Информзащита
Системный интегратор

Системы класса GRC для повышения эффективности процессов управления ИБ

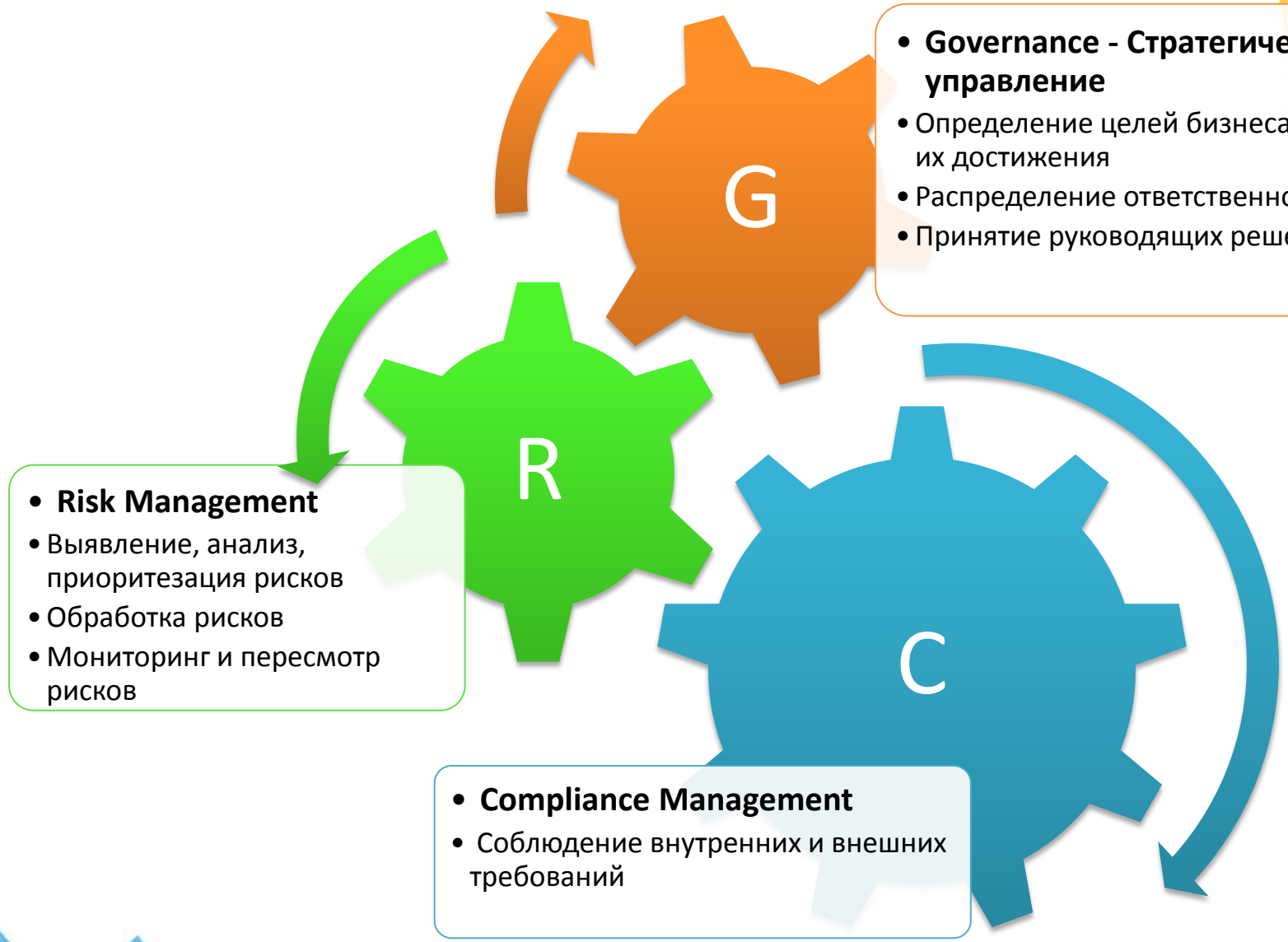
Что такое GRC?

Gartner:

«GRC is neither a project nor a technology, but a corporate objective for improving governance through more-effective compliance and a better understanding of the impact of risk on business performance»

Информзащита
Системный интегратор

GRC, как подход к управлению



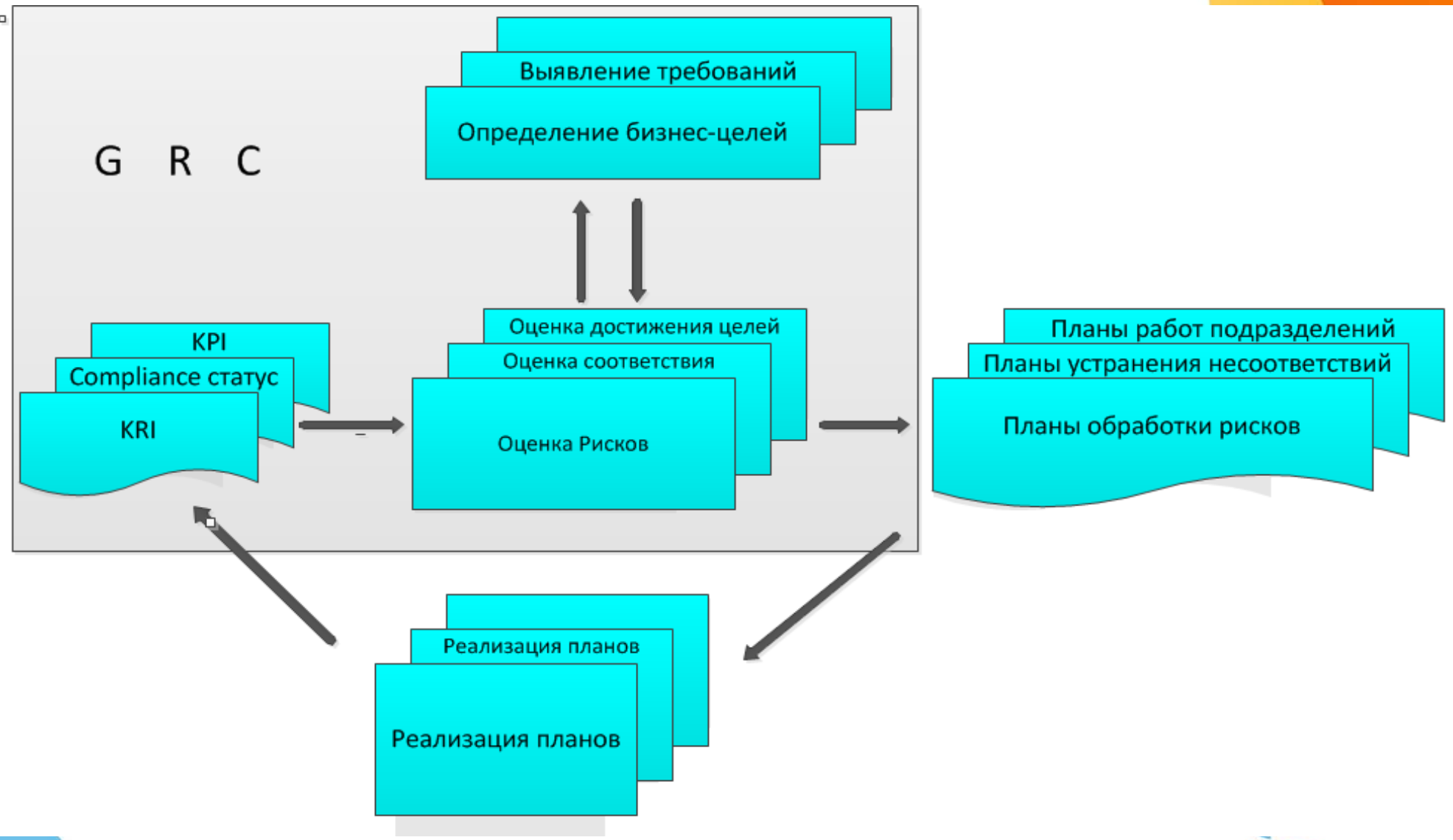
- **Governance - Стратегическое управление**
- Определение целей бизнеса и контроль их достижения
- Распределение ответственностей
- Принятие руководящих решений

- **Risk Management**
- Выявление, анализ, приоритезация рисков
- Обработка рисков
- Мониторинг и пересмотр рисков

- **Compliance Management**
- Соблюдение внутренних и внешних требований

Информзащита
Системный интегратор

GRC, как подход к управлению



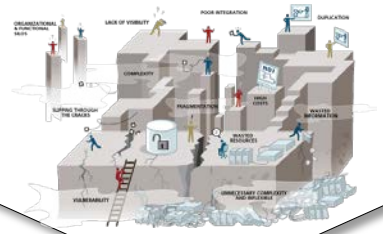
GRC, как класс решений

- Сбор и анализ информации о контролируемом виде деятельности от различных источников
- Предоставление информации о возможных рисках
- Контроль соблюдения внутренних и внешних требований
- Предоставление детальной информации о выполнении деятельности линейным руководителям
- Предоставление информации руководству компании

Информзащита
Системный интегратор

Проблемы СУИБ

Усложнение ИТ ландшафтов

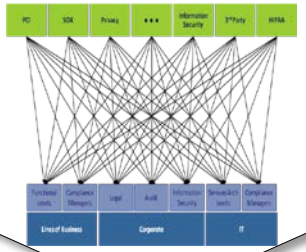


- Несвоевременное выявление и обработка рисков ИБ
- Отсутствие контроля эффективности принятых мер защиты
- Трудность получения «целостной картины» о состоянии ИБ

Бизнес и ИБ говорят на разных «языках»

- Сложность обоснования выделения ресурсов
- Сложность оценки деятельности ИБ
- Не согласованность целей ИБ с целями бизнеса

Много регуляторных требований



- Сложность приоритезации задач ИБ
- Дублирование задач и контролей по разным требования
- Избыточные затраты на подготовку к аудитам по различным стандартам
- Избыточные усилия на подготовку отчетности

Информзащита
Системный интегратор

GRC в контексте информационной безопасности

G

- Определение бизнес-целей и целей ИБ
- Определение принципов обеспечения ИБ
- Распределение ответственностей и обязанностей
- Определение метрик для контроля эффективности принятых мер

R

- Выявление и приоритезация рисков ИБ
- Обработка рисков ИБ
- Мониторинг и пересмотр рисков ИБ

C

- Информирование о внутренних и внешних требованиях, правилах и политиках
- Выполнение требований
- Контроль выполнения требований

Информзащита
Системный интегратор

Когда целесообразно внедрять GRC

Внедрение систем класса GRC имеет смысл только при достижении определенного уровня зрелости СУИБ:

- Широкое использование средств автоматизации (SIEM, сканеры уязвимостей, service desk, и др)
- Реализация (частичная реализация) следующих процессов управления ИБ:
  - Управление рисками нарушения ИБ
  - Управление информационными активами
  - Внутренние аудиты ИБ
  - Управление соответствием требованиям
  - Управление уязвимостями
  - Управление инцидентами ИБ
- Осознание необходимости совершенствования как отдельных процессов управления ИБ, так и СУИБ в целом

Информзащита
Системный интегратор

Платформы GRC, применимые для задач СУИБ

Enterprise GRC

- Решения ориентированны на оценку и управление бизнесом, могут быть использованы для контроля различных процессов управления в масштабах всего предприятия

IT GRC

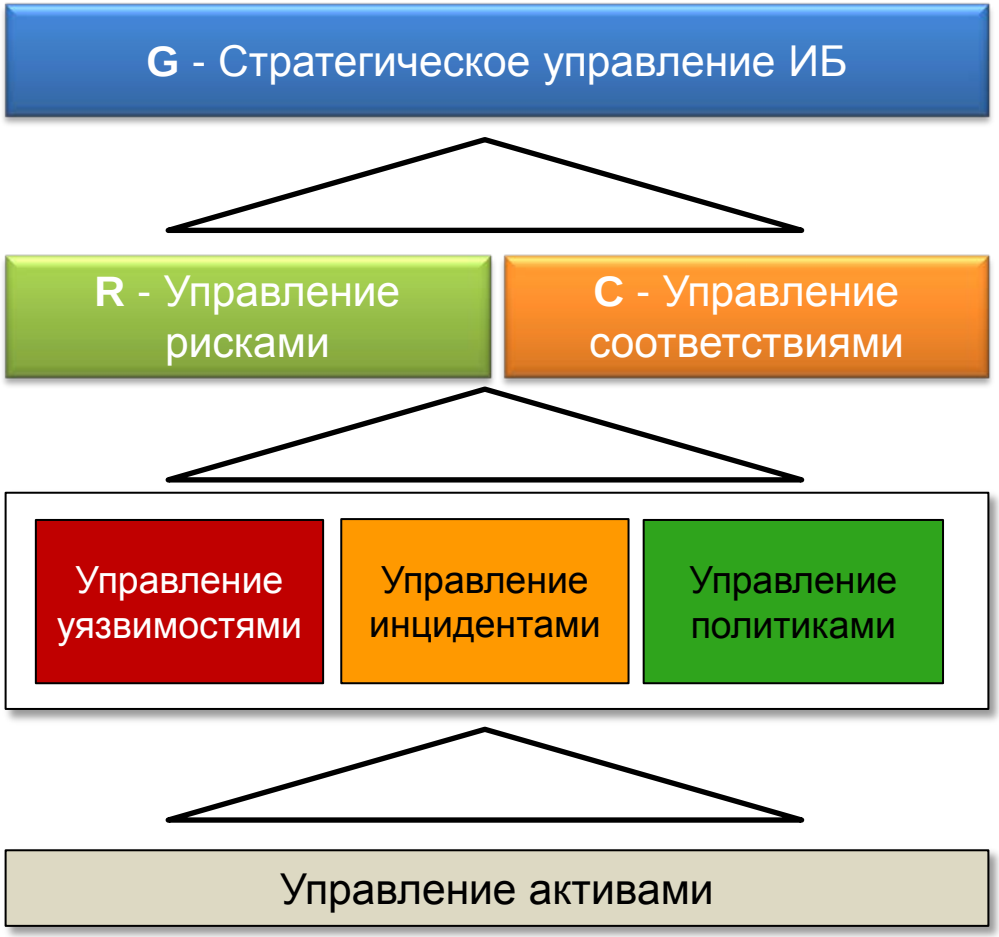
- Решения ориентированные на управление и оценку деятельности связанной с ИТ и ИБ

Информзащита
Системный интегратор

Gartner Magic Quadrant для eGRC

Информзащита
Системный интегратор

GRC - платформа для СУИБ



- Реализует основные процессы управления
- Позволяет оценивать эффективность работы ИБ

- Оптимизация процессов аудита
- Быстрое выявление несоответствий
- Эффективное управление контролями ИБ

- Достоверные источники данных о состоянии активов
- Актуальная информация поступает в систему в момент изменения

- Единый источник согласованной информации об активах
- Основан на бизнес модели организации

Информзащита
Системный интегратор

Критерии выбора GRC-платформы

- Процессы управления ИБ, которые платформа позволяет автоматизировать:
  - Управление рисками нарушения ИБ
  - Управление информационными активами
  - Внутренние аудиты ИБ
  - Управление соответствием требованиям
  - ...
- Методика оценки рисков нарушения ИБ
  - Учет вероятности риска
  - Учет стоимости защищаемого актива
  - ...
  - Возможность изменения методики оценки рисков нарушения ИБ

Информзащита
Системный интегратор

Критерии выбора GRC-платформы

- Используемая база стандартов и требований регуляторов
  - Поддерживаемые международные стандарты
  - Поддерживаемы российские стандарты и требования
- Наличие централизованной базы механизмов защиты
- Интеграция с источниками данных:
  - SIEM
  - Сканеры уязвимостей
  - BI
  - DLP
  - …
- Наличие методики внедрения/опыт успешных внедрений
- Сроки внедрения

  ~ 4 -12 месяцев
- Цена

Информзащита
Системный интегратор

Зоны особого внимания при внедрении GRC

- Регламентация процедур GRC: корректное определение области действия, участников и сфер ответственности
- Интеграция с источниками данных
- Инвентаризация информационных активов и поддержание в актуальном состоянии иерархии информационных активов
- Доработка методик управления рисками нарушения ИБ

Информзащита
Системный интегратор

Что дает внедрение подхода и технологии GRC

- Контроль над рисками нарушения ИБ
- Обоснование и контроль эффективности использования ресурсов
- Контроль эффективности и совершенствование процессов управления ИБ
- Прозрачность деятельности по ИБ для руководства организации
- Соответствие целей ИБ бизнес-целям

Информзащита
Системный интегратор

Информзащита
Системный интегратор

Спасибо за внимание!

Каншина Мария
☎+7(495) 980-2345 (доб. 815)
m.kanshina@infosec.ru