LABMA Bank.ORM

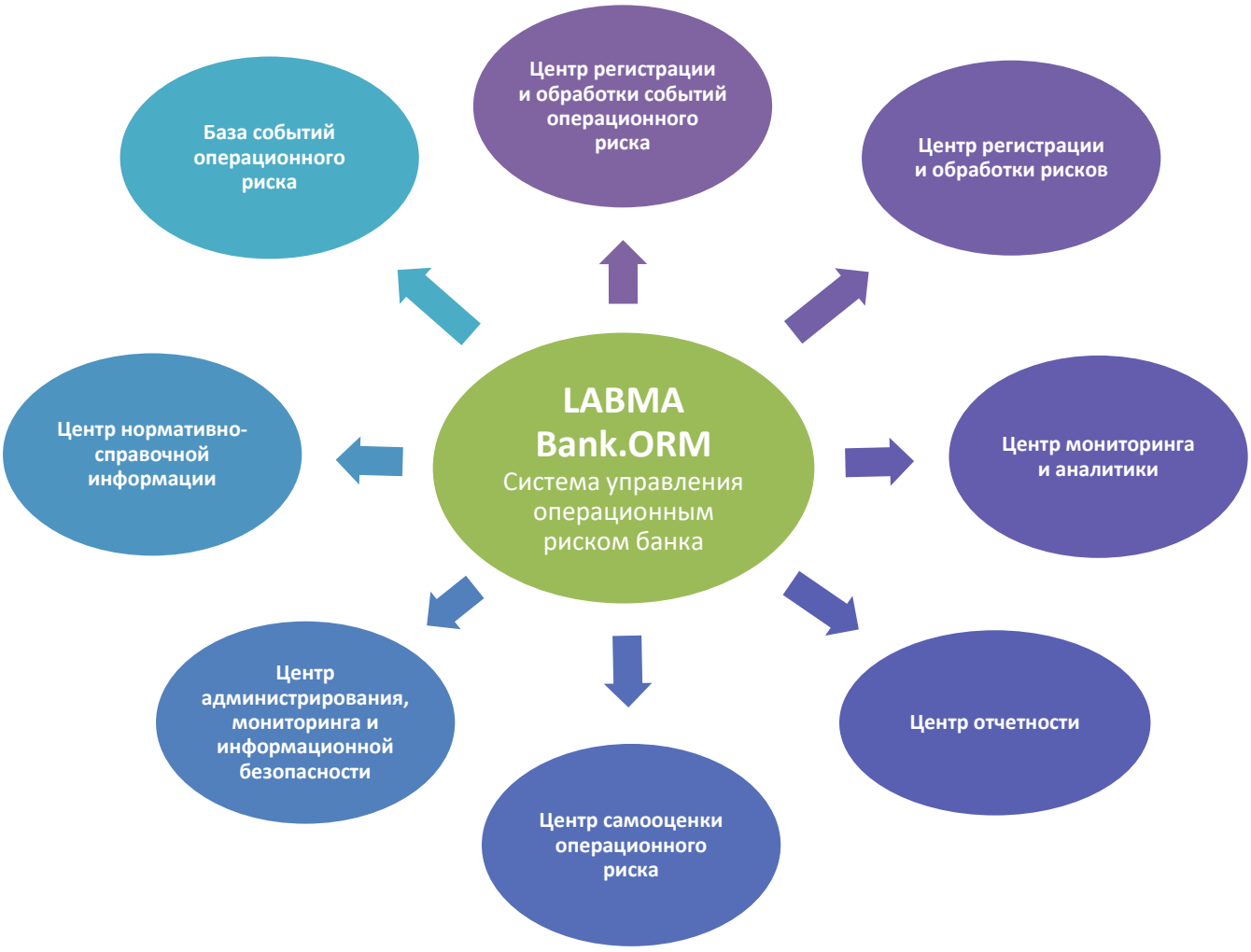
Система управления операционным риском банка

LABMA Bank.ORM – программная система, предназначенная для ведения базы событий операционного риска, выполнения процедур управления операционным риском, расчета показателей и формирования аналитической отчетности в соответствии с требованиями Положений Банка России 716-П и 744-П.

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

Система LABMA 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 LABMA Bank.ORM показана на диаграмме. Компоненты более подробно описаны ниже.



База событий операционного риска	База хранит все зарегистрированные в системе события операционного риска. Каждое событие описывается набором сведений в соответствии с требованиями Положения Банка России от 8 апреля 2020 г. № 716-П: описание, время и место реализации, выявления и регистрации, классификация, данные о понесенных потерях и полученных компенсациях, связь с банковским бизнес-процессом, информация о принятых мерах и др.
Центр регистрации и обработки событий операционного риска	Центр обеспечивает регистрацию событий операционного риска в двух режимах: ручном и автоматическом. В ручном режиме выполняется ввод данных о событиях операционного риска 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 события операционного риска, которые регистрируются в системе (с возможной предварительной модерацией специалистами подразделения риск-менеджмента). Для зарегистрированных событий операционного риска выполняются бизнес-процессы обработки. В точках процесса риск-менеджеры и сотрудники подразделений осуществляют требуемые действия (классификация событий, дополнение сведений, установление связей с иными событиями и др.). Информация вводится на протяжении всего жизненного цикла события. Бизнес-процессы гибко настраиваются в системе.
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 и «тепловая карта» оценки рисков.
Центр мониторинга и аналитики	Центр ведет непрерывный мониторинг состояния базы событий операционного риска; выполняет расчет значений ключевых индикаторов риска («КИР») и контрольных показателей уровня операционного риска («КПУ») в соответствии с правилами расчета, определяемыми в НСИ; ведет контроль над превышением значений КИР и КПУ установленных пороговых значений; автоматически инициирует действия при превышении КИР и КПУ пороговых значений. Центр также обеспечивает расчет размера операционного риска в соответствии с требованиями регулятора.
Центр отчетности	Центр обеспечивает формирование различных отчетов и сводок на основе настраиваемых шаблонов и правил.
Центр самооценки операционного риска	Риск-менеджер конструирует анкету самооценки непосредственной 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: типов операционного риска; классификатора событий операционного риска; мероприятий, направленных на предотвращение событий операционного риска; контролей; способов реагирования на события операционного риска; мероприятий, направленных на ограничение размера потерь от реализации событий операционного риска; бизнес-линий (направлений деятельности) банка; ключевых индикаторов риска и их индексов; контрольных показателей уровня операционного риска.
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 событий операционного риска и регулярной самооценки, а также обеспечивает мониторинг выполняющихся процессов.