

RAV FAQ

What are the RAVs?

The RAVs are the OSSTMM Risk Assessment Values. A RAV is the computation of security operations, controls, and limitations which represents the current state of protection.

What questions can you answer using the RAVs?

The RAVs allow you to answer these fundamental security questions with accuracy:

- *How much (more) money should be spent on security?*

The RAV will show you the protection you have and you can use that to make security projections and define milestones even before you buy a particular solution or implement some new process. From your projections and milestones you can give yourself financial restrictions to meet those goals and get the most return on the investment.

- *What should be secured first?*

The RAV can be used to see the big picture, as a macro lens on a particular application, or anything inbetween. Once a full audit has been made, the RAVs will show which particular part of the scope has the greatest porosity (number of holes) and the weakest controls. Comparing that to business need and asset worth, you can make a ratio of protection strength to value to decide where to start first.

- *How do we best apply protection solutions and which ones do we need?*

A fully completed RAV will show the 10 possible 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 as the protection or controls it provides. So AntiVirus no longer becomes that required AntiVirus solution that all "best practices" say you need rather it becomes a very narrow Authentication control with severe limitations as a blacklist-type of authentication. And a deadbolt is no longer a lock but rather a reduction in visibility and access from the outside vector and an authentication control for those who cannot work the mechanism (like little children) from the inside vector.

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

A key feature of the RAVs 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. You can even see the value of that protection by dividing the price of the solution by the RAV delta.

- *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.

- *Are we 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 threats. Therefore a map can be drawn between the threats brainstormed 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. However, to calculate the potential harm those uncontrolled threats could cost requires the type of guesswork which is beyond the factual basis of the RAVs.

How does the RAV represent risk?

The RAV does not represent risk where risk is known as $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset}$. In that equation, risk is the result of a highly biased equation. However, if we can remove some of the biases 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 assessment. Therefore, the RAV is actually the foundation of a Risk Assessment where the assessor has facts to work with.

Do you need the OSSTMM to use the RAVs?

The RAV requires a security test. Any security test can be used but the more thorough and accurate the test the more the conclusive the results will be. The RAVs were originally designed for operations tests, like the OSSTMM, where the auditor focuses on the behavior of the target rather than the configuration. However, experiments show it is possible to apply the RAV to static code analysis to determine the level of software security complexity and physical security checklist audits to determine the level of protection a physical space will provide.

How do you make a RAV?

The minimum RAV is made by the calculation of porosity which are the holes in the scope. The problem with security metrics is generally in the determination of the assessors to count what they can't possibly really know. This problem does not exist in the RAVs. You get what you know from what is there and from what is not there you make no assumptions. So since you cannot know how secure a target is, you count all that which is visible and interactive outside of the scope and allows for unauthenticated interaction between other targets in the scope. That becomes the porosity. So you don't know how deep or widely the protection extends but you do know where it does not. This porosity value makes the first of 3 parts of the final RAV value. The next part is to account for the controls in place per target. This means going target by target and determining where any of the 10 controls are in place such as Authentication, Subjugation, Non-repudiation, etc. Each control is valued as 0.1 of a pore. This is because having all 10 controls for each pore is functionally the same as closing the pore provided the controls have no limitations. And the third part of the RAV is accounting for the limitations found in the protection and the controls. These are also known as "vulnerabilities". The value of these vulnerabilities comes from the porosity and established controls themselves. With all counts completed, the RAV is basically subtracting porosity and limitations from the controls.

So can the RAV be made quicker/simpler?

If you are looking for a shortcut and don't mind the error margin because you only want to make a quick comparison, you can just calculate the Porosity which means counting the visible and accessible targets. Those who run vulnerability scanners can count porosity and limitations relatively easily and assign default controls for services. Auditors can also create a checklist which offers default controls for different common solutions found. These are all shortcuts to reduce the time to calculation but will affect the overall RAV with an unknown error margin.

What is the accuracy of the RAV?

You may notice Log10 is used to reduce large numbers into human-manageable form. Yes, people like to work with smaller numbers and especially percentages are easier to work with. For a small scope,

the accuracy of using this as a reduction technique is negligible. However, if you have a very large scope with many targets you may want to work with the very large numbers for greater accuracy. It will not change the function of the RAV however or the means of calculation.

What does a RAV actually mean though? What does it prove?

The RAV is designed to rate the effectiveness of your controls for your porosity. The RAV is different from historical measurements because just that one value should tell you how protected something is. Therefore this is a comparative measurement regardless of size of the scope.

What if your RAV value is good but there are no controls for a specific threat, can't you get harmed by that threat?

So an audit determines you have a RAV of 90% from outside the room to the inside for physical threats. Then a fire breaks out in the building and the assets in that room burn to the ground because no fire suppression controls existed (which are composed of the controls of authentication, resilience and continuity). How could that have happened when you were supposedly 90% secure? This is because you were not 90% protected rather that for what you had exposed and interactive was only controlled to a 90% effectiveness rating. Whether that ALSO means you are 90% secure requires more case studies and more implementation research. But it also means that you are 10% exposed. Unfortunately, fire was within that 10%. So to prevent such a situation, the RAV needs to be reviewed on a per-target basis to assure that the controls you want available are effective according to the threats you determine to be high. Remember that RAV is designed to assist Risk Assessment and not replace it.

What happens if the auditor does a bad job assessing and accounting?

What happens if your carpenter doesn't measure right? What if your mechanic fails to read the gauges right? The world is full of what-if scenarios. Therefore the RAVs are designed to be minimally influenced by bad auditing or cheating by eliminating the scope from the metric calculation. However, no metric can be immune from fudging and the only way to assure the most accurate RAV is to have both internal and third-party audits to make the counts and to be sure the auditor will take responsibility over the accuracy of the test like with an OSSTMM STAR (Security Test Audit Report).

Can the RAV be used to measure continuous and subjective processes, like security awareness?

Actually it can. It is possible to calculate the RAV for security according to just what the awareness training covered. Periodic tests of that sort will change the RAV in a way that can be plotted on a timeline to see if security operations are best right after training and trail off in time and if refresher courses bring the scores back up. For example, if training focuses on how operators handle and forward calls, a collection of Human and Telecommunications security tests can be used from the OSSTMM to verify these processes are being followed properly. Limitations and controls used are recorded and the RAV is calculated as normal.

Processes are as important or more important that controls in security, so how do they enter the calculation?

All processes are a function of initializing a set of controls within a space or time. So backing up data regularly is a process of the continuity and integrity controls. If the process is completed successfully then it is scored a 1 for continuity. If it is done in a regular and timely fashion to assure a minimal loss when recovery is needed then it also scores a 1 for integrity. If it is done in a manner where it cannot corrupt previously backed-up data then it scores another 1 for integrity for a total of 2 for the process. This can be done for any process and is the foundation of the Business Integrity Testing methodology project which does for business integrity what the OSSTMM does for security.

Why are there only 10 controls? What happened to all the rest?

The 10 controls represent the categories for which all other controls belong. For example, warning signs, lawsuits, and insurance as controls are all part of the RAV control of Indemnification. The original control count was 12 but research proved that authorization and identification (the other two) are required for authentication. Without either of those two, authentication cannot exist as a control. (I know that traditional security theory says otherwise but they are wrong and you'll know it too when you think it through and do the research). Therefore it was reduced to 10 with those two existing as tests for authentication.

Can the RAVs 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 RAVs help you do such a good job of getting your security under control that you will find the major flaws in most all 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.

Is there a default list for what basic solutions have which controls?

At this time, there is none. It is something that every security solution should have on its packaging like a consumer nutrition information label. That would make it very simple to know exactly what you get, even if they leave off the limitations out of commercial reasons. So you would know that a basic VPN provides privacy, confidentiality and integrity controls or a door peeper provides authentication, subjugation, and integrity controls. Unfortunately, this list does not exist at this time.

Under which control does security awareness training fit?

Training is actually a security process which "configures" people to be more security minded. This itself is not a control but rather a means of configuring protection and controls. It is like accessing the management console on a firewall. It itself is not a control but it is how you set up the protection and controls. That is what training is -- as is a security test or audit-- also a configuration process and not a control.

Can the RAV tell us how well something resists attacks?

Technically, yes. It can tell us how well something is protected and therefore how well it resists attacks. However, the percentage of protection is exactly that, a percentage, which means that as the volume of interactions increases, so does the likelihood that an attack will be of the kind that is not controlled for. More research is required though on this to determine accuracy.