**Определите наиболее подходящий раздел для несоответствия**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Несоответствие** | **Раздел** | **Обоснование (Раздел или пункт устанавливает, что…)** |
| **1** | Организация (банк) не определила нормативные технические стандарты (RTS) строгой аутентификации клиентов (SCA) и безопасной связи в соответствии с PSD2 в рамках определения потребностей внешних заинтересованных сторон. |  |  |
| **2** | Организация не вела никаких записей или другой документированной информации относительно недавнего изменения своей системы контроля доступа. |  |  |
| **3** | Организация использует электронную почту как услугу, предоставляемую внешним поставщиком. Эта информация в системе не отражена. |  |  |
| **4** | Организация определила три цели информационной безопасности, но не установила никаких конкретных целевых показателей или мер. |  |  |
| **5** | Факторы, влияющие на требования заинтересованных сторон, таких как местные органы власти, не отслеживались и не анализировались. |  |  |
| **6** | Не предоставлено объективных свидетельств компетентности лица (лиц), выполняющих работу, связанную с системой менеджмента информационной безопасностью. |  |  |
| **7** | Действия по анализу со стороны руководства не выявили результатов оценки рисков и необходимости внесения изменений в систему менеджмента информационной безопасностью. |  |  |
| **8** | Документ Должностная инструкция для роли менеджера по информационной безопасности не несет никакой идентификации или контроля версий. |  |  |
| **9** | Организация не представила никаких свидетельств того, что она отслеживала или анализировала информацию, касающуюся внутренних и внешних факторов. |  |  |
| **10** | Организация не определила планы по достижению двух из трех целей информационной безопасности. |  |  |
| **11** | В организации не созданы планы обработки рисков для всех рисков, оцененных как неприемлемые (на основе критериев приемлемости риска). |  |  |
| **12** | Несмотря на то, что организация ведет «Реестр рисков компании», не было предоставлено свидетельств надлежащего мониторинга и оценки действий, предпринятых для устранения рисков, включенных в реестр. |  |  |
| **13** | Организация внедрила процедуры и меры по управлению криптографическими ключами, но соответствующий контроль А.8.24. исключен из Положения о применимости. |  |  |
| **14** | У компании не было плана или механизмов для определения или управления компетенциями. |  |  |
| **15** | В компании была высокая текучесть кадров и, как следствие, СМИБ содержала большое количество устаревших и утративших силу документов, а система внутреннего аудита отставала от графика на 4 месяца. |  |  |
| **16** | Политика информационной безопасности не была доведена до сведения заинтересованных лиц внутри организации. |  |  |
| **17** | Область применения системы менеджмента не принимает во внимание связи и зависимости между действиями, выполняемыми организацией, и действиями, выполняемыми другими организациями. |  |  |
| **18** | Программа внутреннего аудита не определяет частоту проведения внутреннего аудита. |  |  |
| **19** | Все внутренние аудиты, проводимые организацией, охватывают основные требования системы менеджмента, но не распространяются на проверку результативности применяемых средств контроля. |  |  |
| **20** | Не всегда определяются причины несоответствия |  |  |
| **21** | При необходимости расширения персонала организация использует внешнего подрядчика. Политика информационной безопасности и условия найма не доводятся до сведения персонала, привлеченного через подрядчика. |  |  |
| **22** | Программа внутреннего аудита включала большое количество так называемых «само-аудитов», когда сотрудники должны были периодически проверять себя. |  |  |
| **23** | Организация не реагирует на нарушения политики управления доступом. |  |  |
| **24** | Не было никаких упоминаний о непрерывном совершенствовании в Политике информационной безопасности. |  |  |
| **25** | В организации не сохранилось свидетельств обучения по информационной безопасности (в которых участвовал персонал). |  |  |

**Пожалуйста, передайте этот лист своему преподавателю по завершении упражнения.**