

Control Focused Cybersecurity

The logo features the word "TALAS" in a large, bold, black sans-serif font. Below it, the word "SECURITY" is written in a smaller, orange sans-serif font, with each letter spaced out. The text is centered over a shield-shaped background composed of multiple overlapping, semi-transparent layers in shades of light gray and light orange.

TALAS
SECURITY

Simplify.
Organize.
Strengthen.
Cybersecurity.

Thank you for considering TALAS Security as your trusted cybersecurity partner, we are excited you are here.

When we decided to build TALAS, we knew we were embarking on a challenging journey. Between rampant cyber-attacks, new regulation, and demanding compliance requirements, our most critical objective emerged quickly, to bring clarity and focus to a space riddled with divided attention and complexity.

We understand our value in this space: We make cybersecurity simple.

Cybersecurity is not a singular task; it's never really done, but rather is a continuous evolution. It challenges you with perpetual risk, requiring you to adapt your defenses, demonstrate compliance and in doing so, establish a culture of constant maturity. These challenges shape the fundamental requirements for our service delivery, to build for defense, organize for compliance and accelerate cyber maturity.

As you explore our services, we invite you to reflect on your specific cybersecurity objectives and their role in your organization's long-term strategy. Consider how a simplified approach to Cybersecurity will contribute to the clarity and focus needed to bring your cybersecurity protections to the next level.

Again, thank you for taking the time to consider TALAS Security as your trusted cybersecurity partner. We are always here for you, feel free to contact us any time.

Sincerely,



Owahn Bazydlo
Co-Founder



Paul Marco
Co-Founder

Table of Contents.....	2
Use Cases.....	3
The TALAS Methodology.....	4
The TALAS Control Stack Framework.....	5
Our Approach.....	6
Logical Segments.....	7
Service Categories.....	8
Services.....	9
Program Assessment.....	10
The vCISO Service.....	11
vCISO Service Delivery Structure.....	12
Controls Assessment.....	13
Cyber Tabletop Service.....	14
Professional Service.....	15
Service Examples.....	16

(315) 561-3816



Info@talas.io



www.talas.io



TALAS-Security



155 Madison Street
Oneida NY, 13421



USE CASES

Reduce Risk. Drive **Value**.

TALAS services are always customized to our client's cybersecurity goals. But no matter what the objective, our delivery is guided by our core value propositions.



MAXIMIZE BUDGETS

Adding a structured approach to Cybersecurity offers several financial advantages. It provides opportunities to optimize your budget, maximize existing cybersecurity investments and reduce waste.

- Enabling unused product capabilities can simultaneously reduce risk and maximize your existing cybersecurity investments.
- Identifying duplicate control capabilities may provide the opportunity to consolidate controls and reduce product spend.
- A properly articulated cyber program may result in lower Cyber insurance premiums.



DEMONSTRATE COMPLIANCE

Limited resources often lead to a difficult choice between focusing on compliance requirements or building defensive capabilities. A well-structured cybersecurity program can address both objectives simultaneously.

- Simultaneously demonstrate compliance while optimizing defense capabilities.
- Be able to articulate your cybersecurity program quickly and accurately.
- Organizing cybersecurity controls will allow you to identify strength and weakness in both your defensive posture as well as your ability to meet regulatory requirements.



DRIVE ACCELERATION

Cybersecurity can be daunting, leaving most organizations unsure of where to start. Our services are specifically crafted to accelerate your cybersecurity objectives by simplifying cybersecurity controls, organizing capabilities, and strengthening your overall security posture.

- Identify and prioritize resources allocation through control and framework alignments.
- Establish and maintain full inventories of cyber controls across your organization.
- Quickly formalize your cybersecurity program and align it with your organizational strategy.

METHODOLOGY

Cybersecurity Works Best When It's Organized Well.

TALAS Security is built to Simplify, Organize, and Strengthen Cybersecurity. Our methodology is how we can quickly and effectively organize your cybersecurity protections, drive clarity, and build program strength.



SIMPLIFY.

Simplification starts with information gathering. To minimize disruption, we use multiple tactics to collect the information necessary to identify where your cybersecurity controls exist, how they are organized and what protections they provide. This allows us to distil the components of your cybersecurity into their simplest form: Controls.



ORGANIZE.

Organizing cybersecurity elements into basic control elements makes our process easy to understand. By matching each control with its place in the TALAS control stack and categorizing them into our six logical network segments, we can assess capability strength, identify weaknesses, and optimize the structure of your cybersecurity program. This method helps meet two goals: demonstrating compliance and building defense.



STRENGTHEN.

Simplifying and organizing your cybersecurity controls provides a straightforward method for pinpointing gaps. Our structured approach enables a thorough evaluation of risk exposure to prioritize risk remediation strategies. This helps you determine where to deploy limited resources to drive the most significant impacts.








FRAMEWORK

Cybersecurity is about Control.

Approaching Cybersecurity through the lens of control is how TALAS simplifies, organizes, and strengthens cybersecurity. Leveraging the TALAS Control Stack Framework brings clarity to your Cybersecurity protections.



The TALAS Control Stack

-  DIRECTIVE
Directives represent the various drivers of a cybersecurity program. These can be frameworks, regulations, internal strategy, or other requirements that an organization must address.
-  POLICIES
Policies establish an operational commitment. They define how you will operate and identify where and when exceptions to those commitments are and are not acceptable.
-  STANDARD
Standards implement the approved operating state for an organization. They are used to operationalize policy and translate external mandates into internal requirements.
-  TECHNOLOGY
Technology controls enable capabilities that allow you to control the use of our technology resources and the actions on your network.
-  PROCESS
Process defines the steps taken to generate an outcome. They outline how a desired result is achieved.
-  PEOPLE
People own, implement, and execute controls and will remain accountable to a control, its performance, health, and output.
-  SERVICE
Services organize connected control elements and define how they are engaged, maintained, and measured when providing a benefit to an organization.

APPROACH

Cybersecurity is not simple,
that's why our **approach** had to
be.

Our approach to Cybersecurity is embodied in our mission and methodology, to Simplify, Organize, and Strengthen Cybersecurity.



ANALYSIS. Learn your organization.

We start each engagement with our information gathering phase. This is where we can learn the uniqueness of our clients' existing Cybersecurity control posture.



ORGANIZATION. Structure and enrich data for clarity.

The program organization phase is where we structure the information gathered in a way that provides clarity and focus.



REPORTING. Provide high value, actionable output.

This is how we record and deliver findings and provide written guidance through inventories, visualizations, roadmaps, and roadmaps aligned with supporting our client's goals.



GOVERNANCE. Accelerate progress and maintain momentum.

We provide regular oversight and guidance as a part of each engagement. Providing governance allows TALAS to remain connected to our client's progress and enables them to maintain their momentum as threats, priorities, and the regulatory landscape shifts.

LOGICAL SEGMENTS

CONTROL Architecture Makes a Difference.

A well-designed control architecture is the first step to managing your attack surface. Layered defenses not only detect and mitigate risks but also enables a proactive approach to cybersecurity resilience.



CLOUD



NETWORK



EMAIL



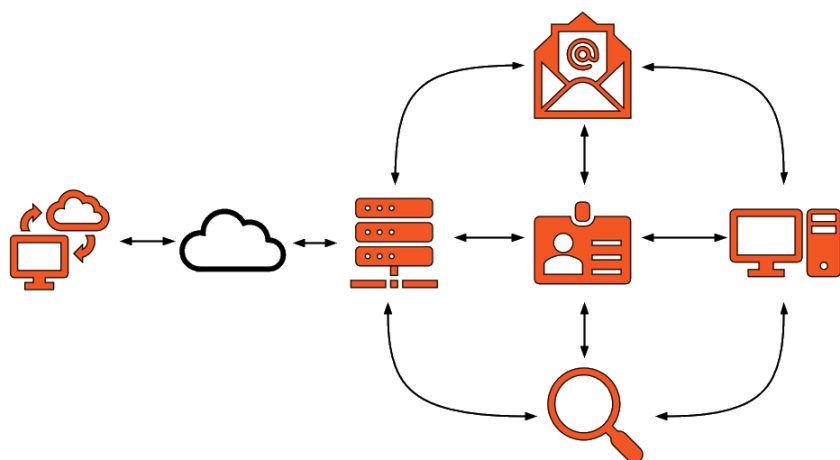
ANALYTICS



ACCESS



ENDPOINT



Logical Segmentation.

TALAS utilizes a proprietary framework to organize the placement of cybersecurity technology controls. We call this our Logical Segments Framework. These segments break a network up into 6 individual parts and allow us to align your existing Cybersecurity controls accordingly. This process allows you to understand how your controls are distributed across on your network.

Defense in Depth.

When evaluating Cybersecurity control architecture, a key design element to incorporate is Defense-in-Depth. This is the concept of positioning your cybersecurity controls in a way where they strategically provide layered protections across your network so that no control is positioned as a single point of failure.

Logical Segments Enable:

- An understanding of your layered defenses.
- A visual representation of your control ecosystem.
- A method to establish architectural clarity.

SERVICE CATEGORIES

Let us Meet You
Where You Are.

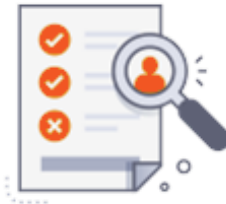
Cybersecurity goals are as unique as our clients. Our services have been designed to align with your objectives.



FULL CYBER PROGRAM MANAGEMENT

Organize your cybersecurity controls with our vCISO service, a solution designed to establish, maintain, and manage your formal cyber program. This service will build defenses, organize compliance, and accelerate your cyber maturity. With TALAS as your trusted partner, you get time back to focus on your core mission while we provide clarity into your cyber protections.

- Full Cyber Program Management
- Controls Management
- Risk Management
- Strategy Development



CYBERSECURITY ASSESSMENTS

Level-up your cybersecurity maturity with our assessment services. Knowing where you are allows you to build strategies to optimize controls and enhance both defense and compliance. Our customized approach ensures precise and proactive protection in the face of evolving cyber threats.

- Cyber Program Review
- Control Maturity Assessment
- Cyber Framework Assessment
- Cyber Tabletop Services



PROFESSIONAL SERVICES

Address your organization's specific Cybersecurity needs by engaging our Professional Services. This customizable service will allow us to tailor solutions to your unique cybersecurity concerns. Our industry experience will allow us to translate your organization's requirements, into custom solutions that accelerate your goals.

- Policy Development & Refresh
- Standards Review and Alignment
- Cyber Strategy Development
- Cyber Program Uplift
- Regulatory Review
- Incident Response Plan Refresh



SERVICES

PROGRAM ASSESSMENT

Cyber Programs Drive Clarity.

Threat actors, regulations, and other mandates pull attention in multiple directions making it difficult to know where to start. This can cause organizations to treat cybersecurity as individual problems to solve rather than taking a holistic approach to building a Cybersecurity program and securing their network.






TALAS Blueprint is our program focused assessment service. It provides the guidance, analysis and tools needed to establish the foundation of an organization's Cybersecurity program. Looking at your program holistically is the first step in enabling cybersecurity advantage using the TALAS methodologies.

OUR APPROACH

4-6 Week Estimated Service Delivery

- Organizational Structure: Identify stakeholders in an organization that manage or are **accountable** for Cybersecurity duties, technology, and incident response.
- Control Coverage: Identify and document **existing** Cybersecurity controls.
- Program Assessment: Establish a **baseline score** against our program pillars covering **130+** different points of assessment.
- Playbooks: Provide customizable cybersecurity event **playbooks** and an **Incident Response Plan**.
- Control Ecosystem: TALAS visualizes your Cyber Control Ecosystem and organizes them into **6 logical network segments**.
- Full Reporting & Directives: Receive a full report and associated directives outlining the **current state** of your program, and the roadmap to building program maturity over time.
- Quarterly Touchpoints: Connect with us **4 times** over the year to obtain guidance and to discuss concerns, strategies, and other Cybersecurity topics.

BLUEPRINT OUTCOMES

-  Increase knowledge of Cybersecurity.
-  Program baseline for driving maturity.
-  Established Cybersecurity program.
-  Visualization of technology controls.
-  Ability to strategically manage organization's Cyber risk.
-  Reusable Cyber Playbooks.
-  Reusable Incident Response Plan.
-  Quarterly Service Touchpoints

TALAS Blueprint provides organizations with a guided experience enabling them to establish the foundational elements of a Cybersecurity program. This provides an organization the direction to position themselves to better meet regulatory requirements and disrupt threat adversaries and initiate a Cybersecurity strategy.

Let TALAS Focus On Your Cybersecurity Program.

Our Virtual Chief Information Security Officer (vCISO) service provides your organization with a cybersecurity partner. This service is focused on providing cybersecurity guidance and support in a way that builds, manages, and maintains your Cybersecurity program. Giving you the time back to focus on your core mission.



TALAS vCISO service is about partnership. It's an opportunity to leverage industry expertise to accelerate your program, build defense and demonstrate compliance.

OUR APPROACH

12 Month Service Delivery

- **Analysis:** Building a Cybersecurity program starts with knowing where you are now. This phase gathers information from across your organization to **baseline your controls** and identify existing cybersecurity capabilities.
- **Design:** Every organization is different. Protecting them requires a detailed understanding of their risks, regulations, and strategic objectives. We **design a program** around the details of your organization and where you want to be.
- **Organize:** Strong Cybersecurity controls are made up of multiple components. Organizing those components allows us to understand **how they work together** to provide the maximum protections possible.
- **Mature:** Understanding the composition of your program allows you to **understand where to focus** resources to build maturity and drive capability.
- **Govern:** Cybersecurity is in a constant state of change. Keeping up with the **threat landscape** means managing a dynamic cyber program and ensuring that it is governed effectively.
- **Report:** Making effective decisions requires good data. Our reporting structure and touch point cadence ensures you have **the information you need** to properly guide your cyber program.

vCISO OUTCOMES

-  Increase knowledge of your Cybersecurity program.
-  A path to defensive and compliance maturity.
-  An established Cybersecurity program.
-  Visualization of technology controls and program structure.
-  Ability to strategically manage organization's Cyber risk.
-  A cybersecurity incident response Plan.
-  Dynamic program management and strategy.
-  A trusted partner that is engrained in organization and focused on your Cybersecurity program.

TALAS Security is built to SIMPLIFY, ORGANIZE, and STRENGTHEN Cybersecurity programs. Our methodology allows us to quickly and effectively make sense of the control elements that make up your Cybersecurity defenses.

vCISO PROGRAM DELIVERY



TALAS
SECURITY
SIMPLIFY. ORGANIZE. STRENGTHEN.

Info Gathering

Program Organization

Program Strengthening

Program Testing & Re-baseline

On-Demand Access & Advisory

Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
Program Kickoff	Program Touchpoint	Program Touchpoint	Program Touchpoint	Program Touchpoint	Program Touchpoint	Program Touchpoint	Program Touchpoint	Program Touchpoint	Program Touchpoint	Program Touchpoint	Program Touchpoint
Culture & Awareness Assessment	Cyber Program Baseline	Strategy Touchpoint	Incident Response Plan (IRP)	Establish Risk Register	Risk Register Maintenance	Risk Register Maintenance	Risk Register Maintenance	Risk Register Maintenance	Risk Register Maintenance	Risk Register Maintenance	Risk Register Maintenance
Business Process Data flows Review	Access Deep-dive	Network Deep-dive	Control Ecosystem Visualization	Build Strategy Roadmap	Annual Strategy Session	Inventory Maintenance	Inventory Maintenance	Inventory Maintenance	Inventory Maintenance	Inventory Maintenance	Inventory Maintenance
Binary Control Survey & Interview	Endpoint Deep-dive	Cloud Deep-dive	Standards Inventory	Directives Inventory	Third Party Inventory	Regulatory Alignment Maintenance	Threat scenario selection	Strategy Touchpoint	Regulatory Alignment Maintenance	Annual Tabletop Exercise	Program Re-baseline
Regulatory Analysis & Alignment	Email Deep-dive	Analytics Deep-dive	Policies Inventory	Technology Control Inventory	People Inventory	Industry Framework Alignment	Annual Tabletop planning	Scenario Development & Logistics			Tabletop Event Report
Establish Threat Profile	Program Roadmap Visualization	Establish Cyber Terminology	Regulatory Alignment Maintenance	Critical System Inventory	Process Inventory	Control Stack Alignment	Tool Rationalization				"State-of-Cyber" Report
Threat Profile Report	Culture & Awareness Report	Cyber Roles	Control Segment Report	Written Information Sec. Program (WISP)	Services Inventory	Inventory Report	Quarterly Customer Satisfaction Survey				Quarterly Customer Satisfaction Survey
Doc Review and analysis	Organization Report	Cyber Program Baseline Report	Quarterly Customer Satisfaction Survey								

Bus. Process Data Flows Report

CONTROLS ASSESSMENT

Cybersecurity is About Control.

Cybersecurity is overwhelming. Complexity, cost, and competing priorities all make securing your network difficult. We bring clarity to Cybersecurity by focusing on your existing Cybersecurity controls.



TALAS Discover is our controls focused assessment service. TALAS deploys a multi-faceted approach to gather information about, and formally document your existing cybersecurity control elements. The result is an in depth understanding of your defensive capability, technical configurations, control placement, and utilization.

OUR APPROACH

6-8 Week Estimated Service Delivery

- Existing Documentation: Collection and analysis of existing Cybersecurity information through **documentation**.
- Customized Surveys: **Information gathering** through surveys related to cyber awareness, technology controls, and **in-depth** analysis of your configurations.
- Interviews: Focused **interviews** to drive clarity, understanding, and quality of information.
- Control Efficiency Scoring: The control efficiency **scores** drive your long-term strategy for building control maturity.
- Control Ecosystem: The control **ecosystem** is organized across our **6 logical network segments**, visualizing your implementation of the defense-in-depth best practice.
- Alignment to Industry Frameworks: Identified controls are aligned against **proprietary** and **industry** Cybersecurity frameworks.
- Full Reporting & Directives: Receive a full report and associated directives outlining the **current state** of your controls, and the roadmap to building control maturity over time.
- Quarterly Touchpoints: Connect with us **4 times** over the year to obtain guidance and to discuss concerns, strategies, and other Cybersecurity topics.

DISCOVER OUTCOMES

-  Documented control efficiency scores for driving maturity.
-  Measured understanding of organizational Cybersecurity awareness.
-  Cyber controls inventoried and visualized.
-  Cyber services are inventoried.
-  Ability to strategically manage the organization's cyber risk.
-  Control alignment to Industry and proprietary frameworks.
-  Quarterly service touchpoints

TALAS Discover provides a deep understanding of an organization's Cybersecurity controls. Focusing on existing controls and capabilities enables your organization to reduce risk for little or no cost and brings clarity to your organization's Cybersecurity control ecosystem.

Play Today to Respond Tomorrow.

There are two types of organizations, those who have been breached and those who will be breached. Armed with this knowledge it is important to know that your Cybersecurity incident response plan will work when called upon.









TALAS Challenge is our incident response assessment and tabletop service. It deploys a time-tested Cybersecurity exercise that allows an organization to practice their planned response to a Cyber-attack...with a twist. Our service will produce a customized tabletop event that incorporates information about your organization's capability, culture, and communications. This information is used to build statistical models that simulate real-world outcomes based on the decisions you make.

OUR APPROACH

6-8 Week Estimated Service Delivery

- Control Discovery: Technical, process, and communication methods are **identified** through surveys and interviews.
- Attack Variables: The TALAS **Threat Selector** contains **5** threat variables to select from allowing an organization to **customize** their threat scenario.
- Statistical Models: Injects are informed by the statistics gathered during discovery mimicking **real outcomes**.
- Custom Scenario: A custom threat scenario is developed for your organization to **simulate** a real Cyber incident.
- Interactive Gameplay: Gameplay is **enabled** throughout the event using injects, statistics, and probability.
- After-Action Report: TALAS will produce an **after-action report** documenting the event, how the scenario was responded to, and the actions your organization can take to strengthen your response process.

CHALLENGE OUTCOMES

-  Respond to scenario injects replicating real world actions.
-  Custom statistics outlining the likely outcomes of your choices.
-  Ability to strategically test, practice and improve your organization's Cyber incident response plan.
-  After-action report outlining improvements you can make to your incident response process.
-  Full event management, from design to logistics to day-of event coordination.
-  Quarterly service touchpoints.

The Cybersecurity industry best practice recommends validating your incident response process at least once a year. TALAS Challenge not only meets this requirement but exceeds it. TALAS has brought realism back to the tabletop exercise by incorporating information about organizational culture, communications, technology, and process controls.

PROFESSIONAL SERVICES

Customized Cybersecurity Solutions.

Cybersecurity problems are unique, and they require unique solutions. The TALAS professional services offerings enable the flexibility required to customize solutions to meet your specific Cybersecurity goals, no matter your need.










We know that solving complex problems requires a detailed and customized approach. The TALAS Professional Services allows us the flexibility needed to tailor specific solutions for most pressing problems.

OUR APPROACH

- **Requirements:** Each professional services **engagement** starts with developing clear requirements to ensure our efforts are highly focused on your core objectives.
- **Estimation:** TALAS will translate your requirements into an accurate estimation of the **effort** required to ensure the engagement goals are met.
- **Project Reporting:** TALAS will provide regular **progress** reports, outlining advancement, open action items and areas of focus.
- **Delivery:** TALAS will close the engagement with a full review of the **deliverables** and any active handoffs that need to occur.

Professional Services OUTCOMES

-  Custom solutions tailored for your organization.
-  Updated or newly developed documentation.
-  Product & industry research.
-  Program element review, design & implementation.
-  Custom assessments.
-  Consulting engagements.
-  Strategic advisory services.

TALAS Security is built to SIMPLIFY, ORGANIZE, and STRENGTHEN Cybersecurity programs. We know that no two organizations are alike, and that each requires custom Cybersecurity solutions to drive maturity and build strength. This is where TALAS professional services allow us to deliver results based on your unique need.

Consulting & Advisory.

We structure your professional services engagements based on need. Whether they are well defined project deliverables, or strategic direction and guidance, TALAS has you covered.



CONSULTATION

Our consulting engagements deliver tangible results or outcomes that directly address your needs or objectives. Consulting engagements are focused on fully scoped objectives with clear deliverables and tangible results.

- Cyber Policy Refresh
- Standards Review and Alignment
- Regulatory Assurance Assessment
- Incident Response Plan Refresh
- Operational Process Development
- Cyber Controls Assessment



ADVISORY

Our advisory engagements focus on providing insights, expertise, and strategic direction to help you make informed decisions. The success of our advisory engagements is measured by the impact on your strategic direction, and the ability to anticipate and mitigate risks.

- Long Term Strategic Guidance
- Cyber Risk Management Maturity Review
- Security Tool Research and Selection
- Cybersecurity Strategy Development
- Cyber Program Review & Guidance

No matter your need, TALAS can produce the expertise and solutions needed to that **accelerate your goals, reduce risk, and maximize the impacts** of your Cybersecurity investments.

TALAS

S E C U R I T Y

(315) 561-3816



Info@talas.io



www.talas.io



TALAS-Security



**155 Madison Street
Oneida NY, 13421**

