Carson

your bridge to better IT

How does a leader create an affordable, sustainable, resilient and dynamic risk management program with the ability to reliably detect threats and morph rapidly to defeat them?

Continuous Monitoring

Find What Matters . . .

Control What Counts

Recent changes in guidance are reshaping how federal security programs are implemented and managed. With the release of NIST Special Publication 800-39, *Managing Information Security Risk,* organizations are shifting towards framing risk across the enterprise to obtain a holistic view.

When establishing an enterprise risk management strategy, it is essential to perform a business impact analysis (BIA) that will identify potential exposure to sudden loss of critical business functions. Agencies can use the BIA as a basis for a risk strategy framework to establish:

- organizational tolerance for risk,
- applicable security controls,
- appropriate metrics and/or measures to monitor risk,
- and risk response.

When establishing a response, it is important to give priority to the high impact risks. Applying the 80/20 rule, it is not uncommon to find 20% of the problems account for 80% of the risk.

Defining risk tolerance levels will be unique to each organization based on probability of occurrence and impact on the business function. Once tolerance levels are defined, the metrics can be developed and applied to monitor risk. **When establishing metrics – measure what matters.**

At Carson, we understand how to find what matters, measure it, analyze results, present actionable information, and assist management in developing a cohesive, cost effective response that creates a secure information technology environment. Read more to find out how . . .

Information security continuous monitoring is defined as maintaining ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions. Continuous monitoring should be focused on the security controls applied to protect system data directly linked to the organization's critical business functions. When focused in this manner and presented properly, the metrics will provide senior executives a view into the level of risk at any point in time.

Continuous monitoring practices are not new; however, the latest revision to NIST SP 800-37 (Rev.1), *Guide to Applying the Risk Management Framework to Federal Information Systems*, pushes federal agencies to move toward near real-time risk management. Organizations will have to rethink how they capture information and infuse more technology to monitor their security posture.

To reduce cost and increase the efficiency of continuous monitoring, the newly revised guidance addresses leveraging technology to automate monitoring efforts. For many agencies this is a daunting task, because they must consider monitoring security control implementations by employing manual and automated processes throughout the enterprise. Simply detecting vulnerability risks may mitigate individual risk occurrences, but it does not provide a view of risk trends over time; nor does it reflect whether the program is improving or regressing in effectiveness.

To be effective over time an organization must understand the components of continuous monitoring, and how each tier of responsible individuals participates in the overall strategy.

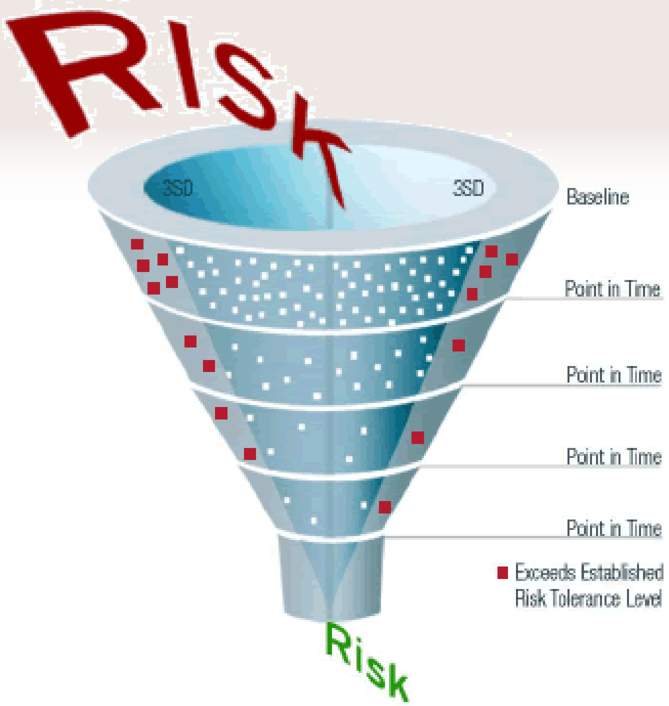
So, how does the person responsible for the agency's security program know if their program is heading in the right direction? The Carson Risk Reduction Model (CRRM), using an integrated data approach, combines the tools and methods employed for continuous monitoring with advanced trend analysis techniques. This approach allows the decision maker to view security trends over time through the use of a tailored risk management dashboard.

The CRRM applies statistical risk monitoring algorithms that run in the background to correlate the security data that has been collected. Its presentation can depict trends related to each security metric and to the holistic security program.

The figure 'Risk Reduction' shows how the implementation of CRRM will help focus the decision making process where it is needed to facilitate continuous risk reduction. With tolerance levels set at 3 standard deviations (3SD at the risk entry point for the initial time period data set) the process takes a Point In Time snapshot. Outliers (events that exceed the Risk Tolerance Level) are highlighted for action. As these events are eliminated the statistical variation is reduced, providing a tighter level of tolerance. This will produce new outliers for elimination.

Through this continuous cycle the funnel effect is produced: fewer risk events, tighter tolerance levels, effective acceptable risk policies and a more effective risk strategy.

Risk Management Model



For additional information request our Continuous Monitoring White Paper
or request a consultation with one of our cyber-security experts.
Carson Associates, 4720 Montgomery Lane, Suite 800, Bethesda, MD 20814
info@carsoninc.com 301.841.0094 www.carsoninc.com