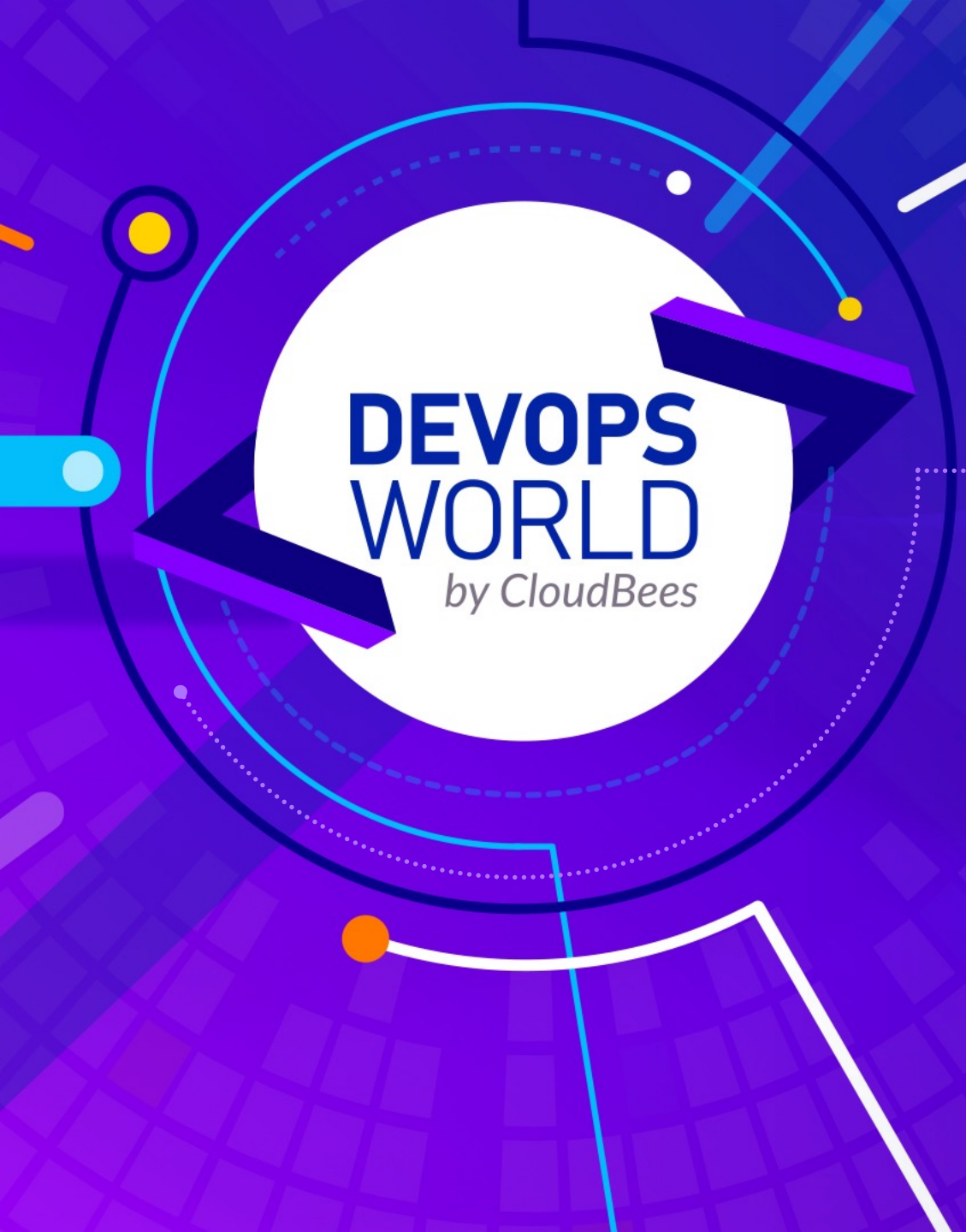


LEADERSHIP

Shift Left:

Can automation fix the InfoSec and Risk Management bottleneck?

Alexander Stein

APPLICATION SECURITY ENGINEER, FLEXION

What is the agenda for today?

Is shifting left for government projects, where security outcomes are prioritized by adaptive risk management and facilitated through new automation, a simple technical problem? Nope!

- Big Picture
  - Why are we here and why do we care?
  - What holds us back from making this easy?
  - Are we honest enough about the present and future of our security posture?
  - Why care and how do we fix it? What changed to make this more urgent?
- What assumptions are holding us back? Why is this not a simple technical lift?
  - Quite a few! More after the commercial break.

Who am I listening to?

- I work on digital service delivery at Flexion.
- I work with federal agency customers, and in my past military customers.
- In those projects, my role is:
  - Application Security Engineer
  - Cloud Engineer
  - DevSecOps Engineer
  - Security Architect
  - “Risk Management” ~~Compliance~~ “Engineer”
- I now work on an OSCAL adoption project (professionally and recreationally)

Why am I taking your advice?

- Disclaimer: these are my opinions.
- Experiences and anecdotes are not about one agency, one project, one situation.
  - Repeat themes, because the challenges are frequent and common
  - No calling out bad apples
  - No need to change names protect the innocent

LEADERSHIP

The Big Picture

Why are we here?

DEVOPSWORLD by CloudBees

Why Are We Here?

- Shifting left implies:
  - Knowing your priorities, understanding them, and where they are
  - Moving certain priorities ahead of others
- The US government and US military have big goals, impacts, and budgets.
  - Can they shift left in a holistic way?
    - If not, can any large organization?
  - They **want** to be perceived as **the most secure**.
    - So … are they?

Why Are We Here?

- But in reality, we have …
  - CISA ED 21-01 Mitigate SolarWinds Orion Code Compromise
  - CISA ED 21-02 Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
  - CISA ED 21-03 Mitigate Pulse Connect Secure Product Vulnerabilities

Why Are We Here?

Eric Mill
@konklone

Replying to @konklone

2/ Agencies and FedRAMP review vendor-supplied documentation, scan results from generic tools, and attestations to various "best practices".

It's done using a maximalist, mindless checklist that NIST (and OMB, through FISMA metrics) inflicts upon federal agencies.

3:22 PM · Dec 19, 2020

69 1 Copy link to Tweet

Eric Mill
@konklone

Replying to @konklone

4/ But it's not optimizing for actual security outcomes. This gigantic basic-error-avoidance compliance apparatus is all-consuming to the people on the ground.

None of this leaves time, money, energy, or imagination for *technical*, *qualitative* security analysis or investment.

3:22 PM · Dec 19, 2020

94 2 Copy link to Tweet

[Eric Mill, formerly GSA, now Federal CIO Advisor (after he posted)]

Why Are We Here?

- Compliance programs should have been risk-based programs (for a while now)
- Reality or perception I hear from feds and contractor colleagues:
  - Rigorous
  - Inflexible
  - Anti-agile (compared to the Agile Manifesto)
    - Process before people-friendliness
    - Comprehensive documentation before functional work product
    - Conforming to plan is more important than responding to change

Why Are We Here?

- USG and military and their Mission Essential Functions (MEFs) are important
- We want perception == reality
- Good security tactics without strategy leaves gaps

LEADERSHIP

The Big Picture

What holds us back?

What holds us back?

- Is the perception == reality gap deep and wide? Usually, yes.
- Why?
  - Capabilities are misunderstood
    - or hard to resource
    - or hard to design
    - or hard to assess objectively
    - or we perceive them as waste of time?
- Why not?
  - Status quo is easy.
  - Honesty is hard, especially about weak spots.

LEADERSHIP

The Big Picture

How honest are we?

How honest are we?

Public servants avoid risk because they are trying to avoid the shame of failure. The “public” in public service means that the fallout from what might otherwise be a “normal” failure ratchets up the sense of exposure. In government, failure can mean public scrutiny, investigations, inspections, audits, newspaper headlines, coupled with the internal personal sense that the value of the work is so crucial and that so many people are relying on us to do it well. High ideals, high stakes, a field ripe for shame events.

- Peter Kamran in “Shame, software, and government”

How honest are we?

- Based on my anecdata:
  - Most aren’t
  - Most don't want to admit it
  - Of course, exceptions to the rule exist (they are the minority)
- Do we need to change key assumptions and key invariants for **OSCALification** to work?
  - Wait, what is OSCAL?
  - Why OSCALify?
  - Do we need to?
  - Do we even want to?

LEADERSHIP

The Big Picture

Why care and how do we fix it?

Why care and how do we fix it?

- Core operational problem: form drives functions. Relevant social media research:

Why care and how do we fix it?

NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSCAL). OSCAL is a set of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results.

- NIST OSCAL Website

Why care and how do we fix it?

FedRAMP is excited to announce that the program has reached an important automation milestone. FedRAMP has worked closely with NIST and industry to develop the Open Security Controls Assessment Language (OSCAL), a standard that can be applied to the publication, implementation, and assessment of security controls.

- FedRAMP Blog December 2019: "FedRAMP Moves to Automate the Authorization Process”

Why care and how do we fix it?

- Is this only about the United States? No.
- Public sector and industry adopters worldwide.
  - Governments
    - EU (ENISA, EUCC, and the Medina Project)
    - Australia (ISM)
  - Advisory bodies and industry standards
    - ISO 27001

Why care and how do we fix it?

- If we are not honest or prepared, can we:
  - automate creation of concrete, actionable guidance?
  - document its application and use for an information system?
  - assess implementations for accuracy?
- Are we automating the well-known or this a digital transformation project?
  - More after the commercial breaks!
  - Really shifting left means:
    - From the onset of the project
    - From project leadership down
  - DevOps is not tools, it is culture!

LEADERSHIP

Of Course We’re Shifting Left! 😉

The Assumptions Holding Us Back

DEVOPSWORLD by CloudBees

LEADERSHIP

The Assumptions Holding Us Back

We Do Adaptive Risk Management, Not Old School Compliance

DEVOPSWORLD
by CloudBees

We Do Adaptive Risk Management, Not Compliance

- If “compliance” and security are different:
  - Compliant … with what!?
  - What is the relationship between the two?
    - In the USG, “compliance program” and “risk-managed program” used interchangeably
    - Risk-managed program should inform priorities of security system, the capabilities
- Is the Risk Management Framework (800-37, 800-53) meant to be adaptive? Yes!
- Are all RMF controls required and implemented blindly? Yes.
- Do empirical risk decisions inform risk management capabilities? Should they?
  - Hint: FedRAMP is publishing their opinion, and it's a yes.

We Do Adaptive Risk Management, Not Compliance

- Impact with and to OSCAL:
  - Compliance capabilities designed for the purpose, not engineered
  - CISOs and ”compliance teams” must understand engineering cultures (DevSecOps) to inform them
  - "Version control risk management and security strategies" very foreign to leadership
  - Engineering adaptive, machine-readable policy only possible for honest, very advanced orgs

LEADERSHIP

The Assumptions Holding Us Back

We Understand Compliance != Security

DEVOPSWORLD
by CloudBees

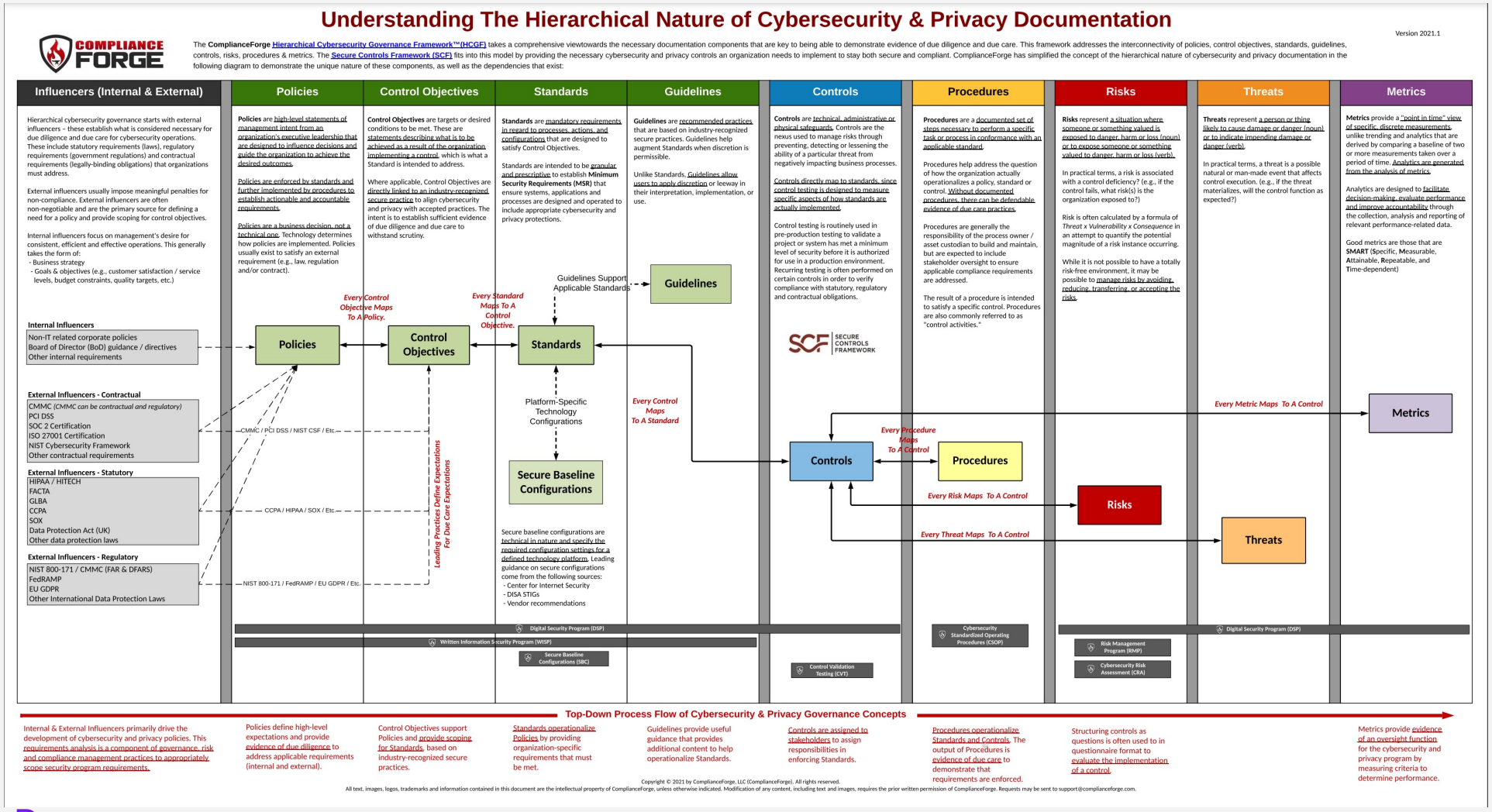
We Understand Compliance != Security

- 800-53 buzzword bingo: goals == capabilities (for compliance & security)
- Some overlap, but significant differences
  - Industry combined all of this, new name is cybersecurity

We Understand Compliance != Security

- Compliance: high-level, strategic capabilities (policies)
- Security: low-level implementation (procedures, processes, guidelines)
- Compliance and security people in USG projects:
  - Different cultures
  - Speak different languages
  - Very often disconnected from each other

We Understand Compliance != Security



We Understand Compliance != Security

- Impact with and to OSCAL:
  - security data sometimes structured
  - compliance data almost always unstructured
  - OSCAL is a government led initiative to necessarily connect them
    - Yes, let that sink in. 😊

LEADERSHIP

The Assumptions Holding Us Back

We Understand Our Technical Risk, It’s Easy to Manage

DEVOPSWORLD
by CloudBees

We Understand Our Technical Risk, It's Easy to Manage

- CISSP book learning is not applicable to real-world
- The authorizing official (AO):
  - Is often not a technical expert
  - Has neither taken tech exams nor has current applied skills
  - Is a federal employee and needs to consult with others
  - Cannot admit their confusion or formulate clarifying questions to engineers

We Understand Our Technical Risk, It's Easy to Manage

- Impact with and to OSCAL:
  - Risk managers and front-line engineers live differently
  - Neither structure data the same way, if at all
  - Difficult (sometimes impossible) to track risk changes/mitigations for complex stuff
    - World is interconnected
    - Internet is a series of tubes
    - Systems are interconnected, risks rarely isolated to one system

LEADERSHIP

The Assumptions Holding Us Back

We Really Know Everything We Deploy

DEVOPSWORLD
by CloudBees

We Really Know Everything We Deploy

- Surprise! Digital services, new or old, are not static.
- Impact with and to OSCAL:
  - FISMA/FedRAMP oversight is not adjacent to inventory mgmt (even for cloud)
  - Inventory is not static or slow to move
  - Inventory is not just servers and not 1 discrete IP address for everything
  - Interconnections and boundaries are never clear-cut (prove me wrong!)

LEADERSHIP

The Assumptions Holding Us Back

Our Auditors Know Exactly How to Assess

DEVOPSWORLD
by CloudBees

Our Auditors Know Exactly How to Assess

- Assessing docs is easy
- Building an experienced assessment org is hard
- Assessors can have opinions and biases
  - Objectivity is a privilege, not a right

Our Auditors Know Exactly How to Assess

- Impact with and to OSCAL:
  - Assessment plans will become increasingly consistent
    - Siloing expertise and not sharing standards will come with penalties
    - Comparing assessment plans and results is easier for oversight bodies
    - Quantity and quality of internal/external audits will forever increase transparency
  - Results must connect to a structured action result
  - Plan and result must refer back to a proper system security plan

LEADERSHIP

The Assumptions Holding Us Back

We Know Each Weakness, Mitigation, and Predict Breaches

DEVOPSWORLD
by CloudBees

We Know Each Weakness, Mitigation, and Predict Breaches

- Plan of Actions and Milestones (POA&Ms):
  - Risk management and security TODOs for the information system
    - Maybe also system issues for the whole engineering org (underreported or never fixed)
  - SAP => SAR => POA&Ms (rinse and repeat during an authorization cycle)
- POA&Ms should honestly cover all risks (open and mitigated)
  - Threat modeling and risk assessment actually go somewhere
  - When we are breached, we should know how and why it was possible
    - Especially when our mitigations were limited or weak
  - Achievable mitigations not done yet in PO&AMS == just-in time budgeting - @its_a_lisa
    - OMB M-02-01 implies this

We Know Each Weakness, Mitigation, and Predict Breaches

- Impact with & to OSCAL:
  - Any PO&AMs and any findings are inherently bad (I'm guilty of this)
  - POA&Ms are far removed from engineering teams
  - POA&Ms are infrequently reviewed

LEADERSHIP

Conclusion

Realism != Pessimism

DEVOPSWORLD by CloudBees

Conclusion

The takeaway is *not* jaded pessimism.

Conclusion

Can OSCAL and next generation automation *completely* solve these problems?

No.

Conclusion

Can OSCAL and next generation automation *help* you shift left?

If we're honest, yes! Come find out how.

NIST's official channels: https://pages.nist.gov/OSCAL/contribute

OSCAL Club's community projects: https://oscal.club

Thank you!

Alexander Stein

APPLICATION SECURITY ENGINEER, FLEXION

LEADERSHIP

Appendix

Additional Slides

DEVOPSWORLD by CloudBees

LEADERSHIP

The Assumptions Holding Us Back

We Use Vanilla 800-53 From NIST

We Use Vanilla 800-53 From NIST

- “We do NIST.”
- “We do RMF.”
- “We use 800-53.”
- Nuance need not apply.

We Use Vanilla 800-53 From NIST

- Impact with & to OSCAL:
  - People tailoring and scoping do not “track changes” (engineers like version control, remember?)
  - No set methodology
  - Usually done in isolation, not collaboratively with system teams
  - "Diffing" from upstream (NIST) and quickly publishing changes? Impossible!