Reducing Risk through Continuous Monitoring

A white paper in our Integrated Risk Management information series

Find What Matters . . .

Control What Counts

Carson

your bridge to better IT

Today's Security Challenges

The Battle against Cyber Threats

The Federal Government has made great strides in implementing security programs to protect its information from cyber threats. Security incidents, however, continue to wreak havoc on Federal agencies as cyber criminals become more sophisticated. As technology continues to evolve, organizations will continue to face increases in security risks. Some top security challenges include cyber war, social engineering, botnets, sophisticated dynamic and encrypted threats, and mobile applications.

Technology's increasing reach is expanding the cyber security battlefield.

Adoption of cloud services, social networking sites (e.g., Twitter, Facebook), and virtualization technologies will continue to blur the network perimeter; while sophisticated cyber criminal methods will entice users and threaten the enterprise. Adopting cloud architecture opens organizations to risks and vulnerabilities as information travels to and from protected networks via a public pipe, creating more opportunities for data contamination or theft. In addition, mobile applications on smart phones (e.g., mobile banking) are becoming more popular, making them an enticing target.

Despite industry and government efforts, criminals continue to find ways around current protective measures.

All of this leads to the inevitable—something will get stolen. Identity theft is now the fastest growing crime in the United States. The FTC estimates that 9 million Americans have their identities stolen each year. Safeguarding and protecting personal identifiable information (PII) in Federal Government systems is more critical than ever before. Industry, as well as the Federal Government, has put standards and guidance into place as a preventive measure to protect PII; however, criminals continue to find ways around these measures.

Agency executives are required to secure their organizations from cyber criminals while complying with Federal laws, regulations and guidance. Not only are leaders challenged by increased and more sophisticated cyber threats, they must also deal with changing guidance, increased compliance reporting, and shrinking budgets.

To further complicate the problem, agencies have numerous security technologies in place that are SCAP compliant; however, their deployment is often disjointed and scattered across many divisions. This can result in an inconsistent flow of security information to decision makers, a disjointed response to threats, and ineffective mitigation of risk across the enterprise. The challenge faced by agency leaders is how to leverage current practices and technologies while methodically keeping an eye on the security horizon. **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?**

Risk Management Strategy

Measure What Matters

Managing risk can take many forms (i.e., program management, security, inventory, investment and budgetary) and is not an exact science. Senior leadership is accountable for risk management decisions and the implementation of effective, organization-wide risk management programs. 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) which 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,
- appropriate metrics and/or measures to monitor risk,
- applicable security controls,
- and risk response

When establishing an organizational risk response, it is important to give priority to the high impact risks. Applying the 80/20 rule, it is not uncommon to find that 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.**

Metrics should be specific, repeatable, and actionable; they should also be aligned with business functions, potential security risks, risk tolerance levels, and federal requirements (i.e., OMB, NIST). What matters may be different from one organization or individual to another. Therefore, identification of applicable security controls is key to implementing an organization's continuous monitoring strategy.

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.

The continuous monitoring and risk management processes are complementary and inseparable.

The health of the continuous monitoring process, at all levels, directly impacts the organization's abilities to effectively monitor and manage risk.

Plan and Practice the Response

The overall risk strategy should include how the organization will respond to risk. Risk responses need to be planned and practiced. The primary purpose of a risk response strategy is to reduce risk to a tolerable level by reducing the frequency and/or impact to an acceptable threshold. In other words, a response needs to be defined so the future residual risk falls within the organizationally-defined risk tolerance limits.

A course of action designed to achieve this goal would consist of a time-phased or situation-dependent combination of risk response measures. Risk response measures can be separately/independently managed and can include the implementation of security controls to mitigate risk, promulgation of security policies to avoid risk or to accept risk in specific circumstances, and organizational agreements to share or transfer risk.

It is important for agency leadership to communicate the risk strategy, risk tolerance, and its impact on risk-based decision making throughout the organization. This top-level, executive commitment ensures resources will be available to develop and implement an effective, organization-wide security risk management program that is supported at all levels of the organization.

Continuous Monitoring

A Key Component of the Risk Management Process

Everyone has a role to play in the risk management process.

It cannot be effective unless policy and strategy are understood, and vigilance is continuous.

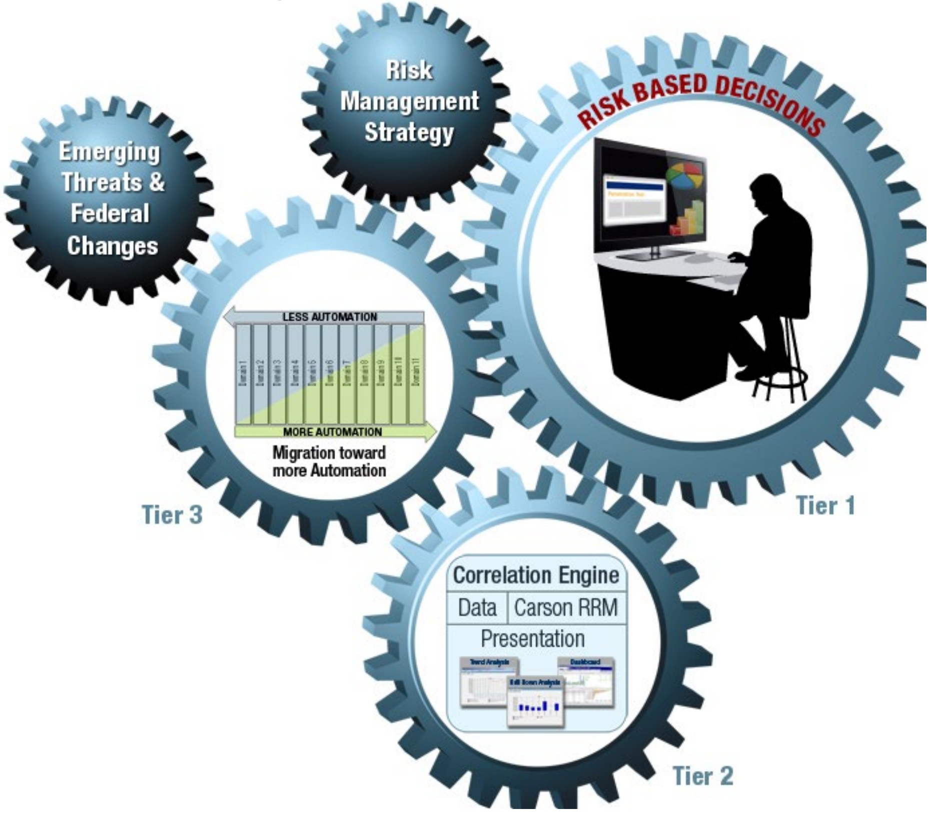
Continuous monitoring practices are not new; however, the latest revision to NIST SP 800-37 (Rev.1), *Guide to Applying the Risk Management Framework to Federal Information Systems*, pushes federal agencies to move toward near real-time risk management. Organizations will have to rethink how they capture 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 participate in the overall strategy. As depicted in the *Continuous Monitoring Process* diagram below, all tiers of the continuous monitoring process are linked.

Tier 3, where information is collected, must adjust its activities based upon emerging threats and changes in Federal policy. This will naturally impact on the data assimilation and analysis activities at Tier 2. The results presented to Tier 1 produce decisions that impact Tier 3 directly and through changes in the enterprise risk management strategy. Thus, you end up with a cyclical continuous monitoring process.

Continuous Monitoring Process



Part of the cost reduction efforts associated with the risk management strategy should be to employ only automated tools that are Security Content Automation Protocol (SCAP) compliant. The employment of SCAP compliant tools ensures they integrate effectively into the monitoring architecture without a lot of customization. This allows the collected and correlated data gathered at Tiers 2 and 3 to be presented to the Tier 1 decision makers in a consistent format that permits effective top-down risk management.

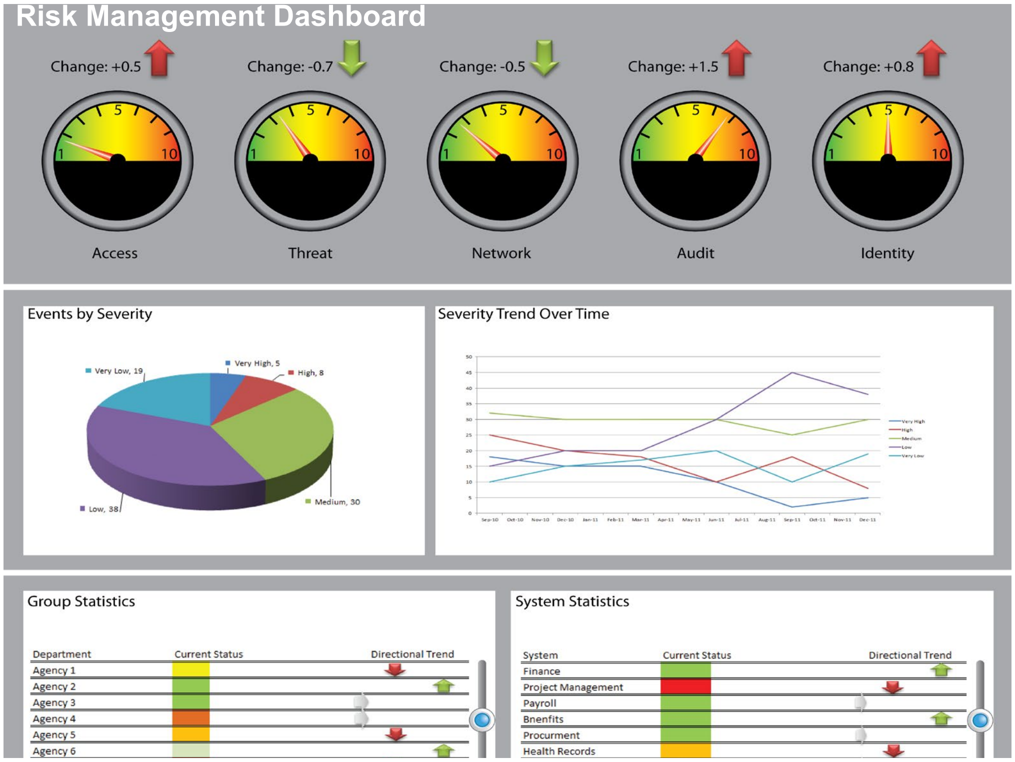
In order for this process to function as designed, a cultural change must exist where security is integrated into the day-to-day routine. It is important to communicate the continuous monitoring hierarchy to the system owners at Tier 3 to obtain their buy-in, so they understand the data being extracted at the system level is required by the Tier 1 decision makers to manage risk. Tier 2 personnel must understand they are responsible for establishing the processes to collect data from Tier 3, and other sources, and correlate to form the metrics used by Tier 1 decision-makers to formulate sound risk-based security program decisions.

Carson Risk Reduction Model

Correlation Engine Methodology

The Carson Risk Reduction Model produces a funnel effect that allows management to focus on continuously eliminating outliers, producing tighter risk tolerance levels and improved risk management.

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 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. Carson works with a variety of flexible information reporting tools to provide appropriate decision support displays with drill down capabilities. A sample Carson designed dashboard, shown below, depicts the level of risk associated with each specific security measurement area/metric within the enterprise-wide risk management process, and provides easily understood indicators of changing conditions.



Group Statistics

Department	Current Status	Directional Trend
Agency 1	🟨	↓
Agency 2	🟩	↑
Agency 3	🟩	→
Agency 4	🟧	→
Agency 5	🟧	↓
Agency 6	🟩	↑

System Statistics

System	Current Status	Directional Trend
Finance	🟩	↑
Project Management	🟥	↓
Payroll	🟩	→
Bnenfits	🟩	↑
Procurment	🟩	→
Health Records	🟧	↓

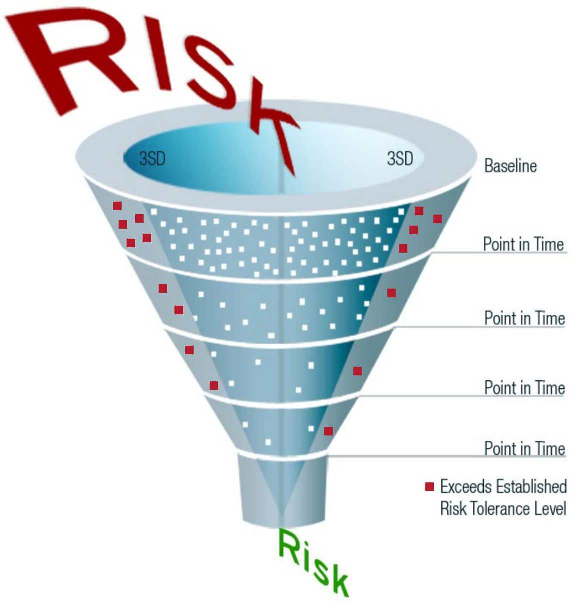
The CRRM applies statistical risk monitoring algorithms that run in the background to correlate the security data that has been collected. Its presentation can depict trends related to each security metric and to the holistic security program.

The CRRM establishes a mean risk average and the risk tolerance levels for each metric, as well as the overall program, by setting the risk tolerance bar at three (adjustable) standard deviations above the mean average. The standard deviation, or risk tolerance level, is based on the initial state of the security program and the level established by the Tier 1 decision makers in accordance with NIST SP 800-39.

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 Reduction Model



About Carson Associates

Your bridge to better IT

Carson Associates has 21 years of experience developing IT security solutions for federal agencies and commercial organizations. We understand the security environment within the Federal Government, and we are experts at turning data into actionable information. We also understand the role of change management and collaborative teamwork as success factors in continuous monitoring implementations. With this background you can count on us to be a part of your IT security team—as your trusted advisor, recommending new approaches and technologies to successfully respond to changing guidance, future cyber threats, and enterprise-wide security challenges.

To learn more about how Carson Associates can help your organization meet evolving cyber-security challenges and comply with the changes in federal security guidance, contact Diane Reilly at (301) 841-0094 or reillydc@carsoninc.com.