Eight Fundamental Security Questions

The rav does not represent risk where risk is known as Risk = Threat x Vulnerability x Asset. In that equation, risk is the result of an informed, however highly biased, equation. If we can remove most of the bias by knowing the level of protection and therefore the level of vulnerability impact, we can reduce the bias in that equation and give a much better risk assessment. Therefore, the rav is actually the factual foundation for a risk assessment where an Analyst has facts to work with. The real power of the rav however is how it can provide answers to the following eight fundamental security questions with great accuracy.

1. *How much money should be spent on security?*

The rav will show the current amount of protection to make security projections and define milestones even before buying a particular solution or implementing some new process. From these projections and milestones, financial restrictions can be created to meet the goals and get the most specific results from the investment. By knowing exactly what is controlled based on the current expenditure, you can also see what is not being controlled for that money. "More" then becomes that which is missing. It is then possible to forecast the cost of filling in the missing controls to achieve a perfect balance or at least a decidedly acceptable level of coverage.

2. *What should be protected first?*

The rav can be used to see security as part of the big picture and as a macro lens on a particular part of a target, or any combination thereof. After analysis, the rav will show which particular part of the scope has the greatest porosity and the weakest controls. Comparing that to one's needs and asset worth, a ratio of protection strength to value can be generated to decide exactly where to start.

3. *What protection solutions do we need and how should we set them up for maximum effectiveness?*

A fully completed rav will show the 10 possible operational controls applied for each target and the limitations of those controls. You can then choose solutions based on which types of controls you want to put in place. The difference now is that you no longer need to look at a solution in terms of what it is rather than as the protection or controls it can provide. This allows you to view products for the controls you need to provide in the areas where controls are currently deficient.

4. *How much improvement is gained by specific security procurements and processes ?*

A key feature of the rav is that you can make a "Delta" by mapping out the benefits and limitations of a particular solution for comparison prior to procurement. This means you can see what changes that solution will make to the scope to compare with other solutions. Combining that map to a rav of the scope where the solution would be placed, the amount of improvement can be gauged even prior to purchase. You can even predict the value of that protection by dividing the price of the solution by the rav delta.

5. *How do we measure the periodic security efforts and improvements?*

With regular audits, the rav can be recalculated and compared to the older value. Thereby the cost of new solutions and processes can be justified regularly as well as the cost of maintaining the current security level.

6. *How do we know if we are reducing our exposure to our threats?*

With specific knowledge of your controls, you can easily tell what part or vector of the scope is weak to specific and most unknown threats. In rav terminology, an unknown threat is just one that can appear where interactions exist but controls do not. Therefore a map can be drawn between the threats determined by the Risk Assessors and the controls in place. Regular metric reviews will show any change in this map and can be done so regularly. Then it is possible to gauge the cost each of those threats has on security by the expenditure on controls.

7. *Can the rav tell us how well something resists attacks?*

Technically, yes. The more you can balance controls with interactions, the smaller the attack surface will be and the more capable the target will have to control known and unknown types of interactions.

8. *Can the rav help me with regulatory compliance?*

Anything that helps you classify all controls and Access points in a scope will help you with compliance audits. The rav helps you do such a good job of getting your security under control that you may even find the major flaws in compliance regulations. While there is no particular compliance right now that asks you to have a particular rav score, showing the OSSTMM STAR with its rav score will help you meet various compliance requirements for a third-party audit and documentation.