



АМТ-ГРУП: Обеспечение бесперебойности функционирования кредитных организаций

Маркин Дмитрий Евгеньевич

Начальник отдела аудита и консалтинга

CISA, ISO 27001/BS 25999 Lead Auditor





Актуальность обеспечения бесперебойности функционирования платежных систем



Обзор семейства стандартов ISO 22300



Подход к созданию системы управления непрерывностью бизнеса



ПЛАН эвакуации



Бесперебойность функционирования платежной системы (БФПС)

- Способность предупреждать нарушения применимых требований (законодательства, правил платежной системы, заключенных договоров и др.)
- Способность восстанавливать надлежащее функционирование платежной системы в случае его нарушения

Риски нарушения БФПС

- Типичные возможности неоказания, ненадлежащего оказания услуг вследствие наступления неблагоприятных событий, связанных с внутренними и внешними факторами функционирования платежной системы



- Привлечение денежных средств физических и юридических лиц во вклады (до востребования и на определенный срок)
- Открытие и ведение банковских счетов физических и юридических лиц
- Осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам
- Осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)

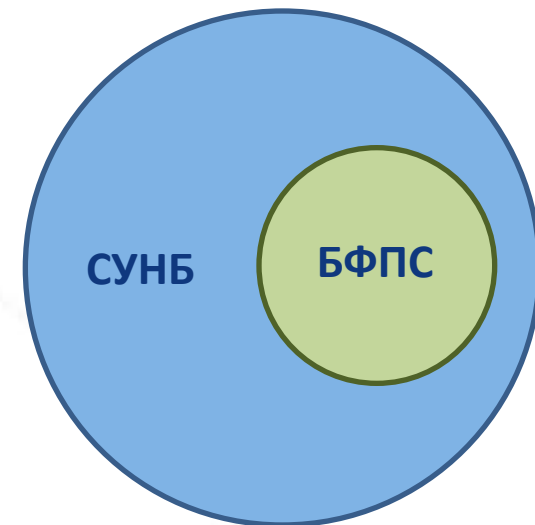
*согласно ст.5 ФЗ-395-1 «О банках и банковской деятельности»



*по данным, полученным в результате исследования, проведенного Acronis совместно с Ponemon Institute в 2012 году

Построение Системы управления непрерывности бизнеса (СУНБ) позволит кредитной организации:

- Продолжать предоставление клиентам продуктов и услуг на приемлемом согласованном уровне после аварийных ситуаций
- Минимизировать ущерб в случае возникновения аварийной ситуации
- Выполнить требования заинтересованных сторон
- Обеспечить безопасность персонала при возникновении аварийной ситуации



Требования Положения ЦБ РФ № 242-П к плану ОНиВД

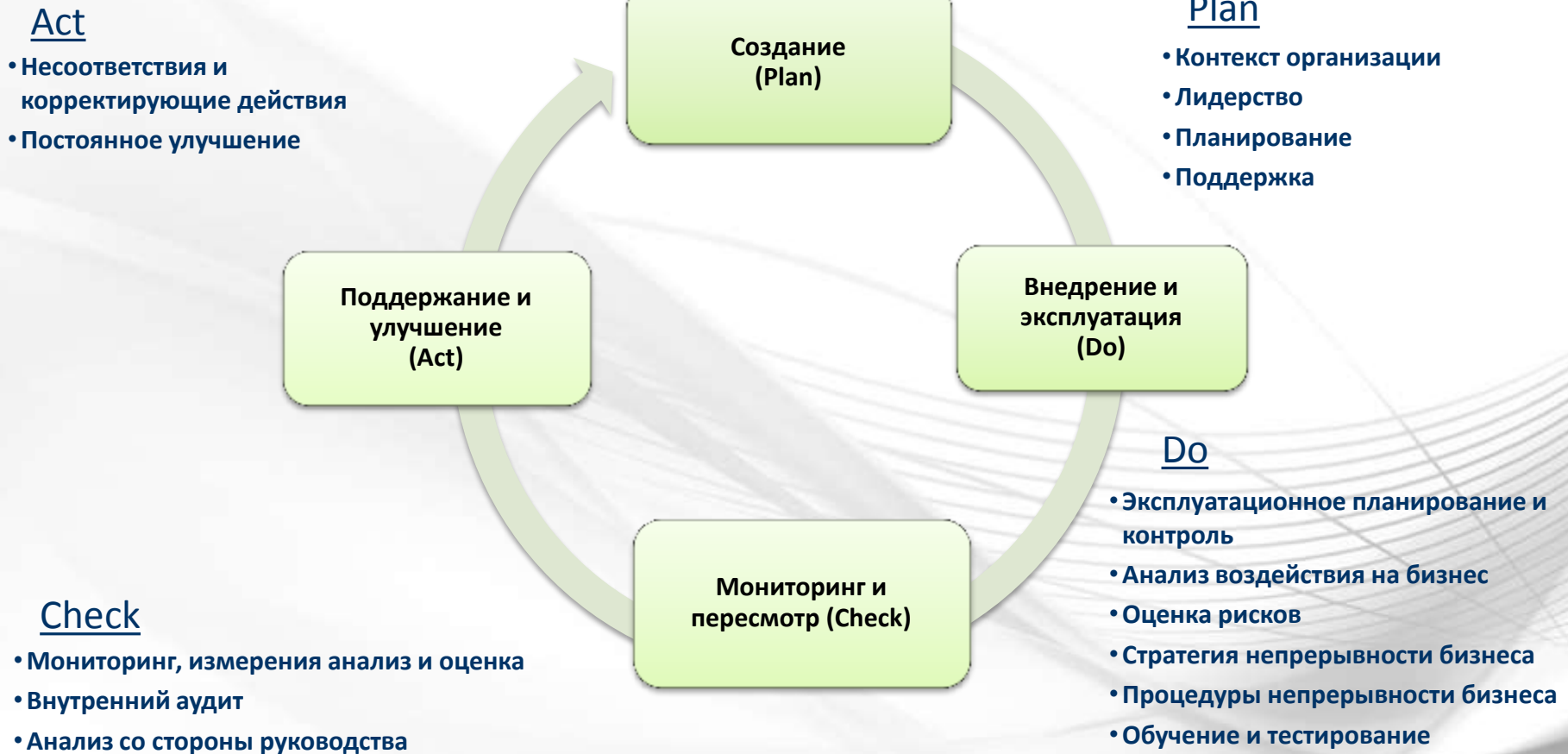
- Использование дублирующих (резервных) АС и (или) устройств
- Восстановление критически важных для деятельности кредитной организации систем
- Определение порядка проверки возможности выполнения плана ОНиВД

Семейство международных стандартов СУНБ разрабатывается техническим комитетом ISO TC 223 (Социальная безопасность)



Социальная безопасность - обеспечение защиты общества и способность реагировать на инциденты, чрезвычайные ситуации и катастрофы, вызванные умышленными и/или непреднамеренными действиями людей, природными катаклизмами и техногенными сбоями

Процессный подход на основе цикла Деминга PDCA (Plan – Do – Check - Act)

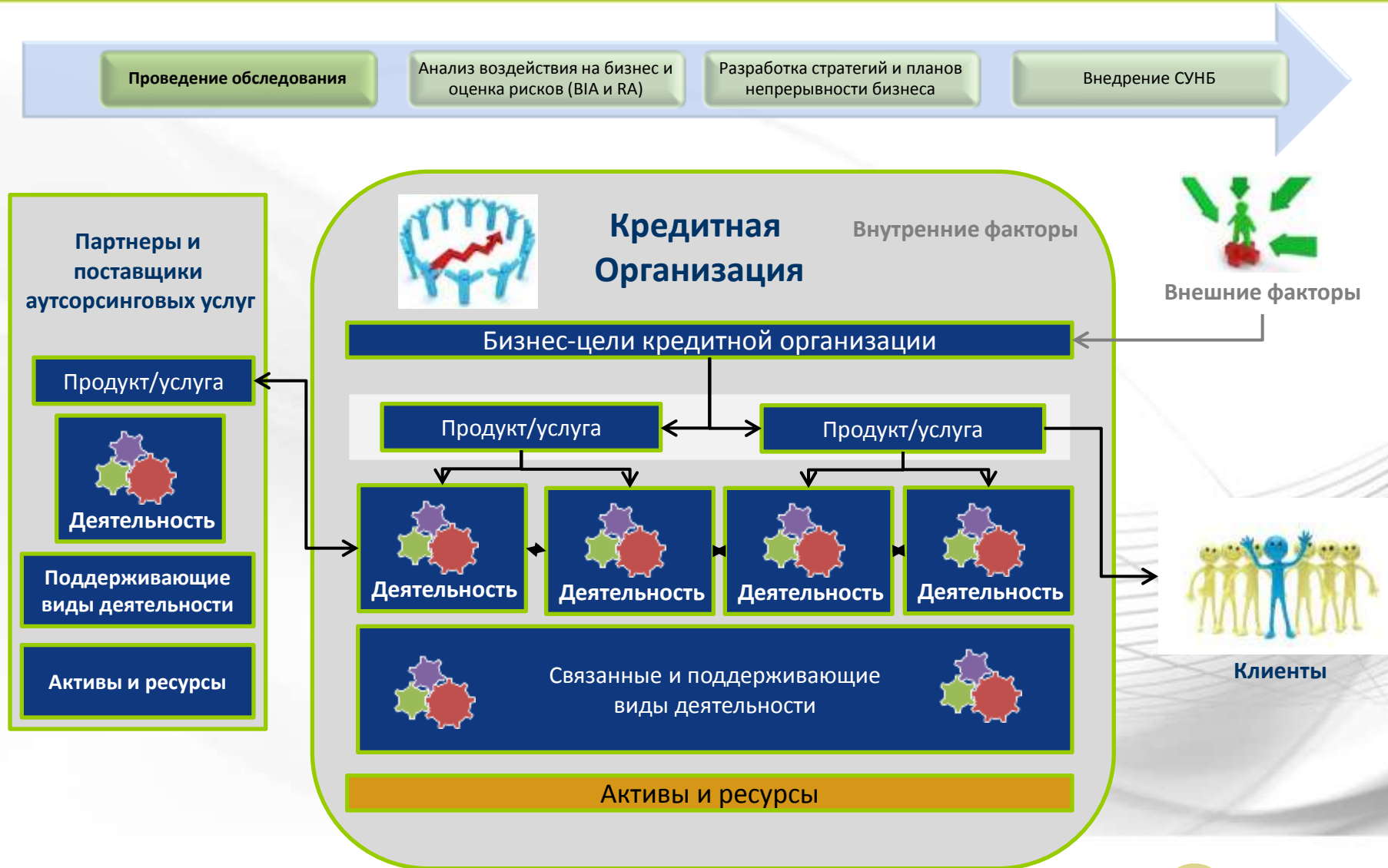


**Проведение
обследования**

**Анализ воздействия
на бизнес и оценка
рисков (BIA и RA)**

**Разработка стратегий
и планов
непрерывности
бизнеса**

Внедрение СУНБ



Проведение обследования

Анализ воздействия на бизнес и
оценка рисков (BIA и RA)

Разработка стратегий и планов
непрерывности бизнеса

Внедрение СУНБ

BIA - Анализ воздействия сбоев на бизнес

Критичные
процессы



Ключевые
показатели
процессов

Некритичные
процессы

242-П + 379-П



Анализ критически важных внутренних банковских процессов, АС, обеспечивающих их осуществление, а также показателей их восстановления

- Срок восстановления
- Допустимый размер потерь информации
- Допустимый размер материальных затрат
- Уровень бесперебойности оказания услуг (операционных услуг, услуг платежного клиринга, расчетных услуг)
- Финансовое состояние операторов услуг платежной инфраструктуры
- Технологическое обеспечение операторов услуг платежной инфраструктуры
- Способы управления ликвидностью и обеспечения исполнения обязательств

ISO 22300



Документированный анализ деятельности и воздействий, которые могут нарушить возможность предоставления продуктов и услуг

- **RTO** – целевое время восстановления
- **RPO** – целевая точка восстановления
- **MAO/ MTPoD** – максимально допустимое время простоя
- **MBCO** – минимальный уровень сервиса (и/или продуктов)
- **Размер и вид ущерба** в случае прерывания деятельности

Проведение обследования

Анализ воздействия на бизнес и
оценка рисков (BIA и RA)

Разработка стратегий и планов
непрерывности бизнеса

Внедрение СУНБ

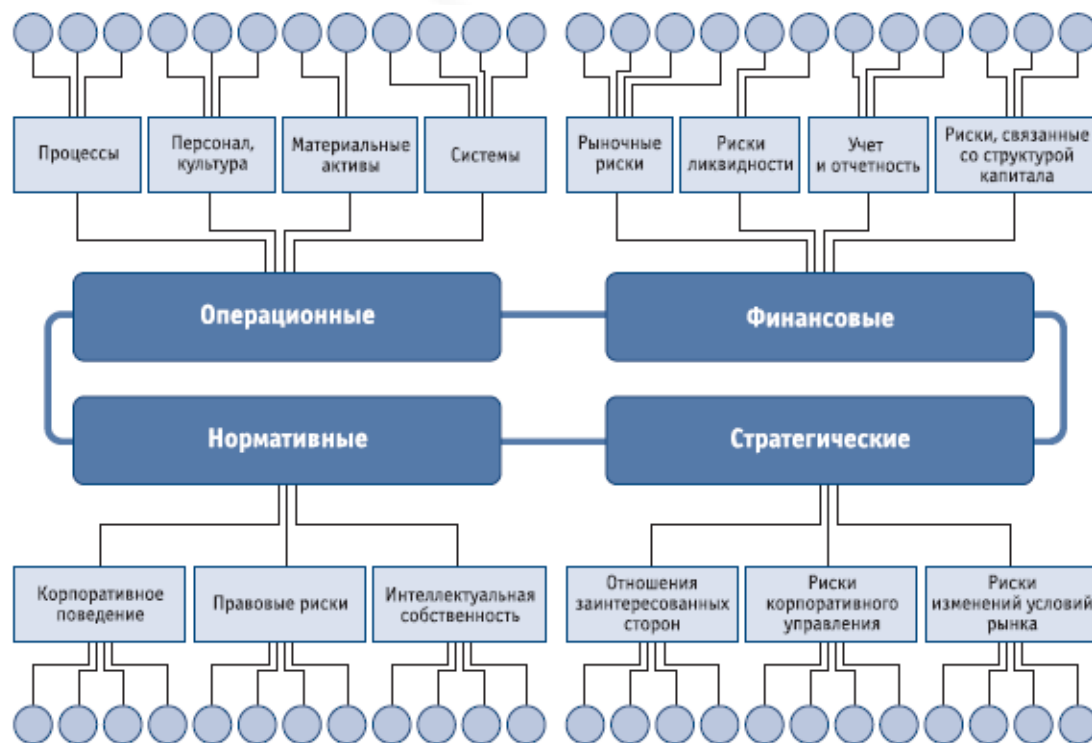
RA – Оценка рисков

Всеобъемлющий целостный процесс, включающий в себя идентификацию, анализ, оценивание рисков реализации различных угроз и их последующую обработку для критичных видов деятельности (ISO 31000:2009 и др)

Определение
приемлемого уровня риска

Идентификация рисков

Анализ и оценивание
рисков



ОЦЕНКА РИСКОВ (RA)

Классификация видов ущерба

13

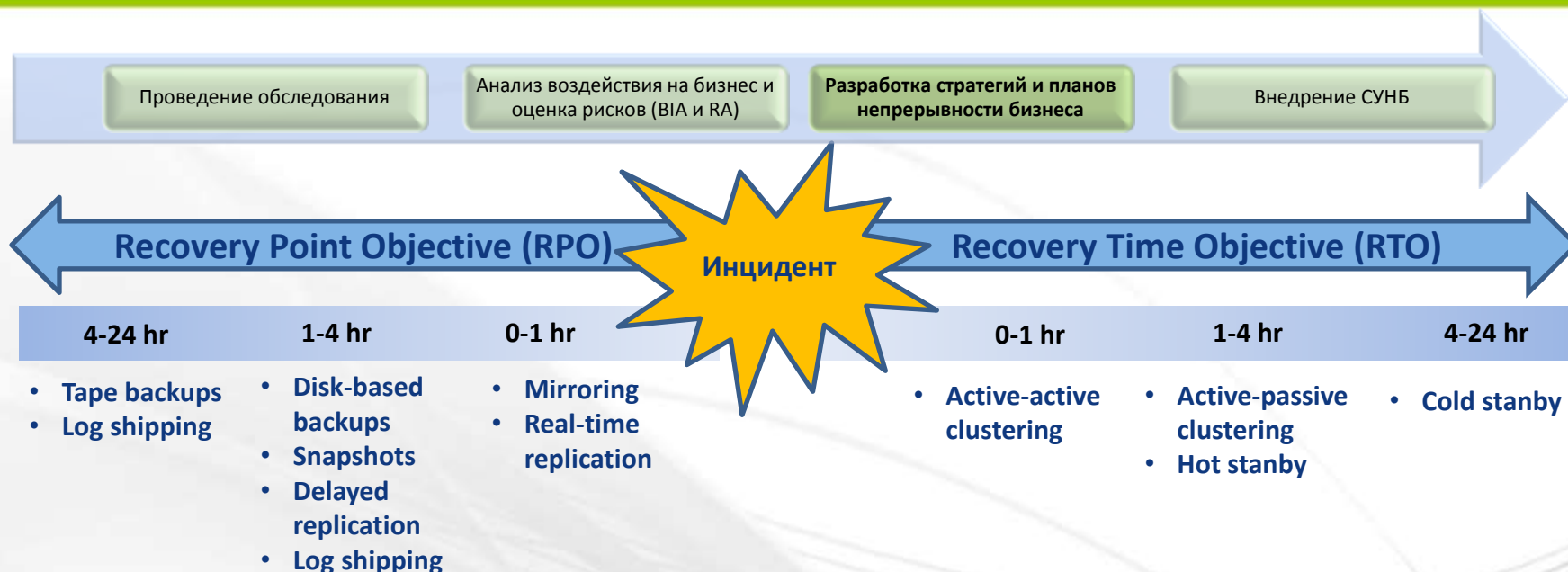
Проведение обследования

Анализ воздействия на бизнес и
оценка рисков (BIA и RA)Разработка стратегий и планов
непрерывности бизнеса

Внедрение СУНБ

ПП РФ № 304 от 21.05.07 «О классификации чрезвычайных ситуаций»

Наименование ЧС	Зона ЧС	Кол-во пострадавших	Размер материального ущерба
Локального характера	Не выходит за пределы территории объекта	≤ 10 чел	≤ 100 тыс. руб
Муниципального характера	Не выходит за пределы территории одного поселения или внутригородской территории города федерального значения	≤ 50 чел	≤ 5 млн. руб
Межмуниципального характера	Затрагивает территорию двух и более поселений, внутригородских территорий города федерального значения или межселенную территорию	≤ 50 чел	≤ 5 млн. руб
Регионального характера	Не выходит за пределы территории одного субъекта РФ	> 50 чел, ≤ 500 чел	> 5 млн. руб ≤ 500 млн. руб
Межрегионального характера	Затрагивает территорию двух и более субъектов РФ	> 50 чел ≤ 500 чел	> 5 млн. руб ≤ 500 млн. руб
Федерального характера	-	> 500 чел	> 500 млн. руб



Возможные типовые стратегии восстановления

- Mirrored sites
- Hot sites
- Warm sites
- Cold sites
- Mobile sites
- Соглашения о взаимной помощи
- Резервные центры обработки данных
- Техническая поддержка и сопровождение поставщиком (аутсорсинг)
- Комбинированный подход

РАЗРАБОТКА ПЛАНОВ УНБ И ИХ АКТИВАЦИЯ ПРИ ВОЗНИКНОВЕНИИ АВАРИЙНОЙ СИТУАЦИИ

15



1

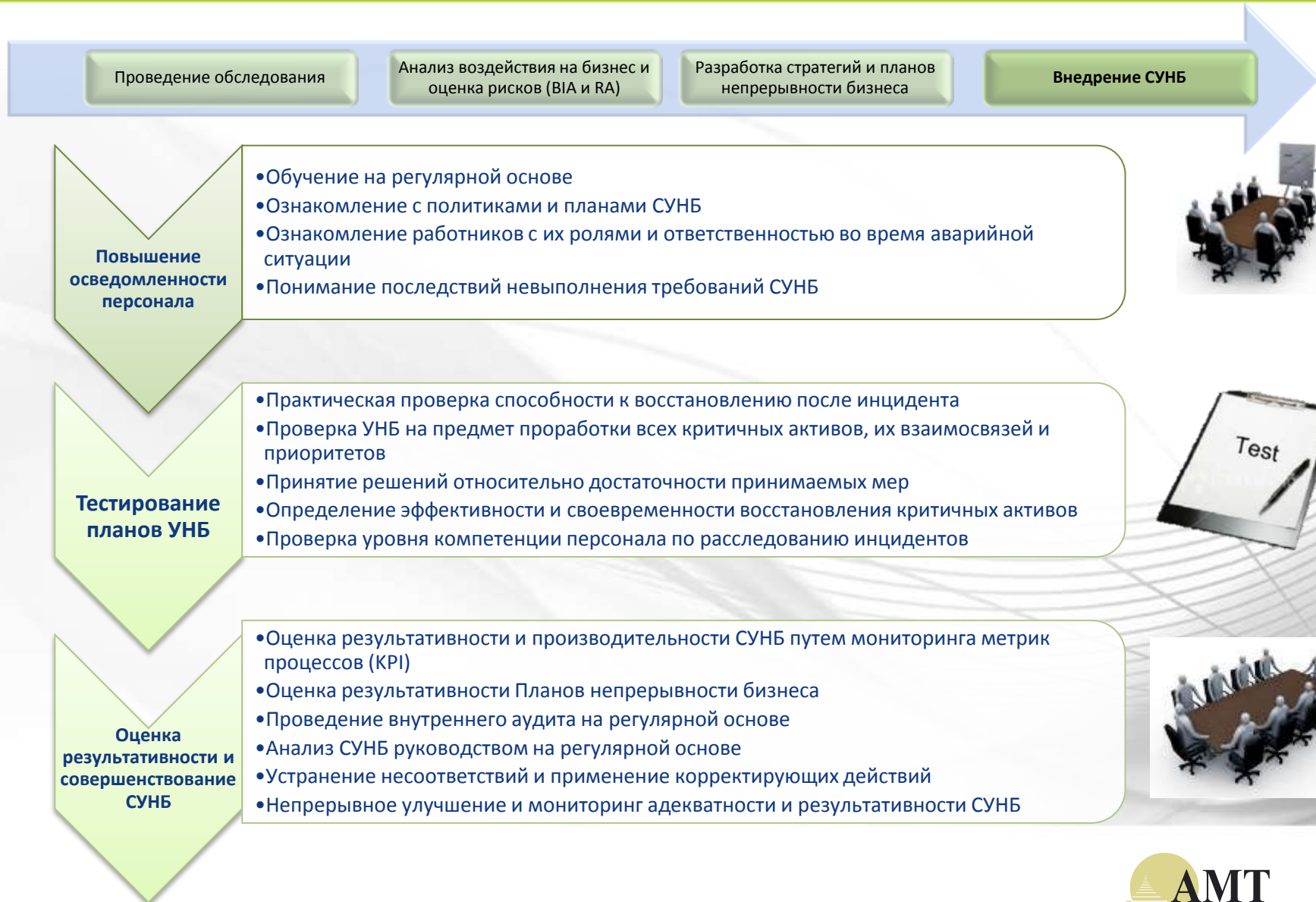
- План реагирования на инциденты (IMP)
- План аварийного восстановления (DRP)
- План коммуникаций
- План социальной безопасности

2

- План обеспечения непрерывности бизнеса (BCP)

3

- План возврата к нормальному состоянию (BRP)



- ✓ **Определение и защита основных продуктов и услуг**, обеспечивающая непрерывность их предоставления
- ✓ **Обеспечение безопасности персонала** при возникновении чрезвычайных ситуаций
- ✓ Развитие взаимоотношений с другими организациями, соответствующими регулирующими органами или государственными ведомствами, местными властями и аварийно-спасательными службами
- ✓ Понимание и обеспечение возможности удовлетворения требований заинтересованных сторон
- ✓ **Защита репутации кредитной организации**
- ✓ Обеспечение соблюдения организацией требований законодательства и нормативной базы
- ✓ Возможность интеграции со смежными системами менеджмента кредитной организации (ISO 9001, ISO 20000-1, ISO 27001) благодаря использованию процессного подхода

ЗАО «АМТ-ГРУП»
ул. Шаболовка, д. 31Б
Департамент Информационной Безопасности
Тел.: 495 725-7660 Факс: 495 725-7663
info@amt.ru <http://www.amt.ru>

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Маркин Дмитрий Евгеньевич
Начальник отдела аудита и консалтинга
CISA, ISO 27001/BS 25999 Lead Auditor