Оценка соответствия проводится в соответствии с методикой, установленной ГОСТ Р 57580.2-2018. Аудиторы проверяют полноту реализации мер из ГОСТ Р 57580.1-2017. ГОСТ Р 57580.2-2018 (далее – ГОСТ Р 57580.2), устанавливает требования к методике и оформлению результатов оценки соответствия защиты информации финансовой организации при выборе и реализации организационных и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1.

Каждая мера оценивается по двухбалльной шкале:

0 – мера не реализована,
1 – мера реализована.

При этом ГОСТ Р 57580.2-2018 не указывает, какую оценку следует выставить – 0 или 1, если мера выполнена частично. Общий подход следующий: если мера у вас реализована не в полном объеме, тогда численная оценка по реализации такой меры равна 0.

Также оцениваются меры по направлениям защиты информации: планирование, реализация, контроль и совершенствование, оценка полноты реализации мер защиты информации на этапах жизненного цикла автоматизированных систем и приложений. При оценке этих мер возможны три числовых значения:

0 –полностью не реализуется,
0,5 –реализуется не в полном объеме,
1 – реализуется в полном объеме.

В общей сложности ГОСТ Р 57580.1 содержит более 400 мер. По каждой мере оценивается полнота реализации, заполняются опросные листы с подписями интервьюируемых и ответственных лиц со стороны проверяемой организации. По каждой мере требуется собрать свидетельства аудита (которые являются приложением к отчету об оценке соответствия).

В качестве свидетельств оценки реализации мер могут выступать:

- документы проверяемой организации;
- устные высказывания сотрудников;
- параметры конфигураций и настроек технических средств;
- технические и программные средства сбора свидетельств.

Сам аудитор решает какие именно свидетельства выбирать для оценки выполнения тех или иных мер.

В результате аудита формируется отчет для проверяемой организации. Отчет содержит, в частности:

- рассчитанную итоговую оценку уровня соответствия;
- таблицы с числовыми значениями оценок по каждой оцениваемой мере;
- заполненные листы сбора свидетельств с подписями ответственных лиц проверяемой организации и аудиторов;
- собранные в процессе аудита свидетельства оценки;
- рекомендации по совершенствованию системы защиты информации (далее – ЗИ) и устранению выявленных нарушений.

Итоговая оценка соответствия защиты информации – это число в интервале от 0 до 1, которое рассчитывается по формуле. Если упрощенно, то итоговая оценка – это среднее арифметическое оценок, полученных по каждой мере, с применением дополнительных коэффициентов по направлениям защиты информации. На общую оценку влияют также нарушения, выявленные аудиторами во время проверки.

К 01.01.2021 кредитные организации должны обеспечить уровень соответствия не ниже третьего по ГОСТ Р 57580.2-2018. Некредитные организации должны обеспечить такой же уровень соответствия к 01.01.2022.

Для сведения, третий уровень соответствия означает, что организационные и технические меры процесса системы ЗИ реализуются в значительном количестве на постоянной основе в соответствии с общими подходами (способами), установленными в финансовой организации. Контроль и совершенствование реализации организационных и технических мер процесса системы ЗИ осуществляются бессистемно и/или эпизодически.