Information Technology Risk Management

The Cyber-Security Discussion Series for Federal Government security experts . . .

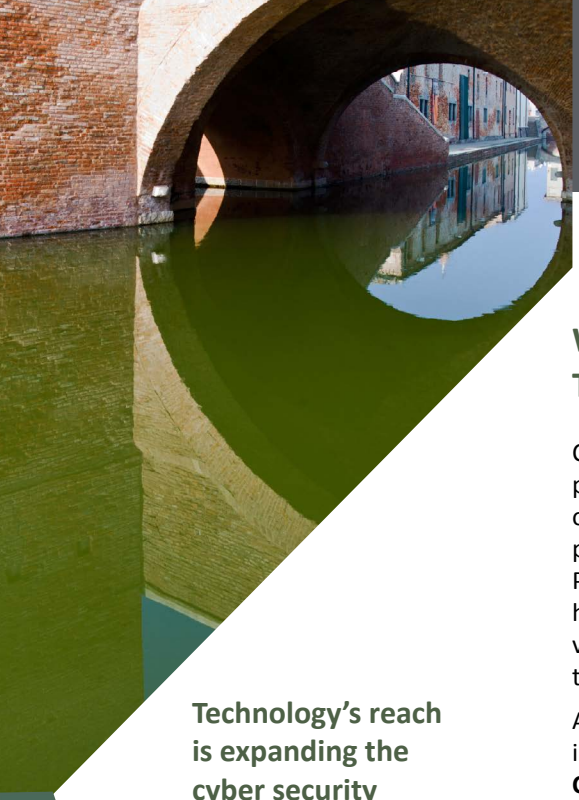
by Carson Associates

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?

Find What Matters . . .
Control What Counts



Technology's reach is expanding the cyber security battlefield. Emerging technologies will continue to blur the network perimeter, while sophisticated cyber-criminal methods will entice users and threaten the enterprise.

Why Risk Management?
The Battle Against Cyber Threats

Cyber criminals continue to find ways around current measures to protect information. In one of the most publicized data compromises of the year 47,000 Social Security numbers, corporate emails, internal proprietary data and unreleased movies were taken from Sony Pictures, as reported by media outlets such as Wired. In this incident, hackers gained access by equipping a malware program with a stolen valid digital certificate. This allowed the attackers to bypass various types of security controls.

As technology continues to evolve, organizations will continue to face increases and changes in security risks:
Cloud Computing - Adopting cloud architecture allows organizations to tap into never before seen levels of efficiency, but at the same time, opens them to risks and vulnerabilities as information travels to and from protected networks via public pipes, creating more opportunities for data contamination or theft.

Bring Your Own Device (BYOD) – BYOD, especially mobile devices, is becoming more popular, but trying to manage multiple platforms brings greater risks.

Social Networking - Social networking sites (e.g., Twitter, Facebook, Snapchat) continue to grow in popularity, exposing large amounts of personal information. With this exposure, along with increased online financial transactions, our vulnerability to identity theft is increasing. No surprise then, that it has become the fastest growing crime in the United States. The Federal Trade Commission (FTC) estimates more than 109 million Americans have their identities stolen each year. Safeguarding and protecting personal identifiable information (PII) in both commercial and Federal Government systems is more critical than ever before. Industry and the Federal Government have put standards and guidance into place as a preventive measure to protect PII; however, criminals continue to find ways around these measures.

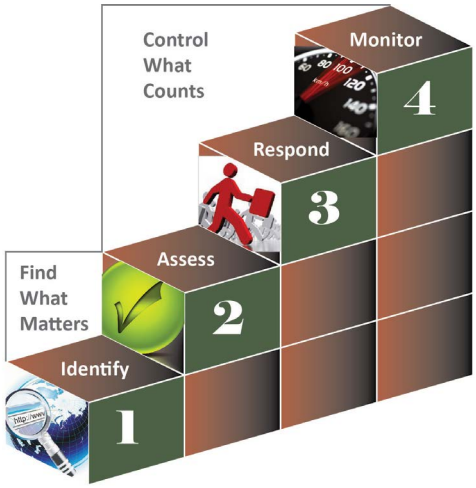
Personal Information (PII) Data Storage and Integrated Architectures – Yes, the ability to hack computer systems is often the principle culprit in cyber-crime. There are many reasons to protect PII beyond just the threat of identity theft, as our entire information environment becomes more integrated. In fact, this integration increases the potential for information misuse at many levels, driving greater risk and more complex risk scenarios to be dealt with.
Since you can't safeguard yourself from every possible risk, the best way to protect your organization is through an operational Information Technology Risk Management (ITRM) program.

What is Risk Management?
Find what matters - Control what counts

Who will be able to accept the responsibility for risk? It needs to be someone with budget authority so controls requiring resources can be applied when needed.

An effective Risk Management Process, as shown in Figure 1, is the identification, assessment, response, and monitoring of risk to your organization's information infrastructure, and therefore its mission. The goal is to reduce the potential impact from a threat exploiting an organization's vulnerabilities. No organization has the resources to monitor and control **everything all the time** - therefore you need to manage risks carefully and prioritize and develop measured responses by **finding what matters** and **controlling what counts**.

Figure 1: Find/Control Risk Management Process



Risk Management Strategy

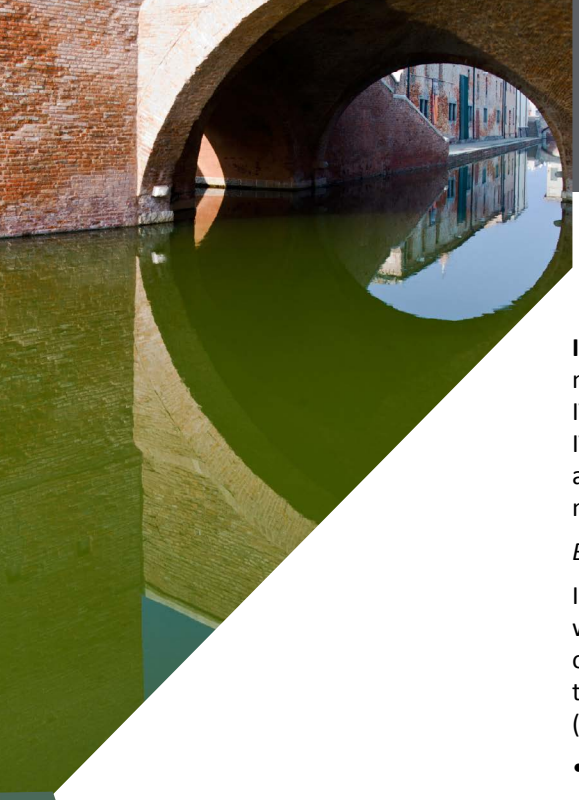
A successful ITRM program starts with a well thought out risk management strategy strongly supported by leadership. Proper planning will help you develop a viable ITRM program with the ability to identify threats and adapt promptly to defuse them. A risk management strategy will document how your organization intends to identify, assess, respond to, and monitor risks.

Some of the high-level considerations when documenting a risk management strategy include:

- Who will be accountable for risks and do they have budgetary control that will allow them to apply the necessary resources to mitigate risks?
- Who will be responsible for managing the day-to-day ITRM program?
- How will accountability be maintained for personnel with risk management responsibilities?
- Does my organization already have an overall risk management program? If so, where will my ITRM program overlap and what resources should be shared across the programs?
- What training is available for personnel with risk management responsibilities?
- What existing tools can I use to assist with the risk management process?

Now - Find What Matters
Step 1: Identify

The first component of a risk management program is to identify the elements necessary to frame the program.



Identify the scope - The identification of the scope is one of the most critical components of this step. The scope determines what IT components and organizations will be considered as part of your ITRM program. ITRM program scope affects the range of information available to make risk-based decisions and is determined by the senior management that is requesting the risk management strategy.

Business Impact Analysis

In order to understand the scope of what you are protecting and why you're protecting it, you must start with understanding your organization's mission and what business functions/ processes support the mission. To do this you should execute a business impact analysis (BIA), which will help to determine:

- Which IT components support which business functions/ processes
- Personnel supporting your organization's business functions/ processes
- External organizations dependent on the continuation of your organization's mission
- The Maximum Allowable Outage time for IT components
- A priority for the resumption of components
- Business function/ process criticality
- How you choose to respond to risks affecting business functions/ processes and ultimately the overall mission of your organization

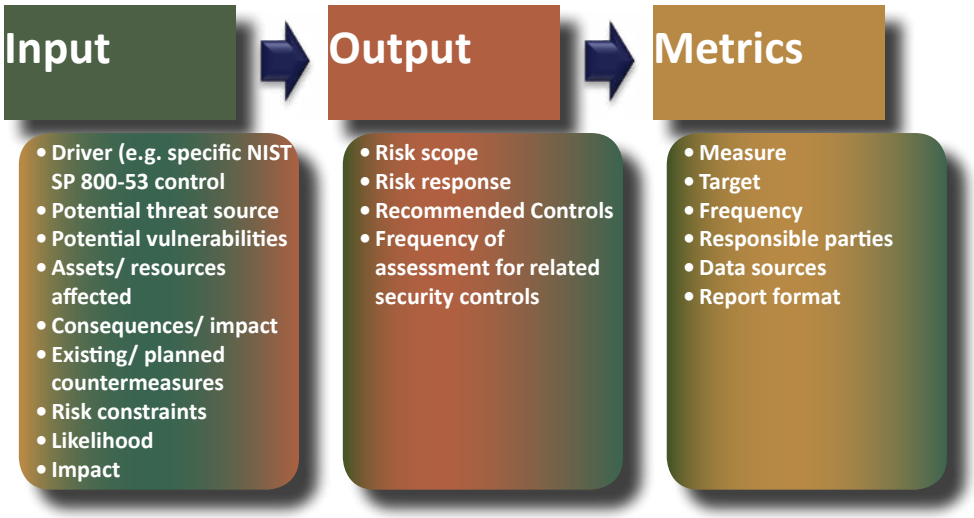
Identify Assumptions, Constraints, and Risk Tolerance - As part of the risk framing step in the overall risk management process, organizations identify the specific assumptions, constraints, and risk tolerance used to make investment and operational decisions in regards to risks. Understanding these 'risk profiles' will increase the chances of a successful and well thought-out risk management strategy:

- Risk Assumptions – A common frame of reference for addressing risks throughout your organization.
- Risk Constraints - Limitations or restrictions on your organization's ability to respond to risk (e.g., lack of funds, technology limitations, bureaucracy)
- Risk Tolerance - The level of risk your organization is willing to accept.

Risk Profiles

As mentioned earlier, risk profiles (elements of which are shown in Figure 2) help to capture the risk assumptions, constraints and tolerances. They promote a common terminology and frame of reference for comparing and addressing risks across your organization's business areas.

Figure 2: Elements of a Risk Profile



Identify tools - As a part of this step, identify what tools you have at your disposal to assist in risk management:

- Vulnerability scanning/ asset management tool to identify vulnerabilities and discover network components
- Risk management applications/ software

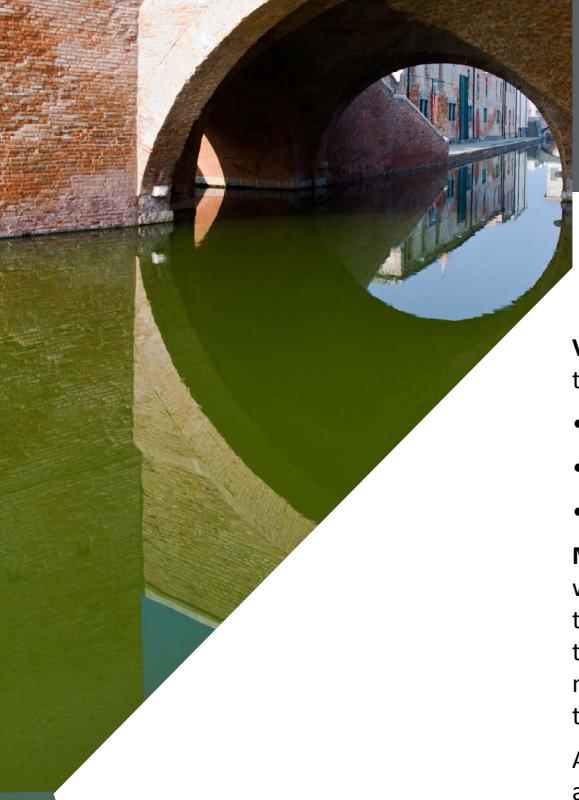
Identify Expectations and Training Needs - For those personnel responsible for managing risk, clearly define the responsibilities and expectations, and develop a training plan. Training organizations (e.g., SANS, INFOSEC Institute), social networks (e.g., LinkedIn groups, GovLoop), and professional organizations and certifications (e.g., ISACA, ISC2) can provide the training you need to help staff stay informed, and ahead of emerging threats.

Now Control What Counts
Step 2: Assess

In step 2, you need to identify a risk model that will be used to assess your risk. Regardless of the risk model used, similar components are identified.

Threat-sources - Determine what threat sources can exploit the vulnerabilities of your organization. Some useful sources in determining threat-sources to your organization can include:

- Historical data (past incidents and frequency of incidents or threats listed on previous assessments)
- Brainstorming amongst various business units
- Threats that may have occurred at similar organizations
- US Computer Emergency Readiness Team (CERT)
- Federal Emergency Management Agency (FEMA) (e.g., environmental threats)
- Your insurance agency



Vulnerabilities - Vulnerabilities can be determined through several techniques (or a combination of techniques):

- Vulnerability scanning tools
- Penetration Testing
- Assessments (interview, examine, test)

Matching threats to vulnerabilities – Once you have determined what your threat-sources and vulnerabilities are, your model needs to define the strength of their relationship. Matching threat sources to vulnerabilities is not always a one-to-one scenario. You may have multiple threats that can exploit a single vulnerability or one threat that can exploit multiple vulnerabilities.

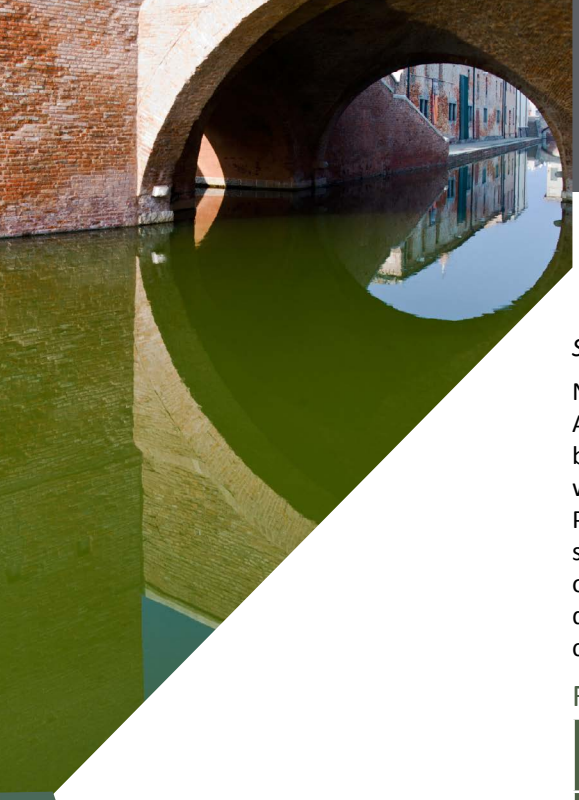
A documented approach to determine the likelihood and impact of a threat-vulnerability match occurring should be established so the overall risk determination is consistent. This can be done through a qualitative approach, quantitative approach, or semi-qualitative/ combination.

Qualitative Approach

A qualitative approach offers flexibility in how you respond to risks. In Figure 3, we show a qualitative scale for Event Likelihood and Impact, and show the degree of potential severity of an incident based upon the intersection of the two scales, e.g. the intersection of a "moderate event likelihood' with a 'high impact' results in a 'moderate" incident severity. Each organization needs to look at the intersection points and make its own judgments on the weighting it wants to assign.

Figure 3: A Qualitative Approach to Risk Assessment

Event	Impact				
Likelihood	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low



Semi-Quantitative Approach

NIST Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments was revised to offer a semi-quantitative approach. It can be used for both risk profiling and to determine the frequency with which security controls should be assessed. According to NIST Special Publication 800-30, Semi-quantitative assessments typically employ a set of methods, principles or rules for assessing risk using bins, scales, or representative numbers. Figure 4 below is an example of a semi-quantitative risk assessment, and Figure 5 is an example of a security controls assessment schedule.

Figure 4: Semi-Quantitative Risk Assessment

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	1-4	1	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

Risk scoring and risk profiles can be used to determine security controls assessment frequency.

Figure 5: Security Controls Assessment

Qualitative Values	Example Risk Score Range	Frequency of Security Control Assessment Example 1	Frequency of Security Control Assessment Example 1
Very High	1000 - 825	Bi-weekly	Monthly
High	825 - 650	Monthly	Quarterly
Moderate	650 - 475	Quarterly	Annually
Low	475 - 300	Annual	Every two years
Very Low	300 - 1	Annual	Every three years

Continue to Control What Counts
Step 3: Respond

Risk response can include risk acceptance, risk avoidance, risk mitigation, and/or risk sharing/transfer. Each of these is explained in Figure 6. How you respond to risk will depend on identified assumptions, constraints, and your organization's tolerance toward each risk.

Figure 6: Risk Response Approaches

Risk Response	Explanation	Cost
Risk Acceptance	The risks within your organizational risk tolerance	Low in costs initially, but if risk is realized, may be costly
Risk Avoidance	Taking actions to completely eliminate the technology or activity that is the foundation for the risk	Can be costly (and risk avoidance measures are not always guaranteed)
Risk Mitigation	The appropriate response for that portion of risk that cannot be accepted, avoided, shared, or transferred	Cost may vary depending on the risk and the solution used to mitigate or reduce the risk
Risk Sharing/ Transfer	Shifting risk liability and responsibility to other organizations (e.g., using insurance to transfer risk from your organization to an insurance company)	Cost-effective when risk transferred to a competent, properly prepared owner

Continue to Control What Counts
Step 4: Monitor

Continuous Monitoring (CM) – NIST defines Continuous Monitoring as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. 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. This involves moving from documentation-based security to a greater reliance on automation of security. As part of your risk management strategy, you should have a documented continuous monitoring capability that:

- Determines what to monitor based on a risk assessment
- Establishes a frequency of monitoring based on types of risks
- Establishes automated tools for near real-time monitoring
- Develops metrics to determine effectiveness and uses results to fine-tune continuous monitoring and risk management strategy.

The Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) framework and SANS Top 20 Critical Security Controls are just two approaches that can be used to assist with a continuous monitoring capability. There are others, so you will need to choose the method that best fits your organization. Implementation time, cost, and complexity are a few factors to consider when making this choice. In addition, a hybrid of several methods may be used, or seeking a commercial tool that has already automated this process can be another choice. For this discussion, we will further explore CAESARS and SANS Top 20.

Continuous Monitoring and CAESARS Framework

Multiple external systems will interface with your continuous monitoring capability and the domains on which you choose to focus. The Department of Homeland Security, Federal Network Security Branch identifies 11 domains within their CAESARS Reference Architecture Report. These domains include the following:

- Vulnerability Management
- Patch Management
- Event Management
- Incident Management
- Malware Detection
- Asset Management
- Configuration Management
- Network Management
- License Management
- Information Management
- Software Assurance

The CAESARS Reference Architecture Report resulted from collaboration between the Departments of State, Justice, and Treasury and allows for the assessment of an organization's security posture on a near real-time basis, moves risk management from a point-in-time process to a continuous risk management process, and focuses on controls that can be automated.

Although CAESARS is not a full risk management capability, its framework can serve as a major component of your ITRM program.

As depicted in Figure 7, CEASARS contains four subsystems:

Figure 7: CEASARS

Sensor Subsystem - The sensor subsystem should provide the ability, on an enterprise-wide basis, to monitor and identify weaknesses in security configuration settings in computing and networking assets throughout their system life cycles. It includes all platforms upon which CAESARS is expected to report, including end-user devices, database servers, network servers and security appliances.

Database/Repository Subsystem - The CAESARS Database/ Repository Subsystem should house all data collected by the Sensor Subsystem and transferred to CAESARS. It also includes any tools required to perform data pull operations from the Sensor Subsystem platform.

Analysis/Risk Scoring Subsystem – Consists of analytic risk analysis/ scoring tools (centralized and decentralized).

Presentation and Reporting Subsystem – Presentation tools/ dashboards.

Continuous Monitoring and SANS Top 20 Critical Security Controls

The SANS Top 20 Critical Controls are based on security controls that are effective in blocking currently known high-priority attacks as well as

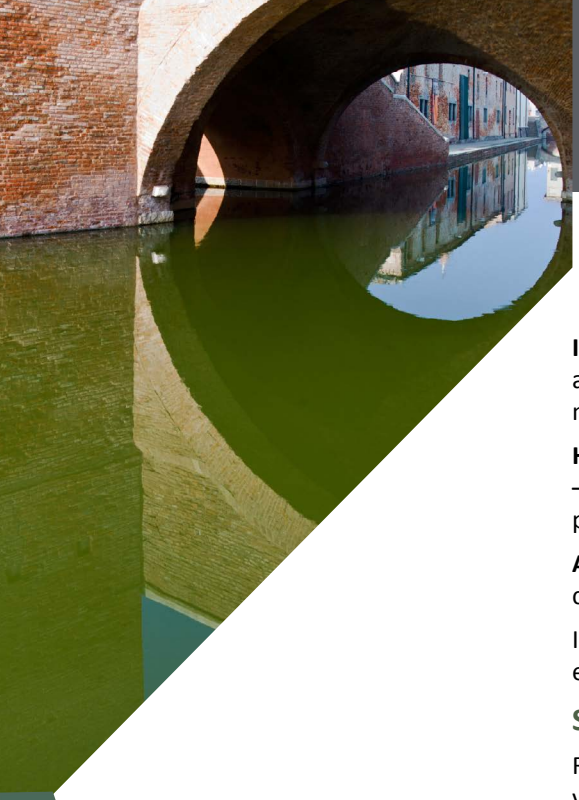
those attack types expected in the near future.

The Controls represent a prioritized baseline of information security measures and are designed to support organizations with different levels of information security capabilities. The SANS approach is "offense must inform defense" and that's what the implementation of the 20 security controls is designed to achieve. SANS's Top 20 Critical Security Controls include the following:

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Protection
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

Each control is broken in to four areas for implementation purposes:

Quick wins - fundamental aspects that rapidly improve the security stance generally without major procedural, architectural, or technical changes to the environment



Improved visibility and attribution – Improving the process, architecture, and technical capabilities so your organization can monitor

Hardened configuration and improved information security hygiene – Improve security posture by reducing the number and impact of potential security vulnerabilities

Advanced - Further improves security beyond the other three sub-controls

In addition, SANS's website provides "user-vetted tools" to implement each control (free and fee-based).

Summary

Risk must be pro-actively managed to identify and respond to new vulnerabilities and minimize cost associated with a breach of security. A risk management strategy will help you develop a sustainable and dynamic ITRM program. Continuous monitoring will help you control what matters, provide a near real-time awareness of your security posture, and Influence management decisions and buy-in.

About Carson Associates

Your Bridge to Better IT

Carson Associates has 22 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 comply with the evolving changes in federal security guidance, send a message to: *marketing@carsoninc.com* or call and ask for *Diane Reilly at 301.656.4565*