Online Services строго контролируется. • Серверы служб терминалов настраиваются для работы с высоким уровнем шифрования. • Группа Microsoft Online Services выпустила для пользователей смарт-карты с сертификатом и учетной записью домена для удаленного подключения. Документ «Microsoft User authentication for external connections» (Проверка подлинности пользователя Майкрософт для внешних подключений) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.4.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
SA-08 **Архитектура системы безопасности — безопасность сети**	Сетевые среды должны быть разработаны и настроены на ограничение соединений между доверенными и недоверенными сетями, а также проверяться через запланированные интервалы времени с документированием коммерческого обоснования использования разрешенных служб, протоколов и портов, включая обоснование или компенсирующие меры, внедренные для протоколов, которые считаются небезопасными. В схемах архитектуры сети должны быть явно указаны среды высокого риска и потоки данных, которые могут оказать влияние на соблюдение регулятивных норм.	Сети в центрах обработки данных Office 365 созданы с использованием нескольких отдельных сетевых сегментов. Такое деление на сегменты позволяет физически отделить наиболее важные внутренние серверы и устройства хранения от общедоступных интерфейсов. Документ «Segregation in networks» (Разделение в сетях) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.4.5. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix
Критерий SA-09

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
SA-09 **Архитектура системы безопасности — сегментация**	Системные и сетевые среды разделены с помощью брандмауэров, чтобы гарантировать выполнение следующих требований: • требования заказчиков и бизнес-требования; • требования безопасности; • соответствие правовым, регулятивным и закрепленным в контракте требованиям; • разделение производственных и непроизводственных сред; • защита и изоляция конфиденциальных данных.	Сети в центрах обработки данных Office 365 созданы с использованием нескольких отдельных сетевых сегментов. Такое деление на сегменты позволяет физически отделить наиболее важные внутренние серверы и устройства хранения от общедоступных интерфейсов. Доступ заказчика к службам, предоставляемым через Интернет, берет начало в пользовательских интернет-расположениях и заканчивается в центре обработки данных Майкрософт. Соединения, устанавливаемые между заказчиками и центром обработки данных, шифруются с помощью стандартных отраслевых протоколов TLS и SSL. При использовании протоколов TLS/SSL устанавливается надежное, хорошо защищенное соединение между браузером и сервером, помогающее обеспечить конфиденциальность и целостность данных при обмене между настольным компьютером и центром обработки данных. Фильтрующие маршрутизаторы на периметре сети служб Office 365 обеспечивают безопасность на уровне пакетов и позволяют предотвратить неавторизованный доступ к службам Office 365. Хранение и обработка данных логически разделены между заказчиками одной службы с помощью структуры Active Directory и возможностей, специально разработанных для создания, управления и защиты многопользовательских сред. Многопользовательская архитектура системы безопасности гарантирует, что данные заказчика, хранящиеся в центрах обработки данных общего доступа Office 365, закрыты для попыток доступа или ознакомления со стороны другой организации. Подразделения Active Directory контролируют и предотвращают неавторизованную или непреднамеренную передачу информации с помощью общих ресурсов системы. Клиенты изолированы друг от друга границами безопасности, или приемниками, применяемыми логически через Active Directory. Документ «Security of network services» (Безопасность сетевых служб) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.6.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с SA-10 по SA-11

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
SA-10 **Архитектура системы безопасности — безопасность беспроводной сети**	Должны применяться политики, процедуры и механизмы для защиты беспроводных сетевых сред, таких как: • брандмауэры периметра сети, внедренные и настроенные для ограничения неавторизованного трафика; • настройки безопасности с мощными алгоритмами шифрования для проверки подлинности и передачи данных, заменяющие настройки по умолчанию подрядчика (например, ключи шифрования, пароли, строки SNMP-сообщества и т. д.); • логический и физический доступ пользователей к устройствам беспроводной сети, открытый только авторизованному персоналу; • возможности по обнаружению в беспроводной сети неавторизованных устройств для их своевременного отключения.	Защита беспроводных устройств является частью стандартной системы безопасности управления сетью, включающей в себя и мониторинг. Беспроводные устройства зашифрованы, и доступ к беспроводной сети управляется через многофакторную проверку подлинности (смарт-карта, ноутбук с доверенным модулем прямого доступа). Доступ заказчика из его местонахождения через беспроводную сеть в среду Office 365 должен быть защищен самим заказчиком. Документ «Network security management» (Управление сетевой безопасностью) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.6. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
SA-11 **Архитектура системы безопасности — сети общего доступа**	Доступ к системам с сетевой инфраструктурой общего доступа должен даваться только авторизованным пользователям в соответствии с политиками, процедурами и стандартами безопасности. Сети, открытые для внешних объектов, должны иметь задокументированный план с описанием компенсирующих мер, применяемых для разделения сетевого трафика между организациями.	В Microsoft Online Services существуют процедуры, а также автоматизированные и полуавтоматизированные системы для предоставления и запрета доступа к серверам как в «управляемом» домене, который содержит приложения и данные пользователя, так и в «управляющем» домене, который предоставляет функции управления системами (например, мониторинг, резервное копирование, устранение неполадок, управление программами и исправлениями). Люди в группе Microsoft Online «Доступ и удостоверение» с помощью Microsoft Active Directory управляют доступом к «управляемым» и «управляющим» доменам. В каждой области авторизация предоставляется менеджерами служб по принципу «доступа с минимальными правами». Количество пользователей производственных систем Microsoft Online Services ограничено одним идентификатором пользователя на систему. Группа Microsoft Online Services гарантирует, что системы управления доступом и учетными данными разработаны и применяются в соответствии с политиками и стандартами Microsoft Online Services. Каждый год проводится официальный аудит средств управления ключами Microsoft Online Services, связанных с управлением доступом и удостоверениями, по стандарту SAS 70 Type II для BPOS-D и GFS. Кроме того, эти средства управления проходят внутреннюю оценку соответствия политикам и стандартам Microsoft Online Services. Документ «Network security management and user access management» (Управление сетевой безопасностью и управление доступом пользователей) подпадает под действие стандарта ISO 27001, а именно Приложения A, частей 10.6 и 11.2. Для получения дополнительных сведений рекомендуем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.

Вопросы безопасности Office 365 в контексте CSA Cloud Controls Matrix

Критерии с SA-12 по SA-15

Идентификатор критерия в CCM	Описание (версия CCM R1.1, окончательная)	Ответ корпорации Майкрософт
SA-12 **Архитектура системы безопасности — синхронизация часов**	При синхронизации системных часов всех систем обработки информации внутри организации или точно указанного домена безопасности должен применяться внешний, точный и согласованный источник времени для упрощения отслеживания и восстановления временных шкал деятельности. Примечание. Особые области юрисдикции и орбитальные системы хранения и передачи данных (GPS в США и Galileo Satellite Network в Евросоюзе) могут устанавливать опорные часы, синхронизация которых отлична от синхронизации опорных часов организации; в этом случае такая область юрисдикции или система рассматривается как четко определенный домен безопасности.	Для повышения уровня безопасности и обеспечения высокой точности записей журнала событий и мониторинга все службы Microsoft Online Services используют унифицированные стандарты установки часов (например, PST, GMT, UTC и т. д.). Когда это возможно, службы Microsoft Online Services используют протоколы синхронизации, поддерживающие одно точное время во всех средах Microsoft Online Services. Документ «Clock synchronization» (Синхронизация часов) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.10.6. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
SA-13 **Архитектура системы безопасности — идентификация оборудования**	В качестве метода подтверждения подлинности соединения должна применяться автоматическая система идентификации оборудования. Технологии, учитывающие расположение, могут применяться для проверки подлинности соединения исходя из данных о местоположении оборудования.	Документ «Equipment identification in networks» (Идентификация оборудования в сетях) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 11.4.3. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
SA-14 **Архитектура системы безопасности — ведение журнала аудита и обнаружение вторжений**	Журналы аудита, регистрирующие действия привилегированных пользователей, авторизованные и неавторизованные попытки доступа, системные исключения и события информационной безопасности, должны сохраняться согласно применимым политикам и регулятивным нормам. Журнал аудита должен проверяться не реже одного раза в день, а также должны применяться инструменты проверки целостности файлов (на узлах) и система обнаружения атак (IDS) для облегчения своевременного обнаружения вторжений в сеть, их исследования путем анализа коренной причины и реакции на инциденты. Физический и логический доступ пользователя к журналу аудита должен быть предоставлен только авторизованному персоналу.	Доступ к журналам ограничен и определен политикой. Журналы должны регулярно проверяться. Документ «Audit Logging» (Ведение журнала аудита) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.10.1. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.
SA-15 **Архитектура системы безопасности — мобильный код**	Мобильный код должен быть авторизован перед установкой и использованием, а конфигурация должна обеспечивать работу авторизованного мобильного кода согласно четко определенной политике безопасности. Весь неавторизованный мобильный код должен быть запрещен к выполнению.	Службы Microsoft Online Services представляют собой изолированную сервер-центрированную среду, в которой мобильный код применяется не так часто, как в средах настольных компьютеров. Кроме того, весь код устанавливается на серверы администратором с помощью процесса контроля изменений. Документ «Controls against mobile code» (Средства управления мобильным кодом) подпадает под действие стандарта ISO 27001, а именно Приложения A, части 10.4.2. Для получения дополнительных сведений предлагаем ознакомиться с общедоступными стандартами ISO, по которым мы сертифицированы.