SecurityScorecard

Scorecard as a Standard Contract Term: Best Practice Guidance

In conversations with our customers, we see that most organizations want to have greater influence over their vendor's continuous security management — they want vendors to be proactive in monitoring and improving their Scorecard issues and overall grade. Customers appreciate that Scorecard provides an independent, objective and consistent standard for evaluating security posture.

One of the most effective approaches to influence vendors is through contractual requirements. While the benefits of establishing a minimum standard are easy to understand—coordination, motivation, no grey area— implementing a program can be challenging. Below are best practices gained through our experience and that of our customers.

Elements of an Effective Vendor Contract

An effective Vendor Contract will include three elements that will help outline expectations: contract standard, contract requirements, and contract incentive.

A **contract standard** will define the target that has been agreed by both parties (in this instance, a Scorecard grade). This standard will be continuously accessible, measurable, and provide an objective view.

Contract requirements will provide the criteria that must be adhered to for the standards to be met. The requirements will provide a timeframe for vendors to meet and (in the event of dropping below minimum acceptance criteria) re-establish scoring standards in the platform. This element will also define any exceptions or exclusions to the outlined requirements.

Finally, inclusion of a **contract incentive** will provide the vendor with the rationale for adhering to the contract standards. Contract incentives will fall into one of two categories, Reward or Penalty. The "reward" approach will be used to encourage vendors to follow the agreed upon contract terms. Alternatively, the "penalty" approach will be used when vendors fail to comply with contract terms.

Roll-Out Approach

For existing vendors, customers will need to determine when to approach vendors and implement this program and associated contract changes. Implementing changes will be easier at natural breaks in the contracting cycle, such as a contract renewal or change, but will extend the overall project length.

Another factor to consider is the potential benefit (at a vendor level) created by implementing a contractual standard. Many companies have established business impact or criticality tiers to ensure that risk management effort is commensurate with the potential risk of the vendor. A contractual standard should be considered an additional risk management tool. Implementing a contractual standard in order of biggest impact will provide near-term benefits.

We recommend a hybrid of both approaches above; launch a campaign to implement the contractual standard for all critical vendors regardless of where they are in the contract cycle. And for new vendors or non-critical vendors, implement the change at the next natural break or negotiation of the contract.

Contract Language Options

Two decisions that customers regularly debate prior to implementing a Scorecard contractual standard are the incentive type—reward or penalty—and whether to specifically name a ratings company.

Incentive Type: The majority of customers we have spoken to prefer a reward over a penalty to incentivize customers, although there was no clear choice on the specific reward. Rewards may include better payment terms, higher pricing, pre-qualification for future opportunities or less frequent assessments. The most common penalty was a right to terminate a contract for failure to achieve or maintain a specific grade.

Specify SecurityScorecard: Customers are split as to whether or not they should specify a Scorecard grade as their standard. Those that prefer to name Scorecard felt that it was much easier to track performance if all parties were using Scorecard. Those that leaned towards a generic requirement felt that it would be more likely to be implemented if the vendor had their choice of a program. This second group of individuals still planned to invite vendors to the Scorecard platform and reference the free access to Scorecard.

Change Management

Implementing this change across a large number of contracts requires significant coordination. We recommend the following practices to ensure this change is executed effectively.

- Form a governance committee consisting of various invested parties such as legal, risk functions, procurement and impacted business units. Sell the committee on the concept first and gain their commitment to support the rollout
- Publish educational materials and train relationship/contract owners so they can articulate the necessity for changes and impact to their vendors
- Demonstrate an ability to track performance against the contract standard. With Scorecard, this can be achieved using the historical score data
- Create a vendor policy for you company, if you haven't already. Establish expectations for all vendors and internal contract owners. The policy should be created with procurement and can include items like audit requirements, gifts policy and behavior standards as well as security expectations

Example Contract Language #1 *(For illustration purposes only, not legal advice)*

[Customer] will continuously monitor the security hygiene of *[vendor]* through SecurityScorecard, a security ratings solution. If *[Vendor]* maintains a grade of 'B' or higher within SecurityScorecard for 300 days out of a calendar year, the *[Vendor]* will qualify for 20 day payment terms.

If *[Vendor]* fails to achieve a 'B' grade within 30 days of contract signature or if during the term of the contract *[Vendor's]* score drops below a 'B' grade for 30 consecutive days, *[Customer]* may terminate the agreement upon written notice to *[Vendor]*.

Example Contract Language #2 *(For illustration purposes only, not legal advice)*

During the Term, *[Vendor]* will ensure that it maintains a minimum acceptable security score of at least 80% (or such other percentage as *[Customer]* may require from time to time) from SecurityScorecard, a third-party application that *[Customer]* uses to assess the cyber-security of its vendors. *[Customer]* will use the SecurityScorecard (SSC) cloud-based software to monitor the cyber-security of the software and systems that *[Vendor]* uses to provide the Services under the Agreement and will notify *[Vendor]* if its security score falls below the minimum acceptable security score. In such event, *[Vendor]* will have 30 days to improve its security score so that it equals or exceeds the minimum acceptable security score. If *[Vendor]* fails to meet the minimum acceptable security score at the end of such 30-day period, *[Customer]* may terminate the Agreement upon written notice to *[Vendor]*.

During the term of the Agreement, *[Customer]* will grant *[Vendor]* access to the SecurityScorecard platform, so that "Vendor" may view and monitor its security score and other information supplied by SecurityScorecard, that is directly related to *[Vendor]*.