5 Traps to Avoid as a New CISO

Second Renaissance®

CONTENTS

FIVE TRAPS to avoid

Chief Information Security Officers (CISOs) around the world are challenged by the pace of the mission, increased scope, and flattened budgets. Regulations seemingly come out of nowhere. Keeping up has become the new goal; rather than keeping the mission secure.

Regardless of industry, CISOs and their cybersecurity programs head down the wrong path as requirements, regulations, and the mission itself evolves. While budget constraints are at the heart of many major decisions, the balance of cost and security is at its core a risk management decision and in line with healthy cybersecurity practices. Budget constraints are also largely outside the control (although not outside the influence) of a CISO. Five avoidable traps within a CISO's control, that drain resources for a cybersecurity program are: Loss of Purpose, Internal Disconnect, Playing out of Position, Culture of "NO", and Wasted Effort. Each trap can drain the organization of resources, weaken security posture, and even lower morale of the organizations' cyber warriors.

When the 'why' of program elements cannot be explained succinctly, the organization has fallen into the **LOSS OF PURPOSE TRAP**. Cybersecurity programs did not exist 15 years ago (in many cases) and have experienced growing pains and program offshoots during the maturation process. Program elements exist because "they always have" or "we have to", without a current mission-driven purpose.

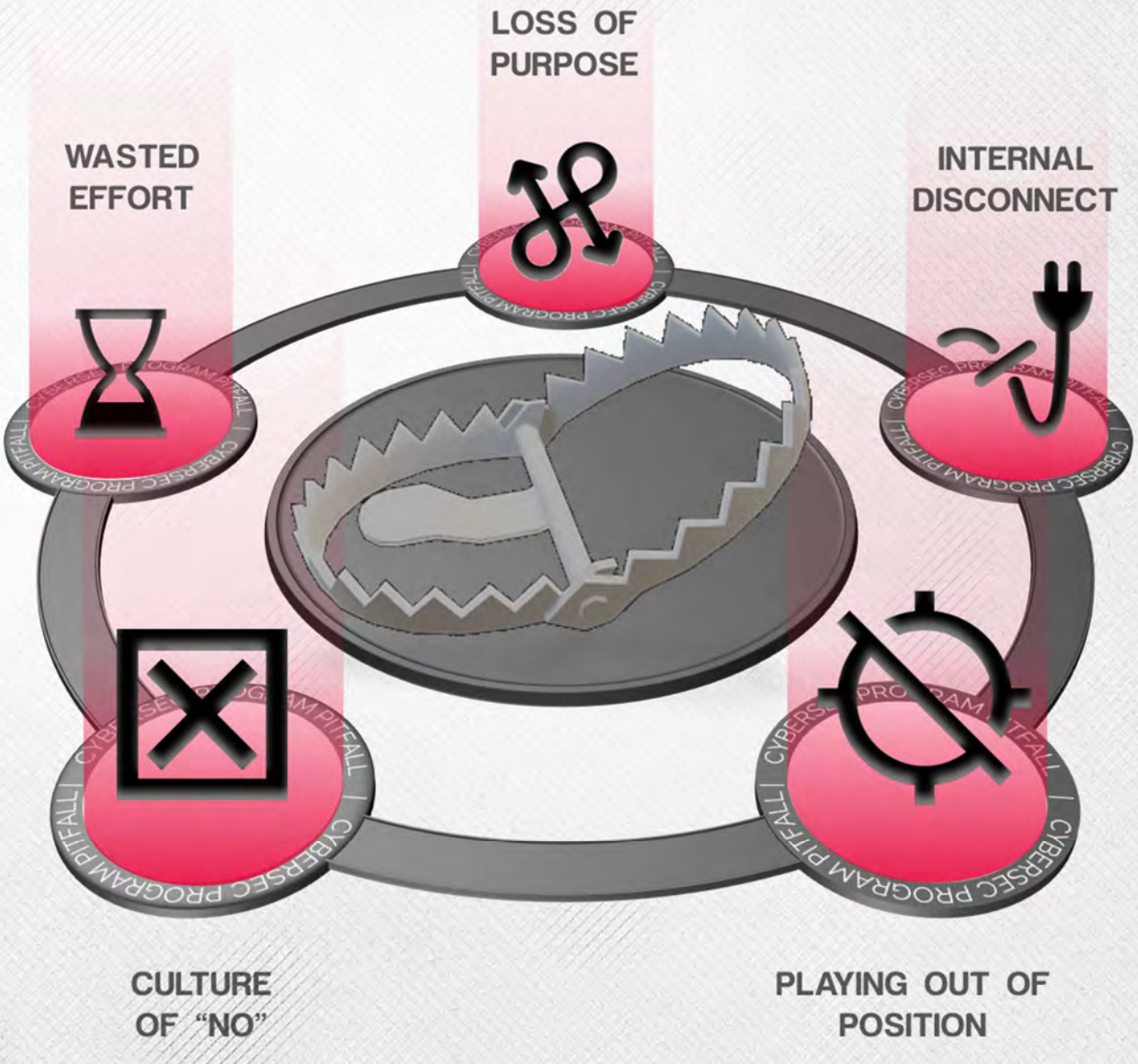
When all the elements of a cybersecurity program cannot be pulled together to form a cohesive picture of the mission-space, the organization has fallen into the **INTERNAL DISCONNECT TRAP**. Often, cybersecurity programs will operate in two or more functional silos, with little to no relationship between the organizations. Disjointed subprograms hinder leadership's ability to make informed decisions, and waste effort in translating between subprograms.

CISOs can be susceptible to the notion that their work is unique, and as a result require dedicated effort to tackle routine business. The **PLAYING OUT OF POSITION TRAP** is when CISOs decide to lead acquisitions, technology migrations and transformations, and other processes that are outside their responsibility and/or redundant with other programs within the organization.

The **CULTURE OF "NO" TRAP** is possibly the most pervasive and damaging to the program's long-term success. CISOs and CIOs alike can contribute to an organization-wide perception that security is an inhibitor to the mission. When cyber warriors aren't engaged in finding solutions to mission problems, they are seen as an enforcer of rules and inhibitor to mission success.

The **WASTED EFFORT TRAP** can take many forms, but always drains resources from more impactful work. Examples include controls applied to individual systems when enterprise solutions would be more efficient, creating documentation that is not often used or reviewed, and performing manual operations when automation is possible.

These Five Traps combine to trip up, distract, and hold captive CISOs and their cybersecurity organizations. When left unchecked, a cybersecurity program will degrade to an organization that doesn't think critically, slows the organization's innovation to a halt, holds a negative reputation within and outside the organization, and has low morale across its cyber warriors.



FIVE TRUTHS to embrace

Cybersecurity touches every aspect of a business. It is a complex and evolving requirement for all businesses and organizations that have information and services worth protecting. While there are traps that drain resources and hinder the mission, there are also truths that serve as foundational guideposts – ensuring the continued alignment of an organization's cybersecurity program with the overall mission.

Each of the five Truths is designed to overcome and avoid one of the five Traps that CISOs and their cybersecurity programs fall into. Loss of Purpose is overcome by Program Strategy; Internal Disconnects are remedied by Unified Communication; Playing out of Position is fixed when Strategic Partnerships are embraced; the Culture of "NO" is torn down with Delivery Integration; and Wasted Effort is redirected with Applied Risk Management.

A well-defined and maintained PROGRAM STRATEGY brings Truth and purpose to every cybersecurity program element. Program offshoots created during the maturation process are brought back into alignment with the overall mission.

Subprograms operating separately are connected through UNIFIED COMMUNICATION, which demonstrates how all subprograms work together to improve the cybersecurity resilience of an organization. Unified reports and dashboards improve leadership's ability to make informed decisions.

The Truth is that CISOs can't do everything well and must rely on STRATEGIC PARTNERSHIPS to ensure mission success. Partnering internally and externally with experts in the fields of acquisition, training, application development, and even managed security services frees up CISOs to focus on setting organizational direction, making risk-based decisions, and overseeing all aspects of cybersecurity integration within the organization.

A mission-enabling cybersecurity organization focuses on DELIVERY INTEGRATION – including cybersecurity early in strategic planning, and continually through system development and operations. In current terms, this means cybersecurity inclusion in Scrums, cybersecurity requirements in backlogs, vulnerability scans within the CI Pipeline, and full DevSecOps integration.

The truth is that Risk Management done to be compliant ultimately results in wasted effort, while APPLIED RISK MANAGEMENT continually delivers positive outcomes due to proactive management, regular tailoring, and continuous process improvement.

When these Five Truths are put into practice, a cybersecurity organization becomes a strength of the overall organization and a mission-enabler. Instead of slowing the pace of change, the CISO embraces change and ensures the cybersecurity posture of the organization increases with every sprint. Audits and Congressional Reporting (for Federal organizations) take less effort and yield more favorable results.

LOSS OF PURPOSE

When the 'why' of program elements cannot be explained succinctly, the organization has fallen into the **LOSS OF PURPOSE TRAP**. Cybersecurity programs did not exist 15 years ago (in many cases) and have experienced growing pains and program offshoots during the maturation process. Program elements exist because "they always have" or "we have to", without a current mission-driven purpose.

WE HAVE ALWAYS DONE IT THIS WAY

A US Government Agency reported weekly on Information Security Vulnerability Management (ISVM) Compliance for 50+ of its information systems. Estimated manpower to support this function measured in at 2.5% of the overall workload across the CISO's program. ISVM reporting was perceived as redundant with other weakness remediation activities.

When challenged with the question of 'why', organization leadership were not able to explain succinctly why the ISVM reporting process existing separately from other weakness remediation activities. "We have always done it this way" and "we are required to report it" were the most commonly received answers.

ADDITION BY SUBTRACTION

Without a comprehensive program strategy that linked all cybersecurity program elements to their purpose, there was no way to properly defend the ISVM Compliance program within this US Government Agency.

By building a program strategy, we were able to establish the requirements, clarify its relationship with other vulnerability management processes, and determine that reporting at the information system level was not, in fact, required by US Government or Cabinet-level policies and regulations. The process was adjusted to recoup almost all the effort expended; the equivalent of 2 full time resources, towards other high priority initiatives.

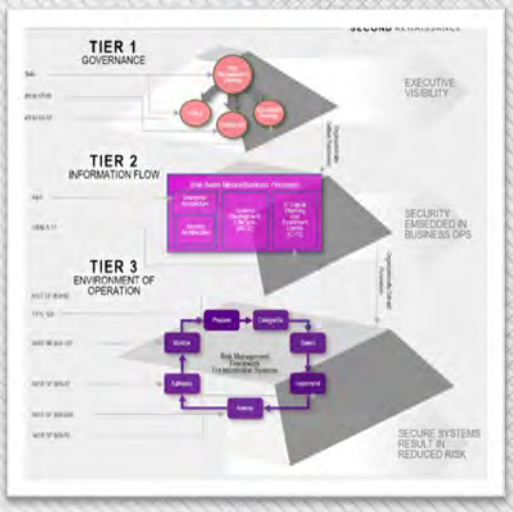
PROGRAM STRATEGY

A well-defined and maintained PROGRAM STRATEGY brings Truth and purpose to every cybersecurity program element. Program offshoots created during the maturation process are brought back into alignment with the overall mission.

A program strategy should be approached from three perspectives, in sequential order. First, align to the NIST Risk Management Framework (RMF) and specifically the three tiers of risk management. Second, map the program's requirements and trace those requirements down through program elements and individual tasks. Finally, evaluate "common sense" security activities that are being performed today and identify how these functions fit against the RMF and requirements map.

RMF Alignment. The NIST Risk Management Framework (RMF) is an excellent basis for a comprehensive cybersecurity program. The foundation for recommended strategic plans organizes activities into three tiers – governance, information flow, and environment of operation.

- ✓ **Governance** elements include policy, investment strategy, and key performance indicators (also referred to as a dashboard). This portion of strategy outlines risk tolerance within the organization, and key stakeholder roles across the organization.
- ✓ **Information Flow** weaves cybersecurity into the business – from Enterprise Architecture to development and operations practices, and even acquisitions.
- ✓ **Environment of Operation** is the portion of the RMF designed for individual information systems. This tier prioritizes activities and streamlines process delivery; including testing and documenting system security.



Second Renaissance's Applied RMF Methodology

Requirements Map. Federal CISOs, for example, have robust regulations for which to adhere starting with FISMA. By mapping FISMA through OMB Memoranda and Cabinet-level policy, a comprehensive taxonomy of all required cybersecurity activities is created.

Bottom-Up Analysis. Aligning existing activities to the Requirements Map (or FISMA Map for Federal CISOs) establishes the purpose behind each activity, and identifies gaps in unaddressed requirements, as well as unmandated functions.

Second Renaissance created the FISMAapp and FISMAmap to facilitate CISO Program analysis

INTERNAL DISCONNECT

When all the elements of a cybersecurity program cannot be pulled together to form a cohesive picture of the mission-space, the organization has fallen into the **INTERNAL DISCONNECT TRAP**. Often, cybersecurity programs will operate in two or more functional silos, with little to no relationship between the organizations. Disjointed subprograms hinder leadership's ability to make informed decisions, and waste effort in translating between subprograms.

SILOS PREVENT COLLABORATION

A Federal Agency operated in four functional silos – Security Operations, Compliance and Risk Management, Audit, and Policy. Each silo rarely interacted with the other. The Security Operations team reported all information from a network defense perspective – unaware of information systems hosted on cloud services or in third-party datacenters. Incident information could not be reconciled with information system boundaries. Compliance and Risk Management paid little attention to information system inventories. The Audit silo communicated directly with system owners and administrators, often asking for information that had already been provided to the Security Operations or Compliance and Risk Management teams. The policy group would author new policies without consulting their affected counterparts – which led to confusion, frustration, and rework across the board.

TEAR DOWN THIS WALL!

A Unified Communication plan was created that identified key touchpoints, aligned data, and consolidated reporting across the silos. The most impactful aspect of the plan started with tagging all assets in BigFix with an Information System ID, allowing for SOC reporting by Information System. This also enabled real-time information system inventory reporting for systems hosted at the Agency datacenter and GovCloud instance. The data alignment also enabled faster identification of responsible parties for incidents, and had the added benefit of rapid identification of rogue assets on the network. By combining the information, Risk Executives could make better informed decisions.

UNIFIED COMMUNICATIONS

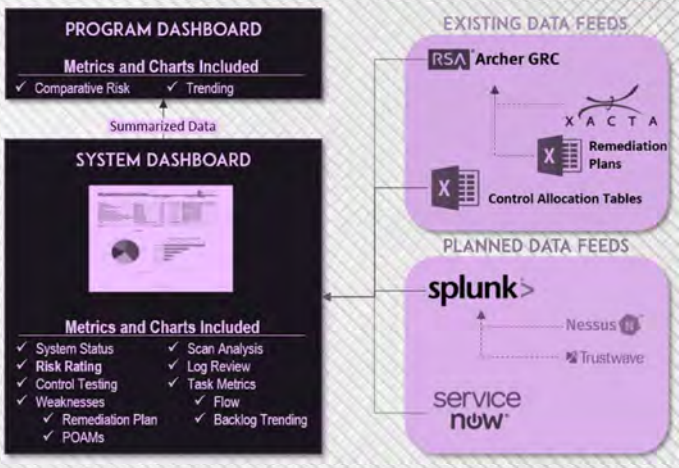
Subprograms operating separately are connected through **UNIFIED COMMUNICATION**, which demonstrates how all subprograms work together to improve the cybersecurity resilience of an organization. Unified reports and dashboards improve leadership's ability to make informed decisions.

- ✓ **Data Alignment.** Unified Communication starts with understanding how the program's information is related. By mapping out and connecting the disparate datasets, a process of data integrity improvement follows and finally data gaps are filled. With a unified dataset, the relationships between information can be explored across all communications – internal and external.

- ✓ **Communications Plan.** Identifying desired communications paths and acceptable modes of communication helps the cybersecurity program operate as one cohesive unit. It also reduces redundant communications, and thus reduces inconsistencies in communication between the program and its stakeholders.

- ✓ **Centralized Datacalls.** All cybersecurity programs suffer from datacalls after datacalls. Centralizing the program's datacall capability allows for standardized processes which increase response quality and integrity of data reported; and reduces impact across all stakeholders as similar and repeat datacalls use already leveraged data for completion.

- ✓ **Holistic Dashboards.** With unified datasets, holistic dashboards that represent and summarize the totality of cybersecurity information can be created to empower risk executive's decision-making. Holistic Dashboards can be created with almost any tool available, and can scale with investment from high-level monthly reporting to automated real-time reports with drill-down capability.



Example of Dashboard Architecture

With Unified Communications, all teams within a cybersecurity program work in concert with one another, amplifying results, increasing speed of delivery, improving satisfaction of program stakeholders, and most importantly improving risk-based decisions.

PLAYING OUT OF POSITION

CISOs can be susceptible to the notion that their work is unique, and as a result require dedicated effort to tackle routine business. The PLAYING OUT OF POSITION TRAP is when CISOs decide to lead acquisitions, technology migrations and transformations, and other processes that are outside their responsibility and/or redundant with other programs within the organization.

JACK OF ALL TRADES, MASTER OF NONE

A Federal Agency's CISO Program took over functions one-by-one that were provided by other parts of the organization, including acquisitions, training, and event planning. The budget ballooned, and soon after other areas of responsibility started lagging behind. Policy updates slid from quarterly to semi-annually and eventually annually. Weakness Remediation analysis shifted from proactive to reactionary based on scorecard defects.

The acquisition services, training, and event planning functions were performed at satisfactory or below-satisfactory levels. While training experts in the domain were implementing on-demand computer-based training and leveraging tools for virtual classrooms, there was no budget to explore those options within the CISO's Program.

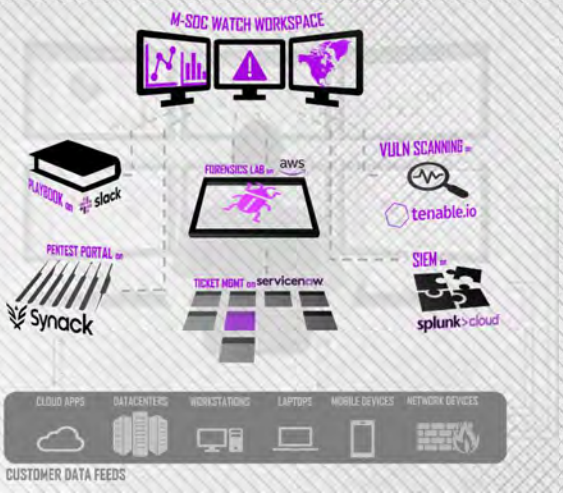
THERE IS NO "I" IN "TEAM"

Through multiple strategy and planning sessions, the CISO understood the need to get out of the training and event planning business, as well as to work more closely with the acquisition department rather than do their work for them. Resources and funding were shifted from employing staff to plan events and conferences, and to serve as training instructors. Managed service providers were tapped for event planning and training, which led to more "full service" delivery – where on-demand training was created that ultimately reduced budget and increased trainee satisfaction, and the preceding conferences were better organized with more professional amenities used.

STRATEGIC PARTNERSHIPS

The Truth is that CISOs can't do everything well and must rely on **STRATEGIC PARTNERSHIPS** to ensure mission success. Partnering internally and externally with experts in the fields of acquisition, training, application development, and even managed security services frees up CISOs to focus on setting organizational direction, making risk-based decisions, and overseeing all aspects of cybersecurity integration within the organization.

Strategic Partnerships with Managed Service Providers include a wide berth of services. Key functions every CISO should evaluate and potentially leverage include: Managed Security Operations, Cybersecurity Awareness Training and Testing, and Security Assessment Services.



Second Renaissance Managed SOC Architecture

- ✓ Managed Security Operations is increasingly the most sought-after managed service partnership for cybersecurity programs. The cost of operating 24/7/365 coverage can be steep. For smaller organizations, the cost to run their own SOC is not realistic. Managed Security Operations allows for 24/7/365 coverage regardless of organizations size, as well as distributing the cost for IT and software licensing evenly across fixed monthly rates.
- ✓ Cybersecurity Awareness Training and Testing functions can be largely outsourced, with 80% of training and testing provided with out-of-the-box solutions. The 20% for organization-specific policy and tailored role-based training can be addressed with typical in-house or external training and management services; filling gaps left by the out-of-the-box solution. This model yields better results for upwards of 50% of the cost.
- ✓ Security Assessment Services are best accomplished through managed service providers when the scope, frequency, and technical expertise has high variability. Security Assessment Service providers pull in the necessary skillsets from across their teams; eliminating the challenge of finding resources that are experts in everything, and instead leverage multiple SMEs.

Second Renaissance Security Assessment Services Toolkit

By leveraging strategic partnerships, the CISO avoids directly dealing with some of the greatest risks to program success, including managing 24/7 coverage, hiring personnel for new and emerging capabilities, and developing and managing tools such as those used for training and phishing testing.

CULTURE OF "NO"

The **CULTURE OF "NO" TRAP** is possibly the most pervasive and damaging trap to the program's long-term success. CISOs and CIOs alike can contribute to an organization-wide perception that security is an inhibitor to the mission. When cyber warriors aren't engaged in finding solutions to mission problems, they are seen as an enforcer of rules and inhibitor to mission success. CIOs have misused cybersecurity requirements as means of pushing enterprise-level control over program IT, as well as intentionally slowing the pace of progress to suit their perspective over the perspective of the program. CISOs that see themselves as gatekeepers can fall into patterns of saying "NO" and withholding permission to move forward, without working collaboratively with their program partners to find acceptable solutions.

ALL STICK, NO CARROT

A Federal Agency CISO routinely inserted herself into system boundary conversations, and often dictated what the boundaries would be to program owners. CISO staff review and approval were written into the enterprise Change Control Board, and would force system development to backtrack hundreds of man-hours' worth of work without discussion or collaboration.

The balance of planned and emergency change requests shifted from 90% planned to 65% emergency. Program personnel abused emergency change request procedures to avoid CISO review and approval. The CISO program took over responsibility for IT Security personnel (ISSO, assessors, security engineers), but the program owners refused to participate. Security documentation created did not accurately reflect what was happening with the systems.

ORGANIZATIONAL TRANSFORMATION TAKES TIME

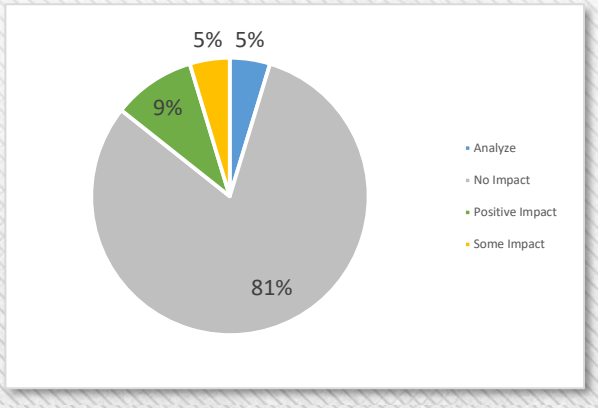
While cybersecurity resources were centralized within the CISO program, we adopted a core principle of Delivery Integration with the programs. For this case study, we started with tackling the change control problem and backed into a holistic change in approach to interacting with program customers. We worked with IT Ops and Enterprise Architecture to re-write the organization's SDLC to include cybersecurity earlier in the process. We embedded cybersecurity professionals within each program team so that we could participate in daily scrums and other program meetings, reducing the Program's need for duplicative communications and expediting the CISO team's responsiveness. Over the next 18 months, program customer satisfaction greatly increased, as did FISMA scores.

DELIVERY INTEGRATION

A mission-enabling cybersecurity organization focuses on **DELIVERY INTEGRATION** – including cybersecurity early in strategic planning, and continually through system development and operations. In current terms, this means cybersecurity inclusion in Scrums, cybersecurity requirements in backlogs, vulnerability scans within the CI Pipeline, and full DevSecOps integration. While delivery integration touches every aspect of a cybersecurity program, two building blocks have the greatest return on investment: Embedded ISSOs, and DevSecOps Integration (SDLC Integration).

- ✓ Embedded ISSOs. The Embedded ISSO model is a centralized delivery model for ISSO services, where the CISO Program controls quality of delivery through training, templates, and quality review. The centrally-controlled ISSOs are embedded within the supported programs which enables participation in daily standups and other key Agile touchpoints. Embedded ISSOs have a greater knowledge and understanding of the underlying mission, which aids problem-solving ability when helping to craft Risk Acceptance Memos, POA&Ms, and other risk-based artifacts.
- ✓ DevSecOps Integration. Building in active participation throughout the SDLC is important to ensuring early collaboration between program teams and CISO teams. As organizations shift towards DevOps models for application delivery, CISOs should partner to include cybersecurity requirements into the CI pipeline. DevSecOps Integration includes vulnerability scanning and review, as well as integrating cybersecurity requirements into the CI pipeline toolchain. From working input validation into build requirements to configuring hardened baselines, cybersecurity requirements can be implemented in CI tools early in the process, rather than adjusted after the fact (built in vs bolted on).

This customer service mindset pervades every aspect of cybersecurity delivery and builds lasting partnerships with the customer – enabling secure, resilient mission delivery.



DevSecOps Intersection with NIST Controls (Assessment performed by Second Renaissance)

WASTED EFFORT

The WASTED EFFORT TRAP can take many forms, but always drains resources from more impactful work. Examples include controls applied to individual systems when enterprise solutions would be more efficient, creating documentation that is not often used or reviewed, and performing manual operations when automation is possible. The largest pockets of wasted effort in Federal CISO Programs are often found within and around the Security Assessment and Authorization process – where NIST guidance has been interpreted as requirement and enforced to minutia by assessors and auditors alike.

WE DON'T NEED TO READ THE MANUAL

A Federal CISO Program relied on strict interpretation of NIST control guidance, rather than applying the concepts of risk management and the RMF. Every control was to be documented uniquely for every system. Every control was tested for every system. This often led to wasted effort in control assessment, where system personnel were forced to show Agency-level policy to assessors over and over again. Controls with little volatility (e.g. datacenter access control procedures) were assessed repeatedly for each system within the datacenter. Each ISSO was left to document control implementations that are outside the scope of their responsibility, which led to poorly documented and inconsistent control implementation language. The average time to ATO a system was upwards of 9 months. Slow progress to ATO led to low levels of engagement from Program teams, which resulted in security documentation that was disjointed from the Program teams' methods for operating the systems.

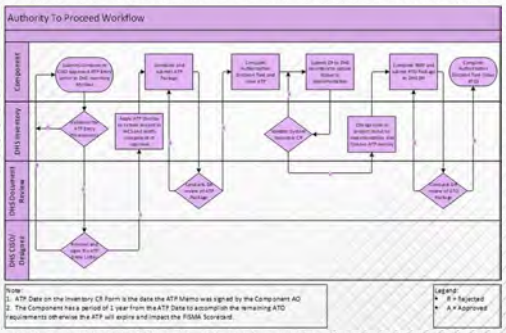
NEXTGEN RISK MANAGEMENT

Recognizing the ATO process was filled with wasted effort, the CISO Program embarked on a three-phase project to improve the value of ATOs. First, a common control program was created, where controls were centralized when possible and documented once for reuse by many systems. The GRC tool was modified to accommodate complex levels of control inheritance. This step reduced control documentation and assessment efforts by upwards of 30%. An Ongoing Authorization program was conceived to maximize the use of regular testing and assessment and eliminate the need for new ATO packages for operational systems every 3 years. Finally, the CISO program created an "Authorization To Proceed (ATP)" Program which is designed to work with today's rapid development and delivery models – providing an Authorization to operate the system while it evolves over time.

APPLIED RISK MANAGEMENT

The truth is that Risk Management done to be compliant ultimately results in wasted effort, while **APPLIED RISK MANAGEMENT** continually delivers positive outcomes due to proactive management, regular tailoring, and continuous process improvement. Applied risk management includes four key aspects: common controls, ongoing authorization, enterprise platforms, and the ATP model.

- ✓ **Common Controls.** Control inheritance is vital in a NIST-based environment where everything from personnel security to encryption methods are measured and documented. We operate in large, complex organization that compartmentalize and share responsibility for the overall mission. Our risk management process must address the shared nature by embracing common controls and Customer Responsibility Matrices (CRM).
- ✓ **Ongoing Authorization.** Breaking away from the 3-year ATO model, Ongoing Authorization programs leverage continuous monitoring determined by mission, system, and control volatility. Frequent Risk Management Board meetings provide Authorizing Officials with the information needed to continually approve system operations, and take corrective action when necessary. Ongoing Authorization programs do not reduce the level of effort spent, but rather reallocate the wasted effort to testing and monitoring with greater return on investment.
- ✓ **Enterprise Platform.** Enterprise cloud platforms with CI pipelines can serve as a form of super common control. Maintenance, incident response, developer and supply chain, media handling, contingency planning, and other policies and procedures can be standardized on the enterprise platform. This greatly reduces the footprint of responsible controls for an individual mission application. With a small set of responsible controls, time taken to document and assess implemented security is greatly reduced.
- ✓ **ATP Model.** The Authorization To Proceed Model pulls the benefits from Common Controls, Ongoing Authorization, and Enterprise Platforms forward into a next-generation ATO model that accounts for rapid product delivery in an Agile organization. Minimally viable security requirements are put in place and tied to the minimally viable product release. Iterative security, integrated with the system's Agile development, allows for improvements over time as the system matures.



Example of DHS ATP Process Flow

By applying true risk management rather than applying security controls in a Compliance-driven manner, CISO Programs unlock greater levels of efficiency and reduce wasted effort. In a budget-constrained environment where the need for cybersecurity is increasing, CISOs cannot afford to waste resources.

about
Second Renaissance

Second Renaissance Incorporated (2RenInc) was founded in 2012 to bring a unique style of cybersecurity and IT consulting to the Federal, State, and Local governments of the United States. We believe that art and science are connected, and that bringing well-rounded expertise to the table unlocks greater levels of value for our customers. Data without a message is just a bunch of numbers. Information without a story can be confusing. Words without visualization can tell an incomplete story. Second Renaissance empowers clients to communicate actionable information to leadership, align action to strategy, and build a high-performing results-oriented culture.

We deliver creative data-driven solutions including cybersecurity program management, governance, risk management framework (RMF) support, Project Management Office (PMO) support, DevSecOps advisory services, cloud security expertise, network security and Zero-Trust Security engineering services, and Data Analytics support to a wide range of mission-critical customers.

- Security Assessment Services
- Managed Security Operations
- Cybersecurity Program Strategy
- Cybersecurity Training and Testing
- Management / PMO Support

Our Purpose

Make Work Visible
Visualize and track performance

Build Something New
Challenge yourself to be creative

Make a Difference
Impact those around you

Enjoy the Pursuit
Have fun along the way

Our Experience

Second Renaissance executives bring 20 years of cybersecurity and IT Management experience spanning multiple federal civilian and defense agencies.

- ✓ Department of Homeland Security (DHS)
- ✓ Department of Justice (DOJ)
- ✓ Department of Energy (DOE)
- ✓ Federal Risk and Authorization Management Program (FedRAMP)

Second Renaissance