



ISIDA Bank.ORM

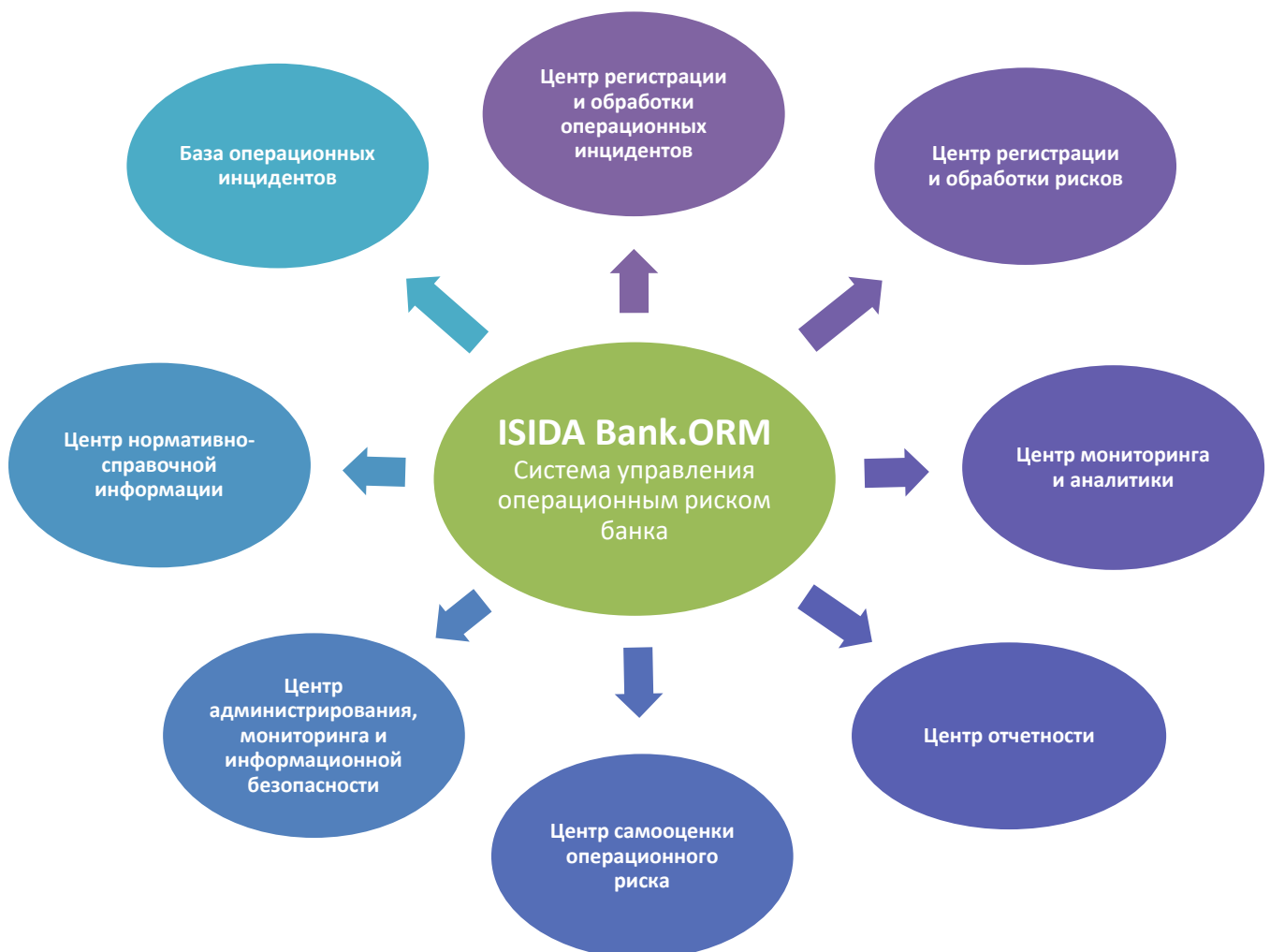
Система управления операционным риском банка

ISIDA Bank.ORM – программная система, предназначенная для ведения базы операционных инцидентов, выполнения процедур управления операционным риском, расчета показателей и формирования аналитической отчетности по операционному риску банка.

Система предоставляет банку комплексный инструментарий для управления операционным риском – мощный, надежный и удобный.

Система ISIDA Bank.ORM построена в соответствии с современной программной архитектурой и легко встраивается в корпоративный IT-ландшафт банка. Для организации информационного взаимодействия с иными корпоративными системами банка имеются развитые интеграционные механизмы. Выполняется полный цикл работ по внедрению системы, а также обеспечивается сопровождение ее эксплуатации.

Общая функциональная структура системы ISIDA Bank.ORM показана на диаграмме. Компоненты более подробно описаны ниже.



| | |
|---|---|
| База операционных инцидентов | База хранит все зарегистрированные в системе операционные инциденты. Каждый инцидент описывается набором сведений: описание, время и место реализации, выявления и регистрации, классификация, данные о понесенных потерях и полученных компенсациях, информация о принятых мерах и др. |
| Центр регистрации и обработки операционных инцидентов | <p>Центр обеспечивает регистрацию операционных инцидентов в двух режимах: ручном и автоматическом. В ручном режиме выполняется ввод данных о операционных инцидентах путем заполнения специальных экранных форм. В автоматическом режиме осуществляется взаимодействие с системами-источниками (АБС, СЭД, CRM-система и др.) и по заранее установленным правилам идентифицируются операционные инциденты, которые регистрируются в системе (с возможной предварительной модерацией специалистами подразделения риск-менеджмента).</p> <p>Для зарегистрированных операционных инцидентов выполняются бизнес-процессы обработки. В точках процесса риск-менеджеры и сотрудники подразделений осуществляют требуемые действия (классификация инцидентов, дополнение сведений, установление связей с иными инцидентами и др.). Информация вводится на протяжении всего жизненного цикла инцидента. Бизнес-процессы гибко настраиваются в системе.</p> |
| Центр регистрации и обработки рисков | Центр обеспечивает ведение реестра рисков: позволяет создавать карточки риска (номер, наименование, вид, тип, владелец, описание, ключевые индикаторы, процессы и др.), описывать контроли и мероприятия для зарегистрированного риска, выполнять оценку рисков. Обеспечивается формирование матрицы рисков и контролей, «тепловой карты» оценки рисков. |
| Центр мониторинга и аналитики | Центр ведет непрерывный мониторинг состояния базы операционных инцидентов; выполняет расчет значений ключевых индикаторов риска («КИР») в соответствии с правилами расчета, определяемыми в НСИ; ведет контроль над превышением лимитов значений КИР и автоматически инициирует действия по обеспечению мер реагирования. Центр также обеспечивает расчет размера операционного риска в соответствии с требованиями регулятора (расчет на основе определения бизнес-индикатора и мультипликатора потерь от операционных инцидентов, Постановление Правления Национального банка Республики Беларусь от 11 июля 2022 г. № 257). |
| Центр отчетности | Центр обеспечивает формирование различных отчетов и сводок на основе настраиваемых шаблонов и правил, в том числе отчета по форме F28342 «Информация об операционных инцидентах». |
| Центр самооценки операционного риска | Риск-менеджер конструирует анкету самооценки непосредственно в системе. Подготовленные анкеты система направляет в подразделения для заполнения. Заполненные анкеты возвращаются риск-менеджеру для анализа. Анкетирование выполняется на регулярной основе; бизнес-процессы движения анкет гибко настраиваются. |
| Центр нормативно-справочной информации | Центр обеспечивает ведение специальных справочников: видов операционного риска; классификатора операционного инцидента; мероприятий, направленных на предотвращение операционных инцидентов; контролей; способов реагирования на операционные инциденты; мероприятий, направленных на ограничение размера потерь от реализации операционных инцидентов; бизнес-линий (видов деятельности) банка; ключевых индикаторов риска и их индексов. |
| Центр администрирования, мониторинга и информационной безопасности | Центр содержит функции управления пользователями, функциональными ролями, правами доступа; ведения журналов аудита операций в системе; конфигурирования параметров работы системы. Центр предоставляет возможности расширения структуры информационных объектов и гибкой настройки бизнес-процессов обработки операционных инцидентов и регулярной самооценки, а также обеспечивает мониторинг выполняющихся процессов. |