SICURA carahsoft.

SICURA

Security Control Management

Building Secure by Design IT Infrastructure

Security Control Management: Building Secure by Design IT Infrastructure

Thank you for downloading this Sicura resource. Carahsoft is the distributor for Sicuracybersecurity solutions available via NASA SEWP V, ITES-SW2, NASPO, and other contract vehicles.

To learn how to take the next step toward acquiring Sicura's solutions, please check out the following resources and information:

For additional resources:
carah.io/sicuraresources

For upcoming events:
carah.io/sicuraevents

For additional Sicura solutions:
carah.io/sicurasolutions

For additional cybersecurity solutions:
carah.io/cybersecuritysolutions

To set up a meeting:
Sicura@carahsoft.com
888-662-2724

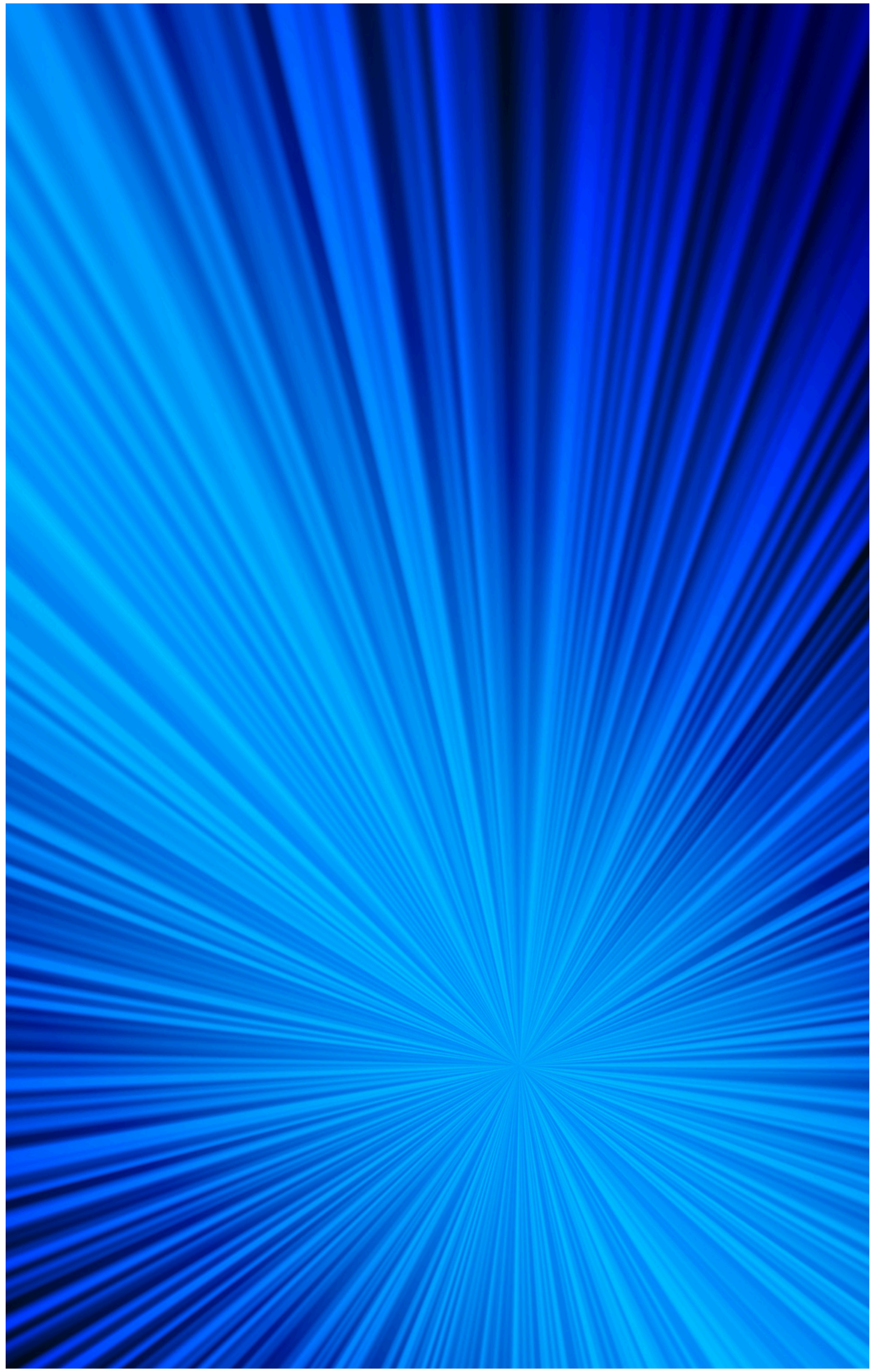
To purchase, check out the contract vehicles available for procurement:
carah.io/sicuracontracts

For more information, contact Carahsoft or our reseller partners:
Sicura@carahsoft.com | 888-662-2724

SICURA

Security Control Management

Building Secure by Design IT Infrastructure



Security and compliance can no longer be bolted-on. **Security Control Management** must be embedded into the foundation of IT infrastructure.

Across government agencies and Fortune 500 companies, IT infrastructure serves as the backbone of operations that power our economy, and our world. Yet too often, this infrastructure is compromised because we are leaving teams tasked with security and compliance at a disadvantage. Vendors provide insecure products, and often-overwhelmed teams deploy without addressing vulnerabilities. We start the race against the attackers and the auditors behind, and we never catch up.

Default settings are left intact, leading to misconfigurations. Patches are missed, leaving systems out-of-date. Security and engineering teams tasked with remediating systems are stuck in an endless loop, diverting valuable time and resources toward compliance, and away from building. At the National Security Agency, we lived this pain while obtaining Authority to Operate (ATO) for critical systems, and we've repeatedly seen the same issues across government and enterprise in the years since.

It's bad enough that ATOs and audits take 12-18 months, and cost millions of dollars. What's worse, these long compliance cycles leave the door open to real danger. In the vulnerabilities that remain unpatched or in the complex handoff between teams during remediation, attackers are waiting to pounce. In breaches of the U.S. Office of Personnel Management, Capital One, and most recently the National Nuclear Security Administration, IT infrastructure provided the entry point for attackers to access systems with some of our nation's most sensitive data.

After major attacks, we often hear the refrain that these breaches could have been prevented. Yet we fail to operationalize the recommended fixes across teams, workflows and tools. Too little changes, and another breach happens.

A new approach is needed to end this cycle. It will take bold action. From C-suites and policymakers to engineers and GRC teams, we must make a commitment to embed security and compliance across every infrastructure deployment. Fortunately, the building blocks are in place. Thanks to the prescient and timely work of the team at the U.S. Cybersecurity and Infrastructure Security Agency (CISA), we have a roadmap to make systems Secure by Design. Agile frameworks such as DevSecOps and Continuous ATO (cATO) are creating new workflows, from the DoD to the private sector. All have recognized the need to shift compliance from a series of manual, fragmented point-in-time checks to an automated, integrated, and always-on cycle.

With this convergence, we are entering the era of Security Control Management (SCM), where a new class of software provides the tools to build secure by design IT infrastructure, not just secure systems after the fact. This eBook serves as a primer on how we reached this moment, how we implement SCM today, and where we are heading next. Our ask is that you read it, share your feedback with us, and send it to others. The purpose of SCM isn't merely to inform a product or a single team. We're transforming security and compliance with a new category of proactive tools and workflows that are built by engineers, for engineers. Join us.

Sincerely,

Lisa Umberger
Co-Founder & CEO, Sicura

Kendall Moore
Co-Founder & CTO, Sicura

Table of Contents

The Landscape Today

IT infrastructure is...

Increasingly complex

An exposed and overlooked attack surface

Reliant on manual and fragmented security + compliance processes

The infrastructure layer is a dangerously overlooked attack surface.

As the industry races ahead to prevent future threats to AI, we risk leaving the IT infrastructure layer exposed today. From OPM to Capital One to the recent SharePoint breach, some of the most damaging attacks of the last decade have originated with IT infrastructure. They all exposed sensitive national security information, and personal data. In each case, attackers exploited flaws in products issued by major technology vendors to gain access to networks. The aftermath of each breach featured calls for reform, but the intervening fixes failed to prevent new attacks from happening.

Underscoring these breaches is a systemic failure: Cybersecurity vendors ship products that are vulnerable out-of-the box. Then, overwhelmed users fail to keep up with patches and remediate configuration drift. As a result, infrastructure lacks basic cyber hygiene that is necessary to keep systems compliant and prevent attacks. Breaches happen. The victims get blamed. Necessary changes aren't made. The cycle repeats.

OPM

Date: 2015
Traced to: Outdated software, failure to implement cybersecurity protocols
Target: 22.1 million personnel records, including background checks
Legal Penalties: $63 million settlement

Capital One

Date: 2019
Traced to: Misconfigured AWS storage bucket
Target: 100 million credit card applications and accounts
Legal Penalties: $270 million (Civil and Settlement)

SharePoint

Date: July 2025
Traced to: Vulnerability in on-prem Microsoft SharePoint Server
Target: 100 organizations, including US Air Force and National Nuclear Security Administration
Status: Under investigation

> "The threat landscape changes **daily**. How do we keep pace? More importantly, how do we stay ahead, and adapt?"
> -Maj. Gen. **Ryan Heritage** (ret.), former Director of Ops, US Cyber Command

SICURA

Every deployment is different.

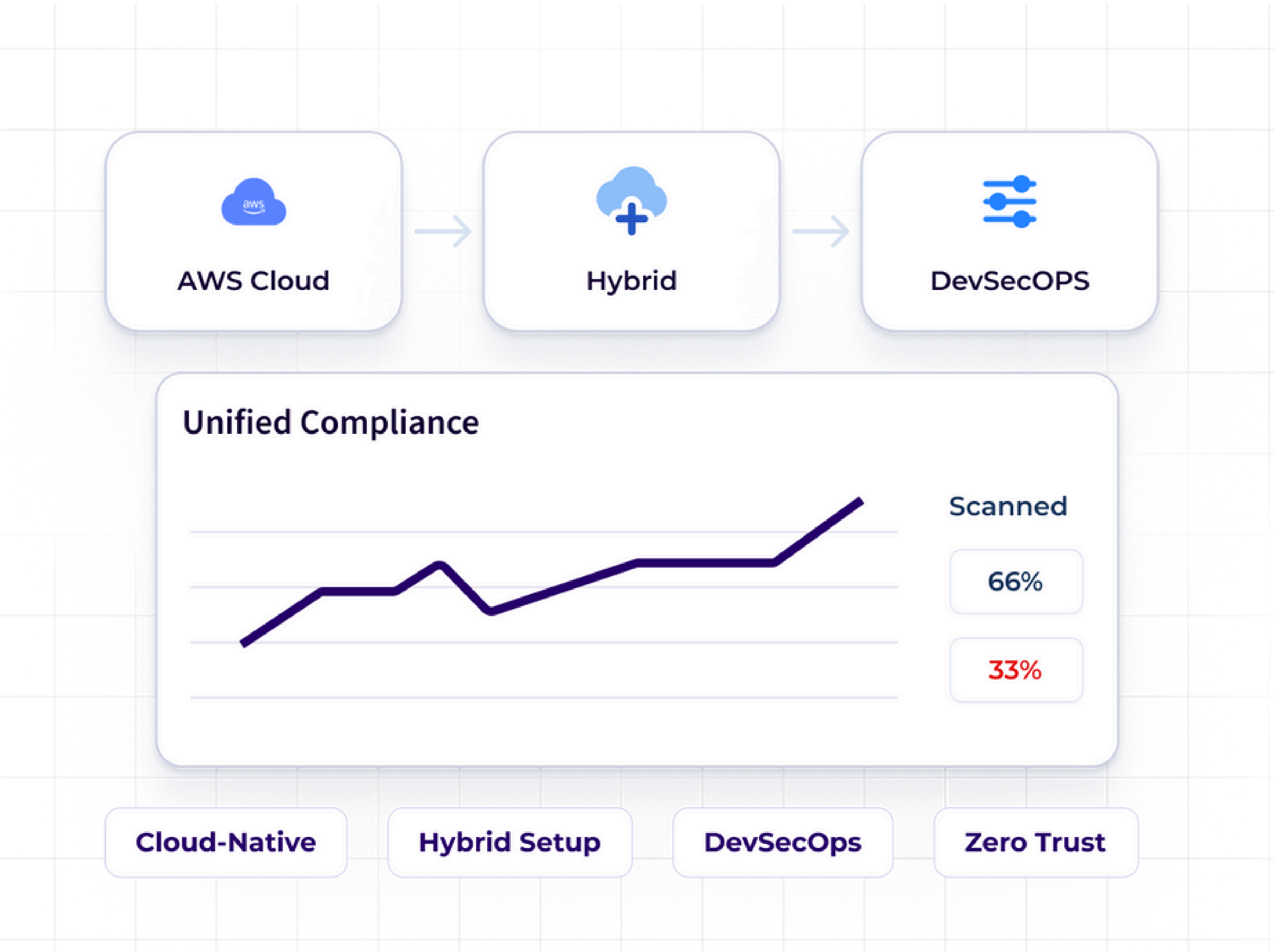
Inside government agencies and enterprises, **two realities about IT infrastructure** are true at the same time:

- Adoption of AI and cloud is rapidly increasing, transforming how large organizations work, and environments are built.
- On-prem infrastructure remains in use by many of the largest and most secure organizations in the world.

An organization does not have one infrastructure. It has **multiple infrastructures**.

Security controls must map:

- Which environment? (On-prem, cloud, hybrid, airgapped)
- Which standard? (DISA STIG, CIS, CMMC)
- Which industry?
- Which geography?



Security and compliance are the work of multiple teams, including:

- Security
- Engineering
- Governance, Risk, and Compliance (GRC)
- Legal
- Operations

The Compliance Gap

Inside most organizations, security and compliance of IT infrastructure is an afterthought by default. Vendors ship products that are insecure out-of-the-box. Organizations must confront misconfigurations from the start, leaving them lagging out of the gate. As vulnerabilities are discovered, vendors issue patches and standards bodies update regulations. But the teams tasked with deploying them are overwhelmed by the pace and volume of threats. They struggle to deploy timely patches as they navigate increasingly complex environments, and make risk calculations that accompany every update.

Compliance is supposed to provide the check on whether systems are secure, but today's processes can't keep up. Authorization and audits provide a periodic check to ensure compliance, but they are held on protracted, multiyear cycles. Security and engineering teams must devise one-time solutions from scratch, even though they don't speak the same language. And when the laborious, time-consuming compliance process is complete, they're left only with one-time fixes that represent little more than bureaucratic box-checking exercises. Systems are out-of-date by the time the next patch is issued, whether an organization is undergoing a compliance check or not.

Compliances processes are

Manual
Spreadsheets and one-time workarounds are the norm

Static
Audits are point-in-time snapshots of a moment

Fragmented
Security, engineering, GRC, legal, operations

The Back-and-Forth Between Security and Engineering

- Security and engineering are stuck in a back-and-forth
- Security scans the system, and provides results to engineering
- Engineering gets results in spreadsheets, and remediation takes heroics
- Results get passed back to security, which find more issues
- Security and engineering talk past each other
- ATOs and audits stretch into months and millions of dollars

The Status Quo Can’t Hold

Expectations are changing across...

- Technical
- Executive and Board-Level
- Policy

The New Default: Technical

By Engineers, for Engineers

Agile software, cloud and AI have shifted how technical teams work. Version control, reusable code libraries, and automated workflows transformed software development. Today, infrastructure, security, and GRC teams have an expectation to be working with machine readable engineering artifacts that present work “as code.”

These artifacts can be integrated with automated frameworks such as:

- DevSecOps
- CI/CD
- Infrastructure as Code (IaC)
- GRC tools

Reusable control sets, not starting over every time

Processes that are automated by default

Workflows that cross security, engineering, and GRC

Security and compliance is part of development pipelines

The New Expectation:

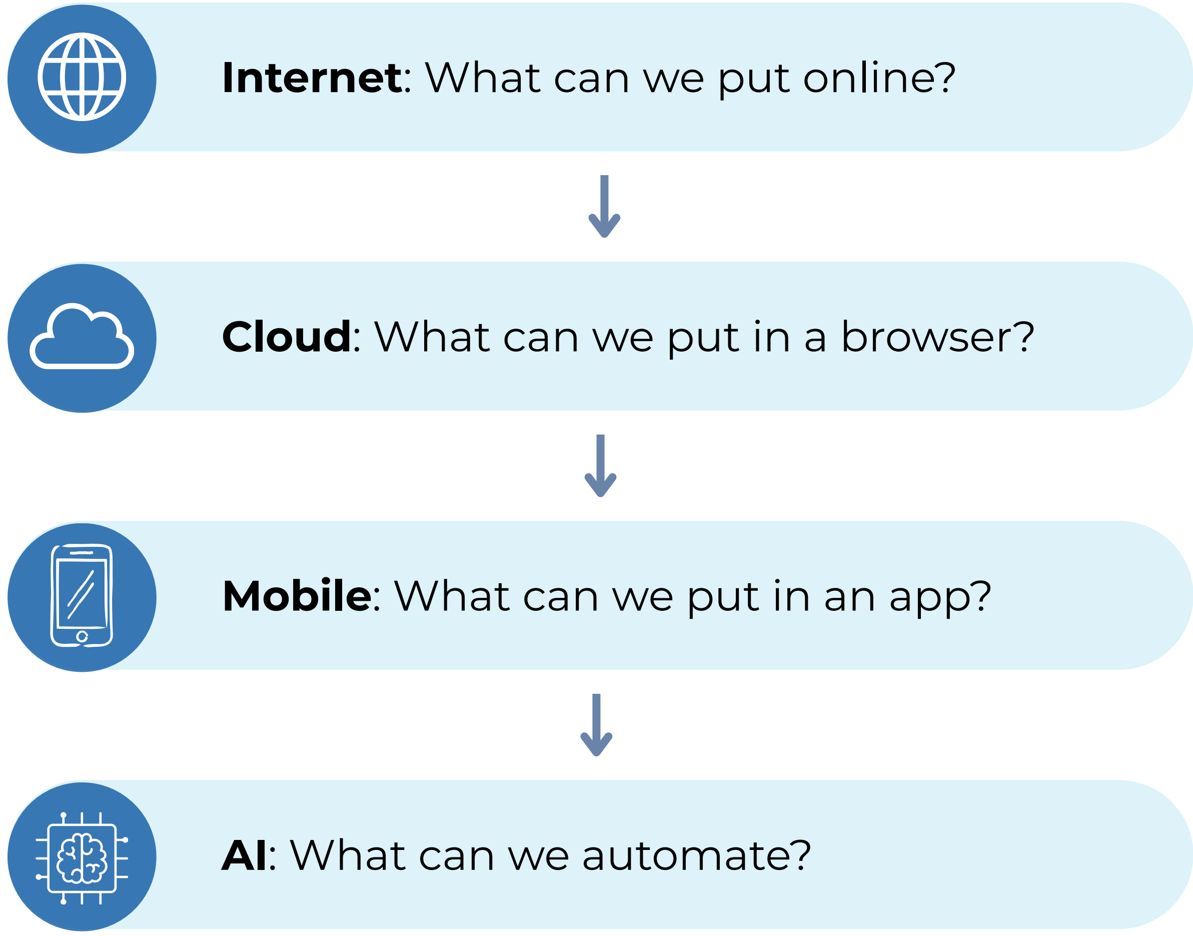
Build secure infrastructure, across the full lifecycle

NOT deploy, then remediate insecure infrastructure later

Continuous Compliance

The risk landscape is rapidly changing. The accelerated digital transformation of the pandemic and rapid emergence of AI put powerful new tools in the hands of workers and customers. We are on the cusp of a generational shift.

We went from…



Internet: What can we put online?

Cloud: What can we put in a browser?

Mobile: What can we put in an app?

AI: What can we automate?

The implications for compliance are immense. Leaders don't want to direct resources to audits and authorization exercises that require:

- Diverting valuable engineering labor away from building and solving
- Operational downtime
- Box-checking that doesn't provide real security

They will expect **continuous** processes that are:

- **Always-on,** to avoid downtime and the risk of coordinating between teams
- **Properly balanced workloads** between humans and machines
- **Responsive,** to improve at the pace of technology, threats, and standards

The New Expectation:

Continuous and automated compliance

NOT manual audits and every-three-year ATOs

Secure by Design

The cybersecurity community is at an inflection point. We continue to face a barrage of attacks and technology is racing ahead. Yet, security and compliance is still an afterthought inside many organizations.

Over the last decade, security experienced the following shifts:

- **Zero Trust:** From perimeter-based to data-based
- **Risk Management Framework:** From one-size to flexible
- **Shift Left:** Security integrated early in the build lifecycle

A decade after many of these ideas were first introduced, **Secure by Design** aims to weave security through every operation and action, flexible to the needs of an environment and, embedded throughout the development lifecycle.

> “We must build a world where technology is built **secure by design**, not bolted on afterwards.”
>
> -**Marene Allison**,
> former CISO, Johnson & Johnson

Inside DoD, the standards are changing.

Responding to an ATO process that consumed months of time, and only occurred every three years, teams began experimenting with Continuous ATO (cATO).

For years, teams of innovators banded together to invent solutions. Now, leaders at the top are declaring that continuous compliance will be the law.

This gave way to the Cybersecurity Risk Management Construct (CSRMC) and Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0).

The Moment for Change is Now

Security Control Management

Security Control Management (SCM) provides continuous hardening, across every infrastructure deployment.

The 5 Principles of Security Control Management

Tailored policies that customize security controls for any standard and organizational need

Automated processes, including enforcement, remediation, and validation

Continuous security and compliance, shifting from point-in-time checks to always-on cycles

Integrated workflows that deliver artifacts to enable engineering, security, compliance, and operations teams to build together and share responsibility

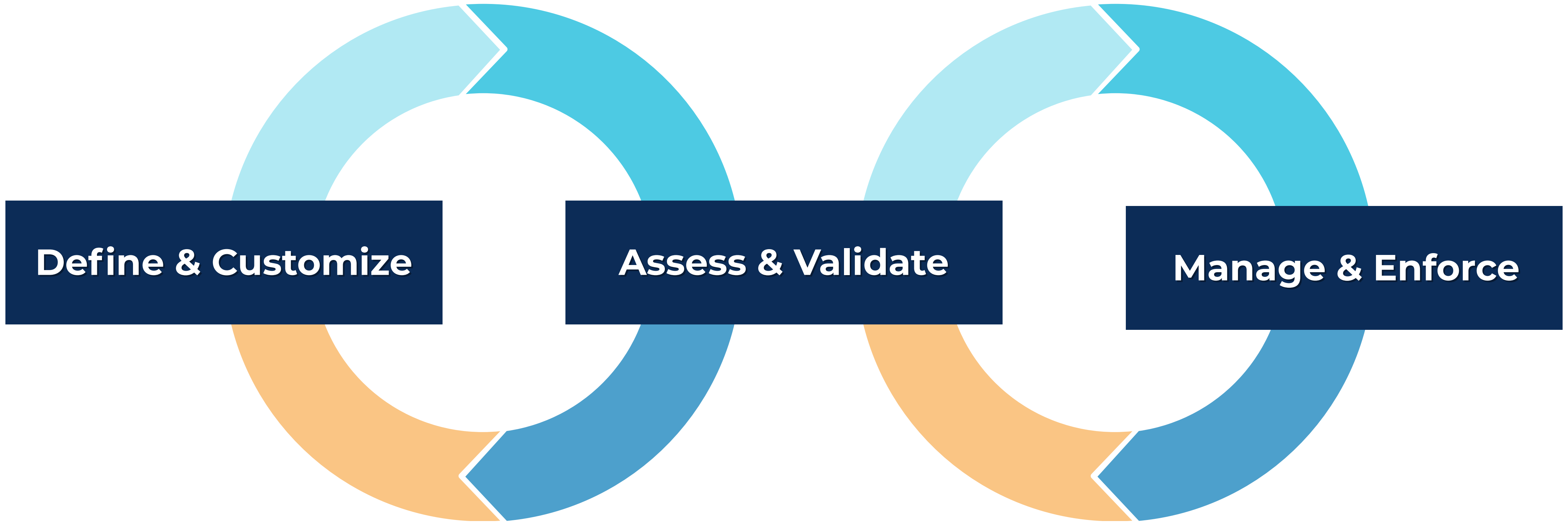
Flexible deployment, including on-prem, cloud, hybrid, or airgapped environments, and agent-based or agentless configurations

The Cycle of Security Control Management

Policy-First
Define a security control policy that is customized to your environment and requirements, then build infrastructure from that policy.

Continuous Monitoring
Assess and validate infrastructure against the policy to detect configuration drift in real time.

Automated Remediation
Take immediate corrective action to manage and enforce policies, so that systems are protected against attackers, and compliant with standards.



What's Next

Momentum is growing.

We're asking you to **join us**. There's room for technologists, executives, policymakers, and more. We all need to work together.

→ **Let's stop solving bureaucratic problems and get back to doing real work.**

Lisa Umberger
CEO & Co-Founder
Sicura

Kendall Moore
CTO & Co-Founder
Sicura

Peter Stephens
COO
Sicura

Marene Allison
Former CISO
Johnson & Johnson

SCM Featured In:

INFOSEC WORLD

DARK READING

Forbes

GOVFORWARD®

SICURA

Let’s Build Secure by Design Infrastructure. Together.

Contact

Peter Stephens, COO, peter@sicura.us

Learn more: sicura.us