Automate
Risk Management Framework
Providing Dynamic Continuous Monitoring, Operationalizing Cybersecurity and Accountability for People, Process and Technology

Computer Network Assurance Corporation (CNA)
Risk Management Framework (RMF)

Risk Management Framework (RMF) provides a structure for managing information system risk. Managing information system risks to the organizational operations includes knowing the pieces (i.e., People, Process and Technology) that make up the infrastructure and an understanding of how those infrastructure pieces works together to provide results.

This risk management process being described changes the traditional focus of Authorization (formally known as Certification and Accreditation (C&A)) as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions. Enabling a consistent, repeatable and comparable approach for information systems and organizations.

Knowing

Your knowledge of what makes up the infrastructure must be factual. It starts with knowing the "People" involved in making the system work. Having knowledge on each of the System Administrators. Having knowledge of which System Administrator is assigned to each device (e.g., server, desktop, laptop, firewall, router and switch to name a few) throughout the entire enterprise and having each of the System Administrators' phone numbers and email addresses. Having the history on each System Administrator of all activities done on each of the devices throughout the entire enterprise.

Having knowledge of each ISSO. Having knowledge of which ISSO is assigned to each system (e.g., OPS Backbone, Server Farm, Admin LAN) throughout the entire enterprise and having each of the ISSOs' phone numbers and email addresses. Having the history on each ISSO of all activities done on each of the systems throughout the entire enterprise. Having this knowledge on all of the people (e.g., AO, SO, CA and Users) having any role on the device, system and enterprise is crucial.

Another key component of the infrastructure is "Process". Your knowledge on the processes that are being implemented on each device, system, and enterprise is vital and adds to your abilities to have collaboration. Having knowledge of how each device, system, and enterprise are reviewed, updated and fixed. Having knowledge of how POA&Ms are assigned, updated, fixed, verified and cleared. Having knowledge of how Configuration Management Plan and Procedures is done with key role player’s interactions. Having knowledge on how Contingency Plan and Procedures are acted on with key role player's interactions. Having knowledge on how maintenance is done on each of the devices throughout the system and enterprise.

The final key component of the infrastructure is "Technology". Your knowledge on the technologies that are being utilized for each device, system, and enterprise is essential and adds to your knowledge of their capabilities and limitations. Having knowledge of what specific technology is in use for each device, system and enterprise. Having knowledge of what operating system is on each of the devices throughout the system and enterprise. Having knowledge of what applications are on each of the device throughout the system and enterprise.
Working Together

So now that you know each device in each of your systems throughout the enterprise, you know each assigned System Administrator for each device, you know the process for having each device updated, you know all known vulnerabilities and you know how to correlate each vulnerability to each of the devices, Now you have the ability to be notified or have the right System Administrator notified within seconds of a new vulnerability enterprise wide. This notification to the System Administrator can show him/her the description of the vulnerability, the fix action, the device that needs updating and the timeline of the action. These notifications are fully automated and scheduled to be re-issued with escalation notifications to secondary points of contact or supervisors. With this data/information/knowledge at hand you would be able to pull the history of works done on each device or history of all works done by a certain System Administrator. Automatically after the System Administrator finishes their fix action activities, the POA&M is updated/cleared, the inventory updated, the configuration control board notified of the works done, why and by whom and all pertinent Authorization Package documentation updated automatically.

Enterprise wide collaboration is a reality. For example, an incident report on a new vulnerability is put together by someone in the field then automatically pushed to the right points of contact such as the CIRT. The CIRT researches the issue and develops a fix action. Now the CIRT can instantly have a full report on how this new vulnerability affects the entire enterprise, a “Look Ahead”. Next the CIRT is able to commit this new vulnerability to the enterprise's custom vulnerability database and within minutes the System Administrators that are the point of contact for the specific devices that are at risk are notified of the new vulnerability. Those System Administrators receive their notification via email, phone call or text message, then clicks on the notification and instantly brought to their account and is provided with a description of the vulnerability/issue, the name/IP of the device, the fix action to be taken and the schedule of the activities. A management report can show in near real time all the actions or non-actions to every device/system enterprise wide.

According to NIST SP 53 Rev 3, the Risk Management Framework (RMF) has the following characteristics:

1. Near Real-Time Continuous Monitoring – “Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;”
2. Management Reporting – “Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;”
3. Birth to Grave IT Asset Management – “Integrates information security into the enterprise architecture and system development life cycle;”
4. Govern the System Security by the Security Controls – “Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems;”
5. Operationalize Cybersecurity – “Links risk management processes at the information
system level to risk management processes at the organization level through a risk executive (function); and”

6. **Common and Inherited Controls** – “Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).”

---

Enabling a consistent, repeatable and comparable approach for information systems and organizations.

---

1. **Near Real-Time Continuous Monitoring** – “Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;”

Continuous Monitoring is the managing and tracking the security state of the information system. Continuous Monitoring is the combination of three elements IT Asset Inventory, Configuration and Change Management and Vulnerability Management. Together these three elements allow the organization to have awareness of risk to their system. This materializes by understanding what you have (i.e., System Inventory); how, who, when and why are changes made to your system (i.e., Configuration & Change Management) and what are the flaws in the system that others can take advantage of (i.e., Vulnerability Management). Putting together these three elements with automation provides near real-time knowledge of the systems risk.

- **IT Asset Inventory** includes all elements of software and hardware that are found in the network environment and is the primary point of accountability for the life-cycle management of information technology assets throughout the organization.
- **Configuration & Change Management** manages the change process for a) hardware, b) system software, c) communications equipment and software, and d) all documentation and procedures associated with the running, support, and maintenance of live systems.
- **Vulnerability Management** is accomplished following the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities in the software of computing systems.

This continuous monitoring program transforms an otherwise static (Document centric) security control assessment and risk determination process into a dynamic (Knowledge centric) process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system. This ability provides organizations with an effective mechanism to automate updates to *security plans, security assessment reports, plans of action and milestones* and the entire authorization package. Now, these documents in the authorization package are “living documents” and updated accordingly based on actual events.

- **Automated Authorization and Assessment (A&A) Documentation Creation** is accomplished for the required A&A documentation package to accredit a system. The information and supporting evidence needed for security authorization is developed
during the detailed security review of an information system, typically referred to as security assessment.

This automation of the continuous monitoring program significantly reduces the level of effort required for the authorization and the reauthorization of the information system.

- **Re-Authorization** is much less time consuming thanks to living data/information/knowledge and no more rewriting documents. Achieve ongoing authorization.

---

2. **Management Reporting** – “Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;”

Management reporting is an automation report capability for management on each device, system and enterprise. This ability provides the decision maker a view they have never seen. The summation and summarization of any and all authorization packages and reports across the entire enterprise or for any specific system or for any specific device, 24 hours a day. Some of the reports that management can request and have fulfilled in seconds are: Risk Assessment Results, Contingency Test Results, Security Assessment Results, POA&M Reports, FISMA Reports, and Custom Report and Matrix.

- **Automated Reporting (POA&M and FISMA)** generates the charting, analysis, and reporting functions that support the customer in their review and prediction of risk.

The old expression of judging apples to apples is a reality as a common look and feel reporting is implemented throughout the enterprise. This standardization can be pushed throughout the enterprise to include but not limited to:

- **Report Management**
  - Status Reports (Enterprise, Division, Unit, or System)
  - Work Flow (Enterprise, Division, Unit, or System)

- **Document Management**
  - Standardize (Completeness and Format)

- **Configuration Change Management**
  - Automated device configuration updates

- **Authorization Management**
  - Authorization and Reauthorization
3. **Birth to Grave IT Asset Management** – “Integrates information security into the enterprise architecture and system development life cycle;”

Birth to Grave IT Asset Management means just that, from the time the asset becomes part of the system, to the time it is scraped for trash, the organization needs to “know” everything about the asset. Some of the things the organization needs to “know” are: what is the asset; where is the asset; who is maintaining the asset; what system is the asset part of; what operation will the asset be part of; and what vulnerabilities does the asset have. The organization needs to “know” this information every minute of the day.

A system is a set of assets structured together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Some of the specific information the organization needs on each asset includes, but not limited to: Technology, Operating System, Gateway Information (Up & Down), Application Information, Port Information, Physical Address, Authorization Official, System Owner (Name & Contact Information), and System Administrator (Name & Contact Information).

The system’s configuration and change management needs to be robust enough to “know” when changes to the system are accomplished and that other related task are done for each asset including, but not limited to: the system description and inventory is automatically updated; a “Change Request Form” is automatically generated; automatic notification to the Change Control Board (CCB) done; the POA&M is automatically updated; and all authorization and assessment documents are automatically updated.

4. **Govern the System Security by the Security Controls** – “Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems;”

Having knowledge on the status of each device and how it is implementing each security control is paramount. The entire methodology and process needs to be based on the real security requirements (i.e., Security Controls). Automation of this entire RMF insures that data, information and knowledge rules and not personalities. Security controls are broken into three classes (i.e., management, operational, and technical). These controls are the safeguards or countermeasures employed within a system to protect the confidentiality, integrity, and availability of the system and the information that is manipulated, shared and stored on the system. The security control’s effectiveness is the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for that system’s operational environment.
The organization needs to understand the risks and other factors that could adversely affect operations and assets, individuals and other organizations. The organization’s officials must understand the status of their system security posture current and what is planned in order to make informed judgments and investments that mitigate risks to an acceptable level.

5. **Operationalize Cybersecurity** — “Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and”

Operationalize cybersecurity is the mechanism for: visualizing, understanding, and assimilating the broad scope and complexities of cybersecurity through graphic, tabular, or textual means. The collection of data/information/knowledge throughout the enterprise on the technologies in use, the understanding of the processes involved combined with the awareness of everyone’s role in the system provides for instant and continuous reporting.

- **Situational Awareness (SA)** involves being aware of what is happening around you to understand how information, events, and your own actions will impact your goals and objectives, both now and in the near future. Having complete, accurate, and up-to-the-minute SA is essential. SA has been recognized as a critical, yet often elusive, foundation for successful decision-making across a broad range of complex and dynamic systems.
- **Collaboration** is a recursive process where organizations work together in an intersection of common goals by sharing knowledge, learning, and building consensus. This collaboration is being done between people to people, system to system and even enterprise to enterprise.
- **Incident Response** reporting capability from anywhere in the enterprise with automatic reporting feeds. Automation of the action report to be instantly sent to just those points of contact that need the information and being able to track each of these action reports as well as each of the devices that need the fix action to be applied on.
- **Look Ahead™** provides an instant view of how a new vulnerability could affect your entire enterprise by device or system.
- **Interaction (Q&A)** with your enterprise data to get answers to questions, like what devices in what systems has port 23 open.
- **Automated Notification** is accomplished for the initial and updated POA&Ms, FISMA Report, Authorization Task, Incident Report, Configuration Change Report, and Custom Matrix Reports to the responsible parties.

6. **Common and Inherited Controls** — “Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).”
Another cost savings that is done for the organization is the introduction of common and inherited/hybrid controls. These common and inherited/hybrid controls are automatically inputted into the organization/system/enterprise processes and documentation, therefore reducing the cost of implementation of that security control by each organization/system/enterprise.

- **Common:** A higher-level organization provides the implementation for the security control identified as common. Controls designated as common are to be cited in all the organization’s System Security Plan (SSP) and in the security control test artifacts included in the authorization package.

- **Inherited/Hybrid:** A higher-level organization provides support for part of the security control for its system. These controls require that system-specific compliance be stated within the SSP in sufficient detail at the designated level.

The objectives of developing Common Controls are to enable the organization to accomplish its mission by: 1) better securing the IT systems that store, process, or transmit organizational information; 2) providing a structured process of planning adequate, cost-effective security protection; and 3) assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the well-documented security controls established as common controls for the organization’s environment.

**Return on Investment**

**Accountability for People, Process and Technology**

*Management Reporting* includes all elements of people, process and technology. This is crucial for the accountability for each individual and their roles in implementing the security controls; for each process as it standardizes the actual services to the system; and for each asset as it fulfills its part in carrying out its portion of the operations throughout the organization. History reports bring knowledge to the management on: what each System Administrator has done for the time they have worked on the device/system/enterprise; what, who and why a device/system/enterprise has been changed throughout its life cycle; and when each of the device/system/enterprise needs to be reauthorized or assessed.

**Dynamic Continuous Monitoring**

*IT Asset Inventory* includes all elements of software and hardware that are found in the network environment and is the primary point of accountability for the life-cycle management of information technology assets throughout the organization.

*Configuration & Change Management* manages the change process for a) hardware, b) system software, c) communications equipment and software, and d) all documentation and procedures associated with the running, support, and maintenance of live systems.

*Vulnerability Management* is accomplished following the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities in the software of computing systems.
Operationalizing Cybersecurity

**Situational Awareness (SA)** involves being aware of what is happening around you to understand how information, events, and your own actions will impact your goals and objectives, both now and in the near future. Having complete, accurate, and up-to-the-minute SA is essential. SA has been recognized as a critical, yet often elusive, foundation for successful decision-making across a broad range of complex and dynamic systems.

**Collaboration** is a recursive process where organizations work together in an intersection of common goals by sharing knowledge, learning, and building consensus.

**Incident Response** reporting capability from anywhere in the enterprise with automatic reporting feeds.

**Look Ahead™** provides an instant view of how a new vulnerability could affect your entire enterprise.

**Interaction (Q&A)** with your enterprise data to get answers to questions.

**Automated Notification** is accomplished for the initial and updated POA&Ms, FISMA Report, Authorization Task, Incident Report, Configuration Change Report, and Custom Matrix Reports to the responsible parties.

**Doing More with Less**

**Automated Authorization and Assessment (A&A) Documentation Creation** is accomplished for the required A&A documentation package to accredit a system. The information and supporting evidence needed for security authorization is developed during the detailed security review of an information system, typically referred to as security assessment.

**Automated Reporting (POA&M and FISMA)** generates the charting, analysis, and reporting functions that support the customer in their review and prediction of risk.

**Re-Authorization** is much less time consuming thanks to living data/information/ knowledge and no more rewriting documents. Achieve ongoing authorization.

Cyber Profile™ is the next generation tool for automating Risk Management Framework (RMF), cybersecurity risk management and FISMA compliance. Designed to provide a real-time picture of an enterprise’s security posture, Cyber Profile™ does away with “snapshots” of security. Using asset level data, Cyber Profile™ gives those responsible for information systems security the granularity needed to truly secure systems and ultimately, their enterprise.

Cyber Profile™ works alongside existing security measures and automated monitoring tools (e.g. client-based agents). Collecting the data from these tools, the National Vulnerability Database, and penetration/vulnerability testing tools, Cyber Profile™ maps all system vulnerabilities in the
enterprise down to the asset level and their associated systems, correlating vulnerabilities to the mission impact.

Identified vulnerabilities result in automatic POA&M generation, security task assignments, email notification, and remediation progress tracking.

Employing a Risk Management Framework-aligned work flow management approach, Cyber Profile™ collects and analyzes the critical system security information, enabling both continuous monitoring and one-step, automated Authorization document package generation. Unlike other document centric tools, Cyber Profile™ knowledge-centric model creates efficiencies in managing organizational security and eliminates the episodic and document-driven approach to security management.

A multi-faceted security application, Cyber Profile™ combines systems data/information/knowledge, the guidelines and requirements established by NIST, and vulnerabilities and exploits data to more effectively manage cybersecurity risk. In highly diverse environments, where there are complex and sophisticated cyber threats and ever increasing vulnerabilities, Cyber Profile™ is the only solution providing near real-time Situational Awareness for Real-time Decisions™.
## ROI

Risk and Cost evaluation for 4 years for Authorization requirement, Continuous Monitoring, and Annual Security Controls Testing.

*All values are per system (system size is Medium)*

**Dollars are in thousands**

<table>
<thead>
<tr>
<th>RISK</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CP</td>
</tr>
<tr>
<td>Initial</td>
<td>100</td>
</tr>
<tr>
<td>C&amp;A Yr1</td>
<td>30</td>
</tr>
<tr>
<td>Accomplish CM Yr1</td>
<td>27</td>
</tr>
<tr>
<td>Controls testing Yr2</td>
<td>25</td>
</tr>
<tr>
<td>Accomplish CM Yr2</td>
<td>23</td>
</tr>
<tr>
<td>Controls testing Yr3</td>
<td>21</td>
</tr>
<tr>
<td>Accomplish CM Yr3</td>
<td>19</td>
</tr>
<tr>
<td>C&amp;A Yr4</td>
<td>13</td>
</tr>
<tr>
<td>Accomplish CM Yr4</td>
<td>11</td>
</tr>
</tbody>
</table>

| Total cost for a 4 year cycle | $154 | $370 |
With Cyber Profile™ risk is on a steady decline.
With Cyber Profile™ cost is a factor lower and more predictable.
Cyber Profile™ lowers your cost and risk.