Построение эффективной системы внутренних ИТ контролей в организации

Плетнев Леонид
Департамент консалтинга и аудита
ЗАО НИП «Информзащита»

Информзащита
Системный интегратор

Проблемы

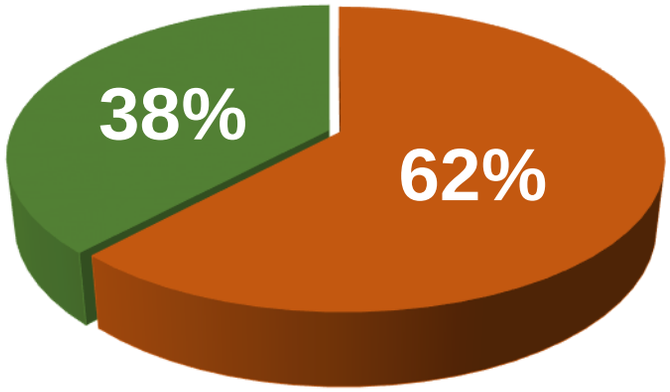
- Служба внутреннего контроля, Служба ИБ, Служба ИТ осуществляют свой контроль. Эти виды контроля не связаны между собой;
- Не определены ответственные за выполнение контроля;
- Различные методики;
- Разная система отчетности и инструменты.

Ответы респондентов на вопрос:

«Каким образом Вы контролируете соответствие?»

- *«Служба ИТ не занимается контролем, это дело СВК»;*
- *«Служба ИБ разработала политики ИБ. Определена ответственность сотрудников, они ознакомлены и поставили свои подписи»;*
- *«СВК проводит аудиты по своему плану. Выполнение некоторых частных требований ИБ проверяется раз в 2-3 года».*

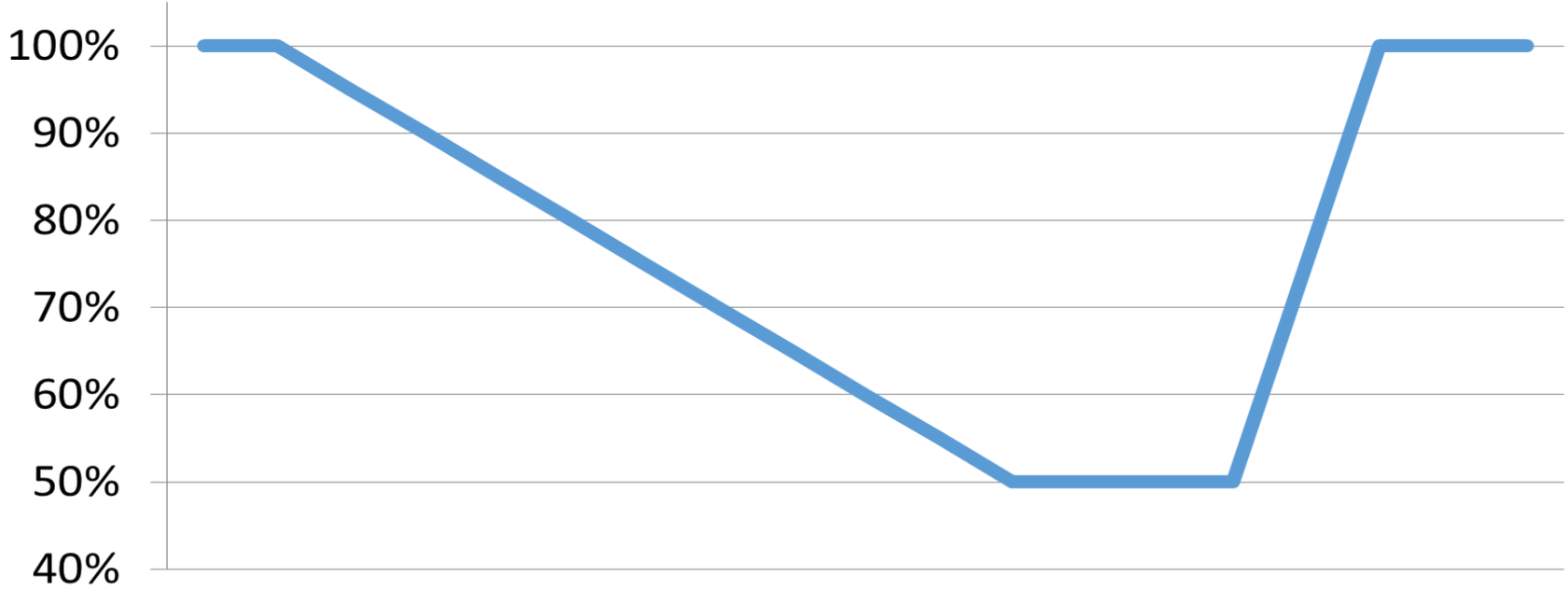
Статистика по ежегодным проектам соответствия в области ИБ*



Результат повторного аудита соответствия через год

Не соответствует Соответствует

Диаграмма снижения уровня соответствия от аудита к аудиту



*По результатам аудитов безопасности, выполненных компанией «Информзащита» в 2014-м году

Информзащита
Системный интегратор

Последствия

Отсутствие единой контрольной среды

- Низкая эффективность системы внутренних контролей (ресурсы);
- Конфликты интересов и саботаж;
- Менеджмент получает недостоверную информацию о состоянии контролируемых процессов.

Задачи

	СВК	СИБ/ДИТ
Определение необходимости контроля	+	+
Определение дизайна контроля	+	+
Автоматизация контролей	-	+
Выполнение контролей	-	+
Оценка результатов контролей	-	+
Оценка правильности функционирования контролей	+	-
Отчетность	+	+
Оценка рисков	-	+
Актуализация перечня и дизайна контролей	+	+

Польза СИБ и ДИТ от СВК

Знания

- Критичность бизнес-процессов

Возможность

- Активного вовлечения бизнес-подразделений
- Риск-менеджеры

Польза СВК от СИБ/ДИТ

Экспертиза о

- ИТ-инфраструктуре;
- Технологиях и тенденциях;
- Актуальных угрозах ИТ/ИБ;
- Защитных мерах ИТ/ИБ;
- Требованиях регуляторов;
- Уязвимостях.

Инструменты СИБ/ДИТ

- Аудиты и самооценки (ежегодно);
- Тесты на проникновение (пентесты);
- Проведение оценок рисков;
- Разработка моделей угроз и нарушителей;
- Мониторинг новых рисков (форумы, конференции, комитеты, отчеты);
- Средства регистрации и контроля доступа (СКД);
- Сканеры уязвимостей, безопасности (Scan);
- Средства антивирусной защиты (AVS);
- Средства предотвращения утечек информации (DLP);
- Средства выявления сетевых вторжений (IDS);
- Средства мониторинга и корреляции событий безопасности (SIEM).

Системный подход

Сформирован перечень выполняемых контролей

Профильные подразделения выполняют контроли на периодической основе

Результаты направляются в контролирующие подразделения

СВК осуществляет независимую выборочную оценку выполняемых контролей

5 свойств контроля

- Контроль не дороже возможного ущерба
- Действительно необходим
- Мотивация
- Простота (встроенный контроль)
- Несколько уровней

Встроенный контроль

- Парольная политика (невозможно задать простой пароль);
- Ограничение подключаемых устройств (невозможно скопировать информацию);
- Автоматическое блокирование экрана (невозможно оставить активный экран);
- Ограничение прав доступа (невозможно выполнить несанкционированные действия);
- Контроль передаваемых «во вне» файлов (невозможно скопировать информацию).

Примеры

Проверка блокировки учетных записей уволенных сотрудников

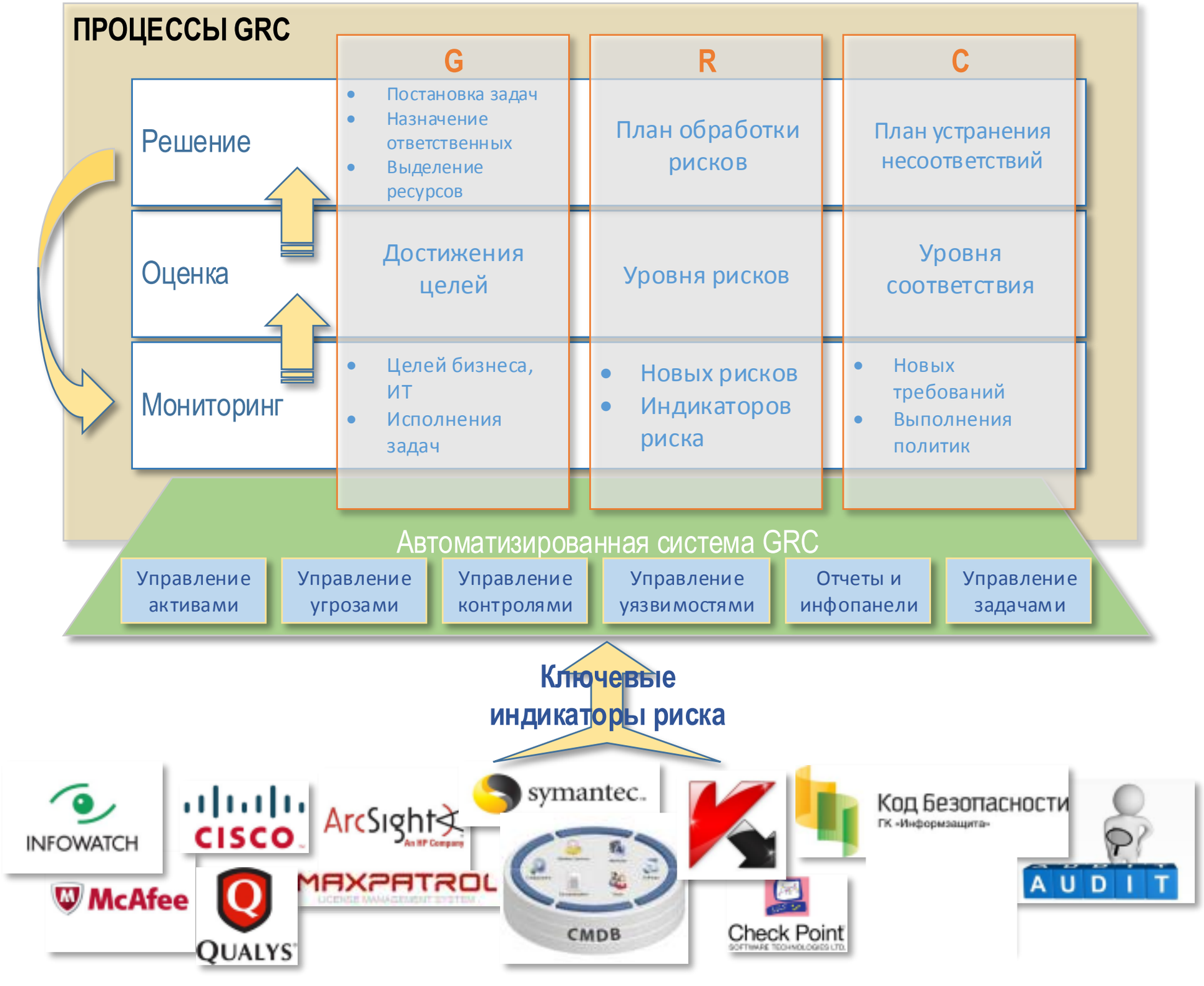
Автоматический запуск скрипта ежемесячно

Результат контроля передается в СИБ по почте

Ручной контроль правильности решений скоринговой кредитной ИС

Ежемесячно сотрудником Департамента рисков

Результат контроля передается в СВК по почте


ПРОЦЕССЫ GRC
G
R
C
Решение
Оценка
Мониторинг
Постановка задач
Назначение ответственных
Выделение ресурсов
План обработки рисков
План устранения несоответствий
Достижения целей
Уровня рисков
Уровня соответствия
Целей бизнеса, ИТ
Исполнения задач
Новых рисков
Индикаторов риска
Новых требований
Выполнения политик
Автоматизированная система GRC
Управление активами
Управление угрозами
Управление контролями
Управление уязвимостями
Отчеты и инфопанели
Управление задачами
Ключевые индикаторы риска
INFOWATCH
CISCO
ArcSight
symantec.
Код Безопасности
ГК «Информзащита»
McAfee
QUALYS
MAXPATROL
CMDB
Check Point
AUDIT

Выводы

- Уверенность в поддержании заданного уровня ИБ, сервисного уровня ИТ;
- Налаживание рабочего взаимодействия с СВК, ИТ, бизнес-подразделениями в режиме онлайн;
- Готовность к внешним аудитам;
- Создание основы для обоснования новых контролей для высшего менеджмента.

Плетнев Леонид
CISM, CISA, PCI QSA
Департамент консалтинга и аудита
Компании «ИНФОРМЗАЩИТА»
☎ +7(495) 980-2345
☎ +7(926) 411-4100

www.infosec.ru

Информзащита
Системный интегратор