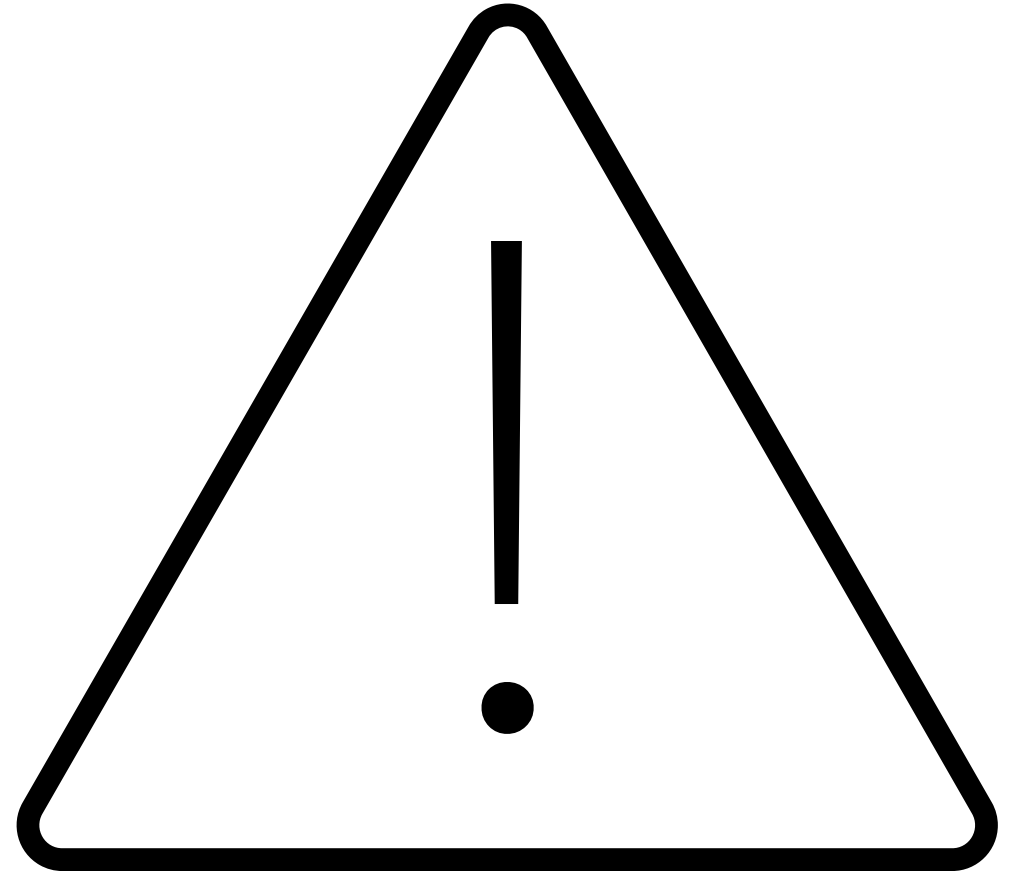

CLOUD OF DUST

HOW TO CREATE SCALABLE
AND EFFICIENT GOVERNANCE
OF CLOUD SYSTEMS



DISCLAIMER

- The opinions expressed in this presentation are my own and do not represent the views or endorsements of my employer or a business.



C:\USERS\SETHEARBY\WHOAMI

- Governance Risk and Compliance Program Manager
- Healthcare/Technology / Consulting
- CISM



WHAT?

Google Translate



Text

Images

Documents

Websites

English - Detected

English

Spanish

French



English

Spanish

Arabic



How to Create Scalable and Efficient Governance of Cloud Systems



How to not lose your shorts when managing multiple cloud environments



65 / 5,000



WHY?

6 of the 7 challenges identified with cloud security by Wiz are related to cloud security governance:

1. Securing 3rd party software and APIs
 2. Lack of visibility
 - ~~3. Cybersecurity skills shortage~~
 4. Cloud data governance
 5. Shadow IT
 6. Evolving attack surface
 7. Juggling Multi-cloud security
- <https://www.wiz.io/academy/cloud-security-challenges>





WHAT CLOUD DOES WELL

- Allows remarkably fast resource availability and implementation
- Shifts capital expenses from operational*
- Reduces maintenance burden and costs for infrastructure



WHERE CLOUD GOES WRONG

- Silos data and access controls to single systems
- “SaaS Sprawl” (shadow IT) where solutions will be created/purchased without governance
- Costs can be extreme*
- Removes IT from provisioning (which often leaves solutions unchecked)



Define	Define responsibilities
Establish	Establish standards
Enable	Enable autonomy
Promote	Promote communication
Report	Report KPIs

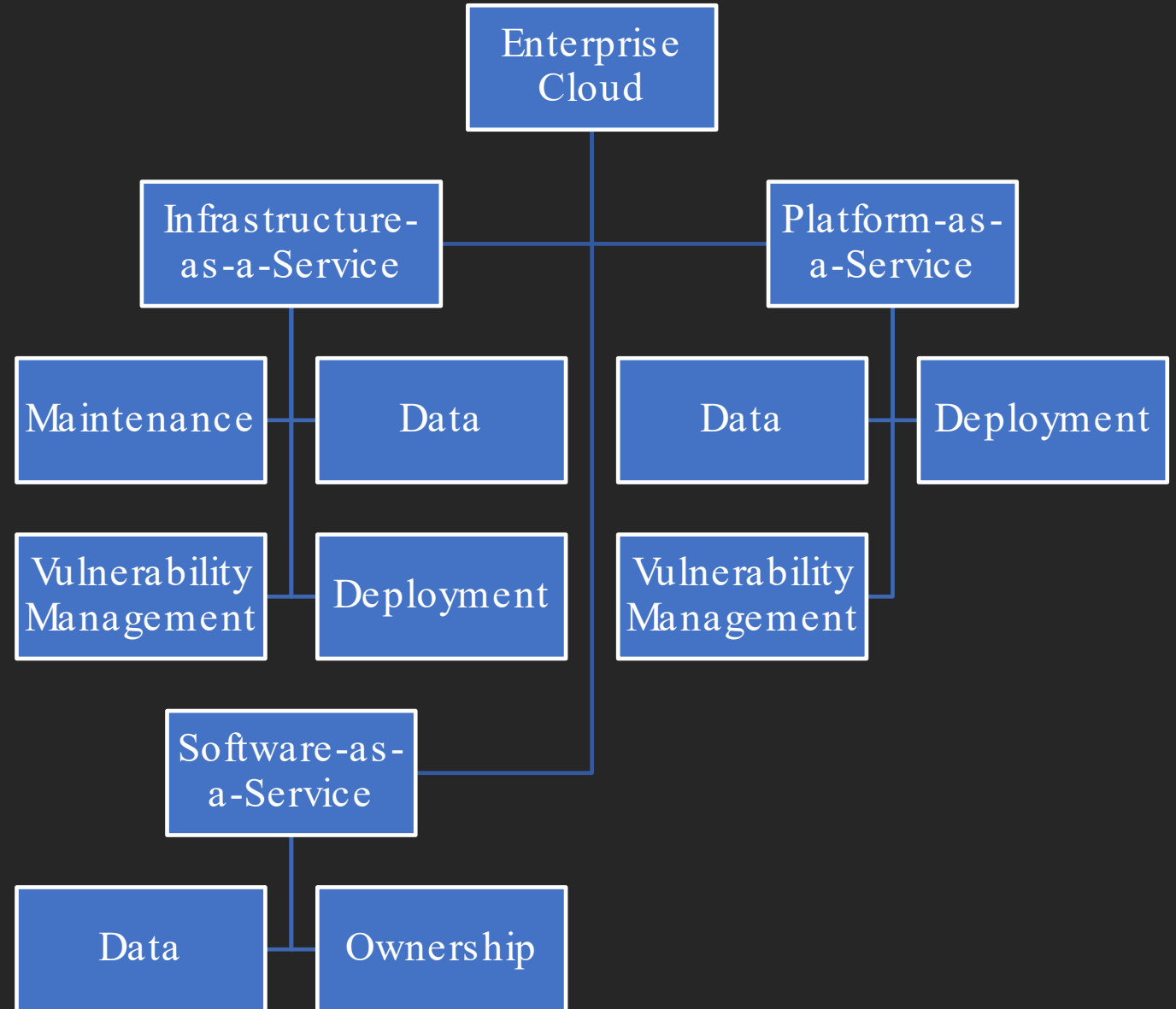
HOW?



DEFINING RESPONSIBILITIES

- Enterprise Cybersecurity organizations often integrated security functions into slow moving IT processes in the past
- Modern cloud deployment teams can use Infrastructure-as-Code (IAC) platforms like to CREATE much faster than SECURE
- Modern Enterprise cloud environments often require specialized resources to maintain, deploy, and secure the environment

CLOUD FUNCTIONAL AREAS



SAMPLE FUNCTIONAL RESPONSIBILITIES OF CLOUD SYSTEMS

IaaS	
Maintenance	IT
Vulnerability Management	Security
Data	IT/Departmental
Deployment	IT/Development
SaaS	
Ownership	Finance/Departmental/IT
Data	Departmental
PaaS	
Deployment	IT/Development
Vulnerability Management	Security
Data	IT/Departmental



DEFINE RESPONSIBILITIES - ONE BITE AT A TIME

- Creating small action teams enables agility
- Stalemates go up not sideways
- Formalize as much as necessary

DEFINING RESPONSIBILITIES - PURPOSE VS PROCESS

- The point is to set assign ownership versus tasks
- Create charters and teams with purpose
- Responsibilities should represent a flowchart versus table



ESTABLISH STANDARDS

- Engineers don't read policies
 - Technology standards can be delivered in a variety of mediums
 - Encourage automation of standards (scripting, images, Continuous Integration, Infrastructure-as-Code, etc.)
 - Great product of functional teams
-



PERFECT IS THE ENEMY OF GOOD - VOLTAIRE

- Standards are the fruit of the policy
- Encourage “standard” development outside of documentation (IaC, images, CI/CD)
- Standard deployment can be audited by non-GRC members (QA)

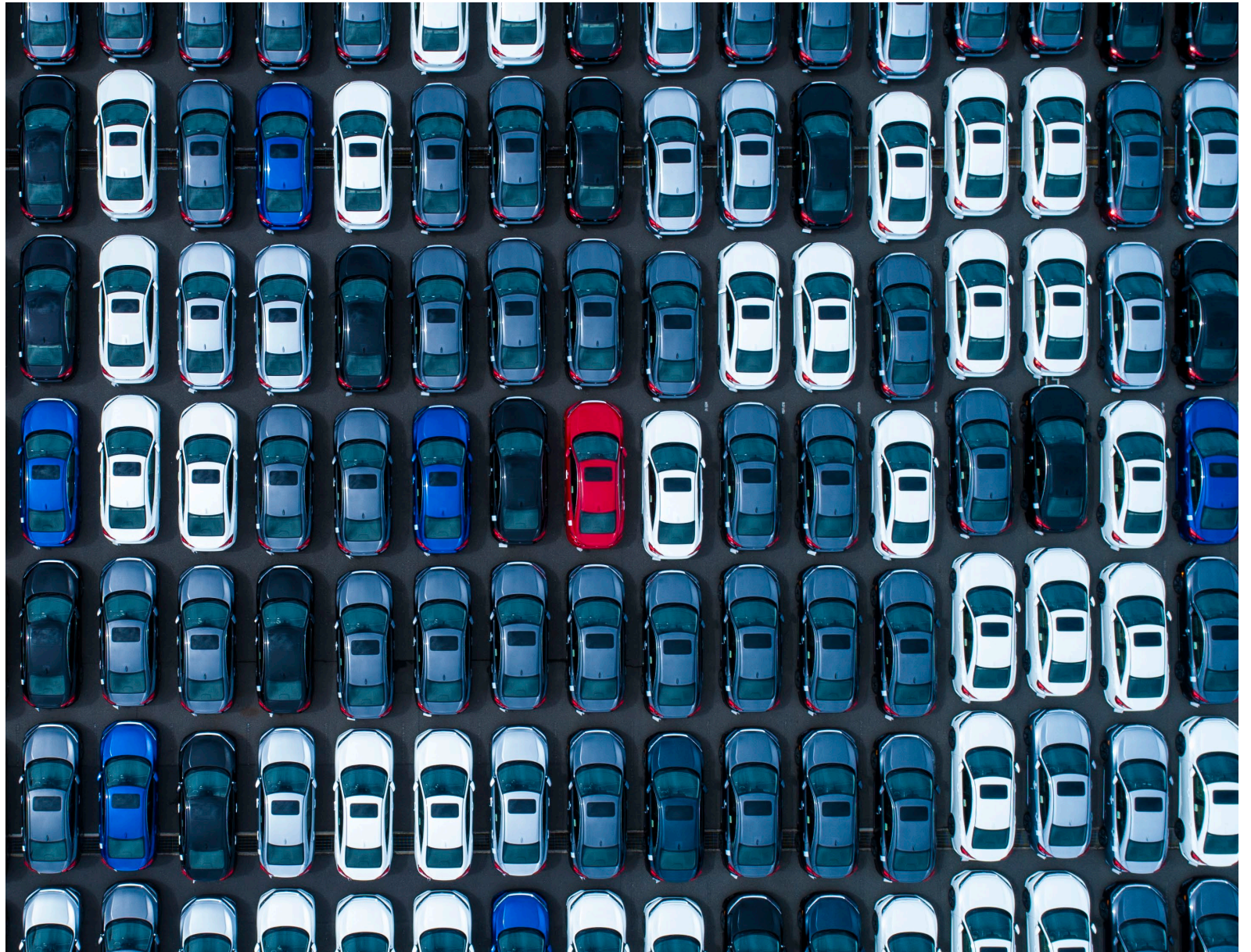
A close-up, low-angle shot of the robot WALL-E. He is holding a Rubik's cube in his right hand. His body is yellow and rusted, with the name 'WALL-E' and a circular logo on his chest. He has large, expressive eyes. The background is a dark, industrial setting with various mechanical parts and structures.

ENABLE AUTONOMY

It does not have to be fast to be
efficient

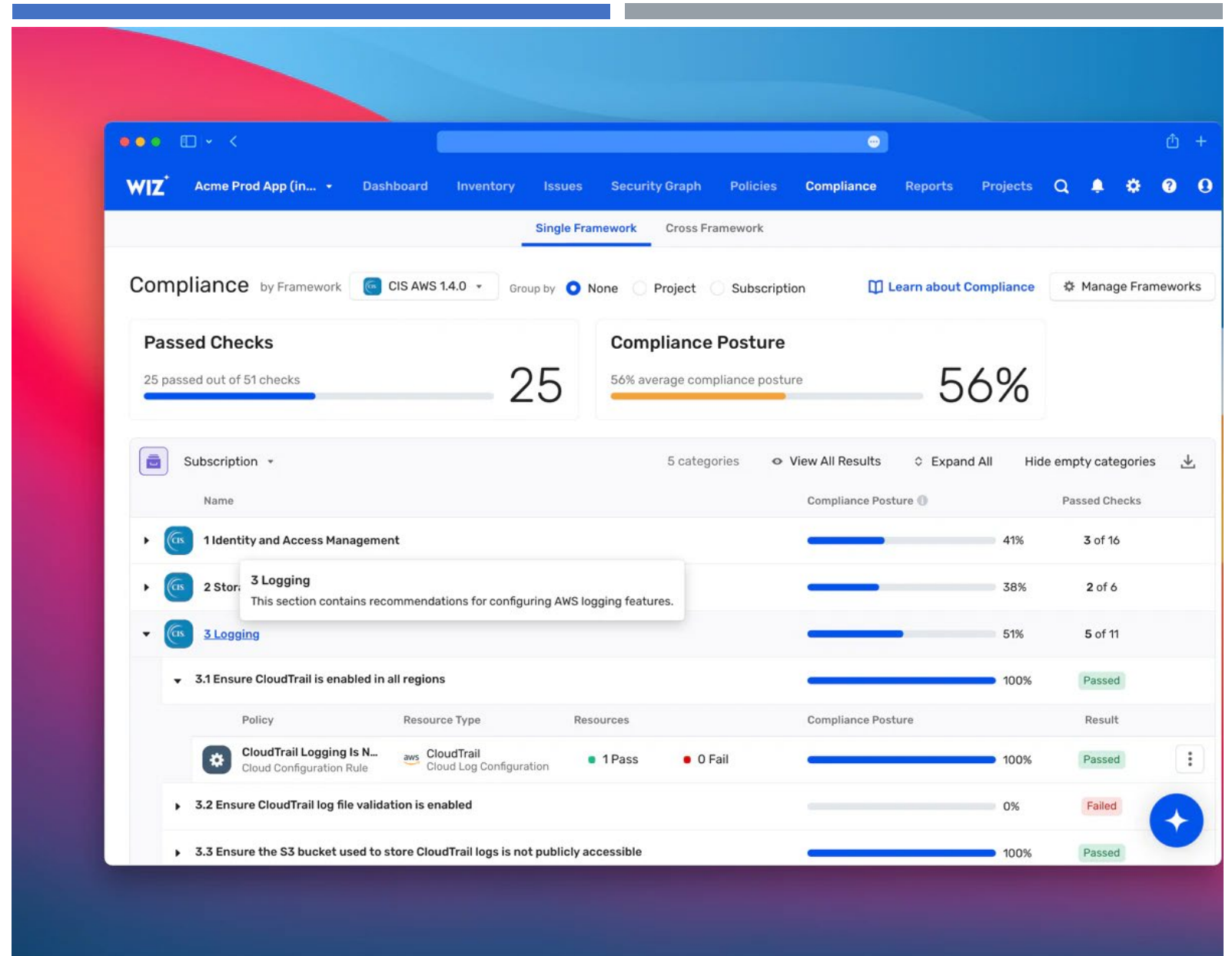
THE GRIDLOCK

- 59% of cyber teams are understaffed (ISACA, 2023)
- Engineers are naturally opposed to bureaucracy
- Needs for availability/resources exceed governance



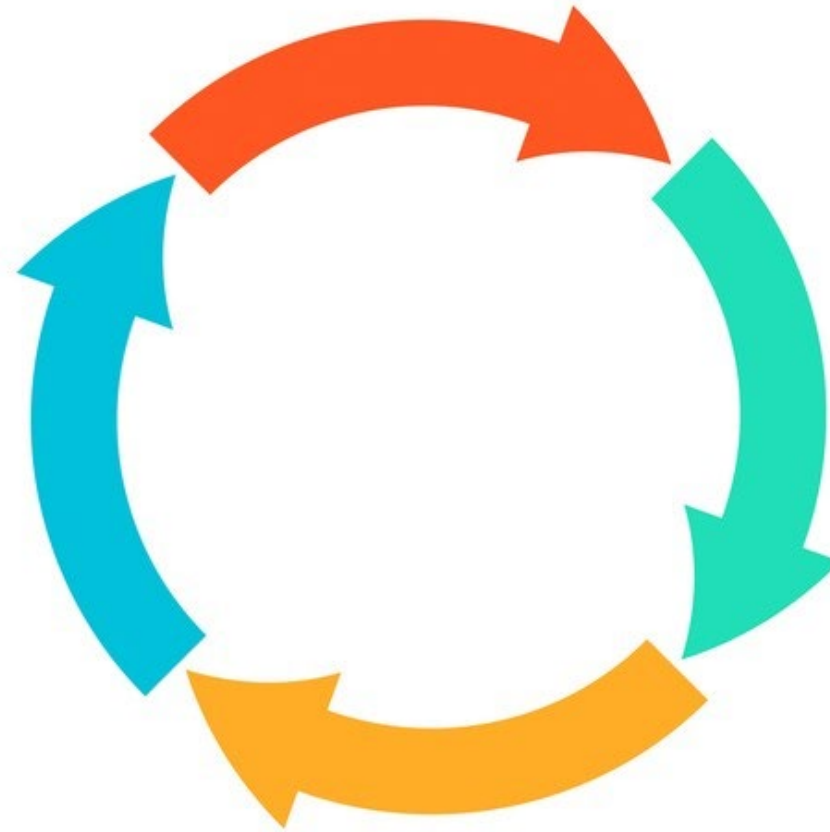
USE TOOLS

- Create avenues for “self-service”
- Develop workflows in ITSM for review and remediation
- Encourage operational leaders to establish champions



AUTONOMYPROCESS

- Allow runways for teams to push changes without security bottlenecks
- Utilize tools (Wiz, Black Kite, Snyk)
- Create feedback loops to ensure quality





PROMOTE COMMUNICATION

“A problem well-defined is a problem half-solved” – Charles Kettering

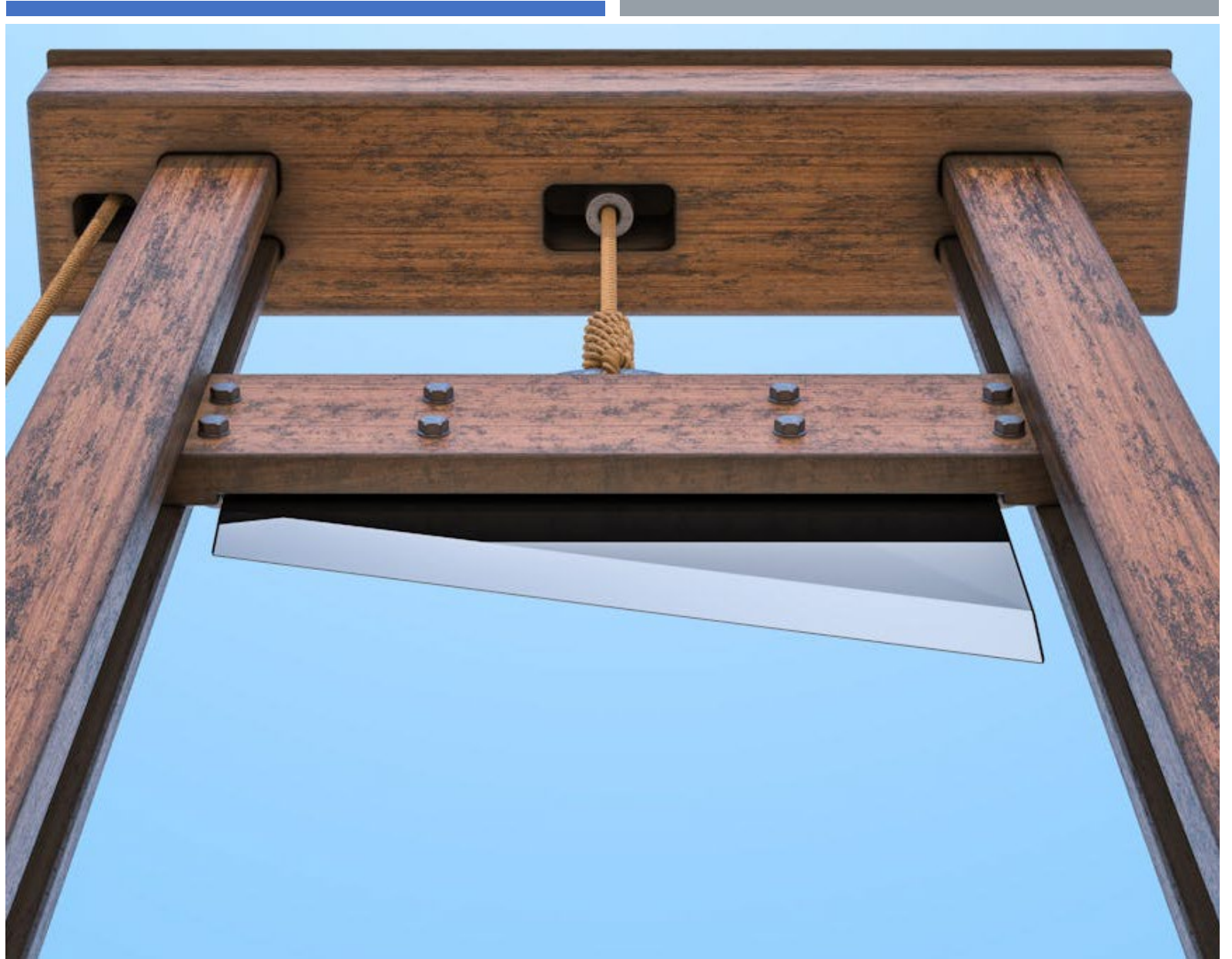


COMMUNICATION != MORE MEETINGS

- But more meetings may help
- Utilize collaboration software (Teams/Slack) to create focus groups for tackling cloud challenges
- Introduce opportunities for issues to be presented directly to engineering

ENGINEERS FIX PROBLEMS

- Good engineers like to fix problems
- High+ severity items may be easily fixed
- Context to identified issues is extremely valuable to both parties



REPORT KPIS

BRAG ABOUT WHAT
YOU'VE DONE





FRUITS OF LABOR

- Simple metrics help demonstrate value of combined teams
- Allows WIP to be illustrated
- Does not have to be pretty

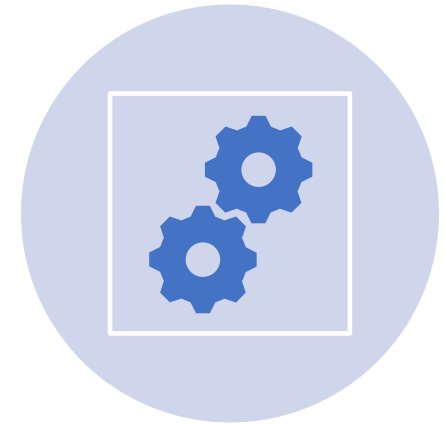
ESTABLISH COMBINED METRICS



OPEN VS CLOSED
VULNERABILITIES



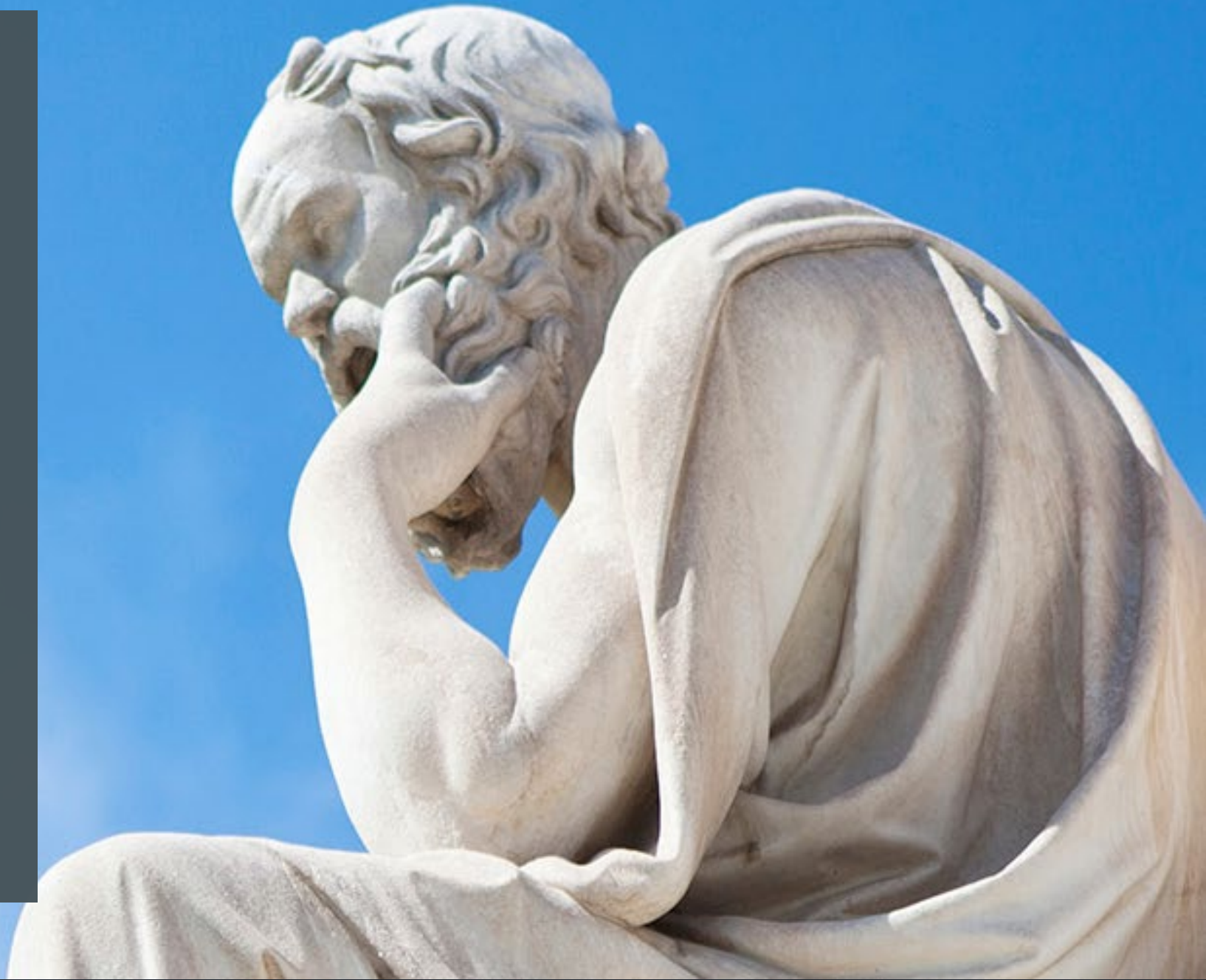
VENDOR RISK ASSESSMENTS
COMPLETED



SYSTEM STANDARD
DEPLOYMENT

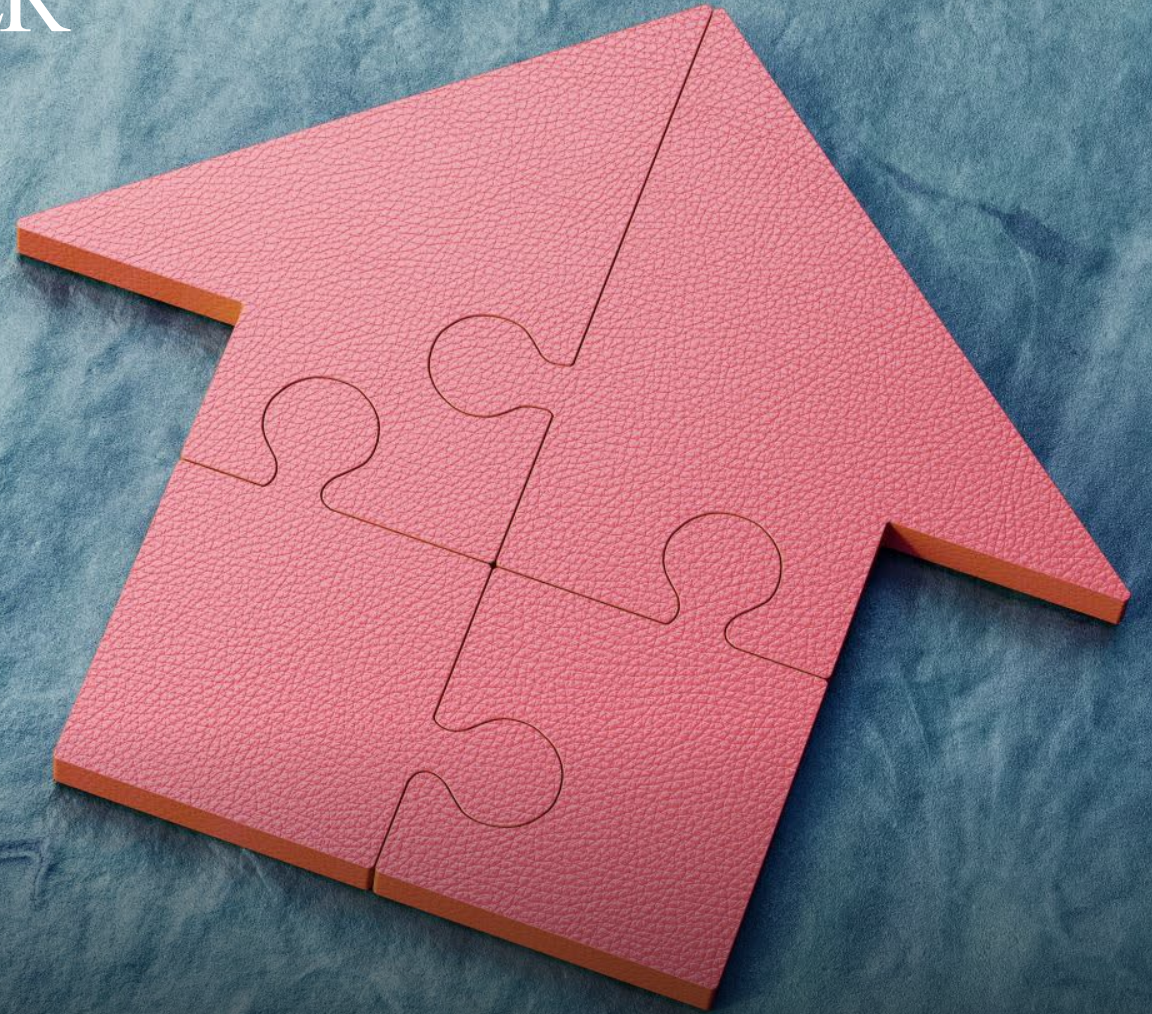
WHY MUTUAL METRICS MATTER

- Can't argue numbers
- Quantifying work helps demonstrate resource contention
- Shows effectiveness of focus groups



PUTTING IT ALL TOGETHER

- Create clarity of functional domains and establish working relationships
- Create standards to enforce expectations
- Enable runways for autonomous security processes
- Create conduits for engineers and GRC members to communicate directly
- Establish metrics that capture IT and Security cooperations



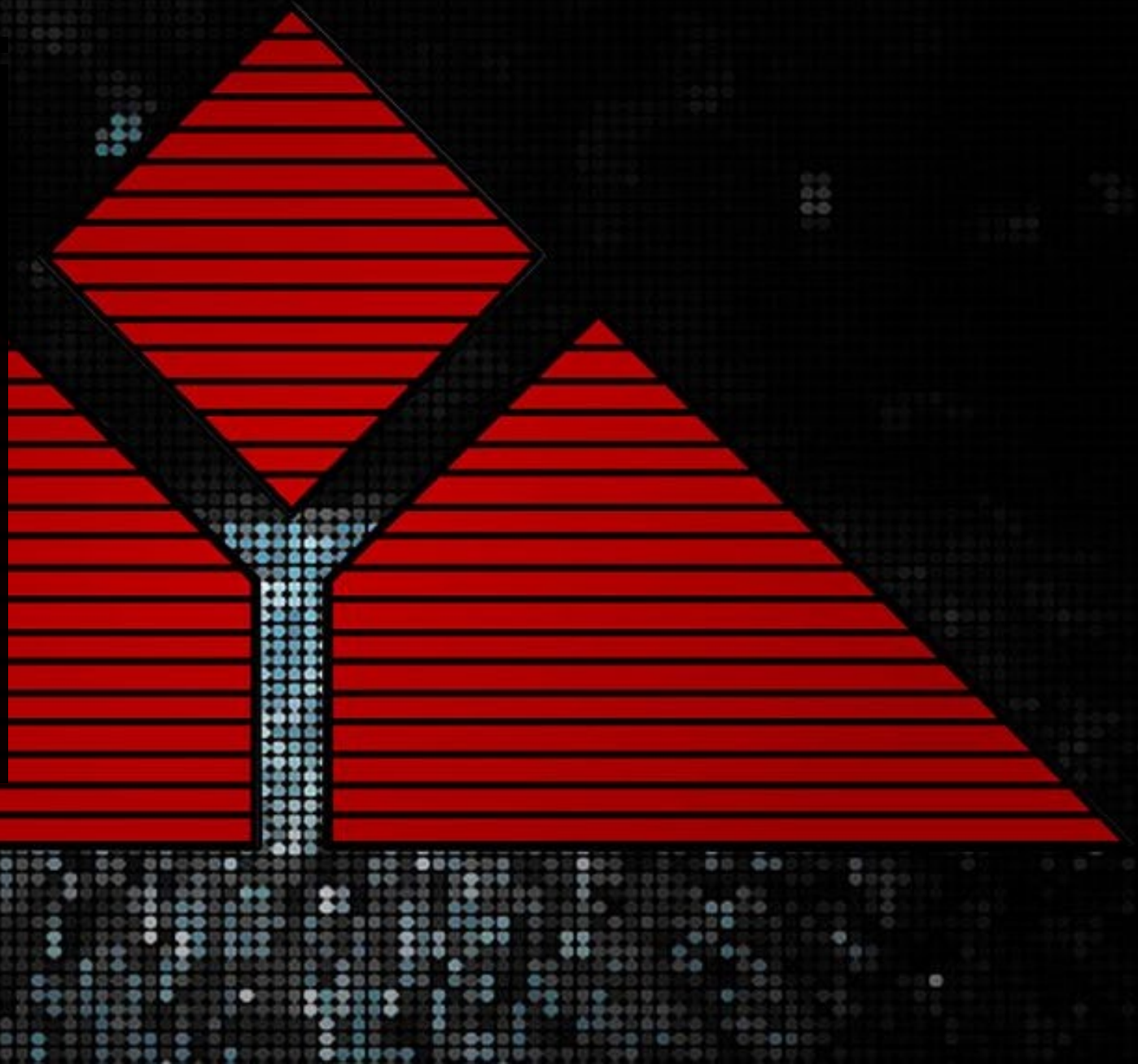


THE GOVERNATOR(S)?

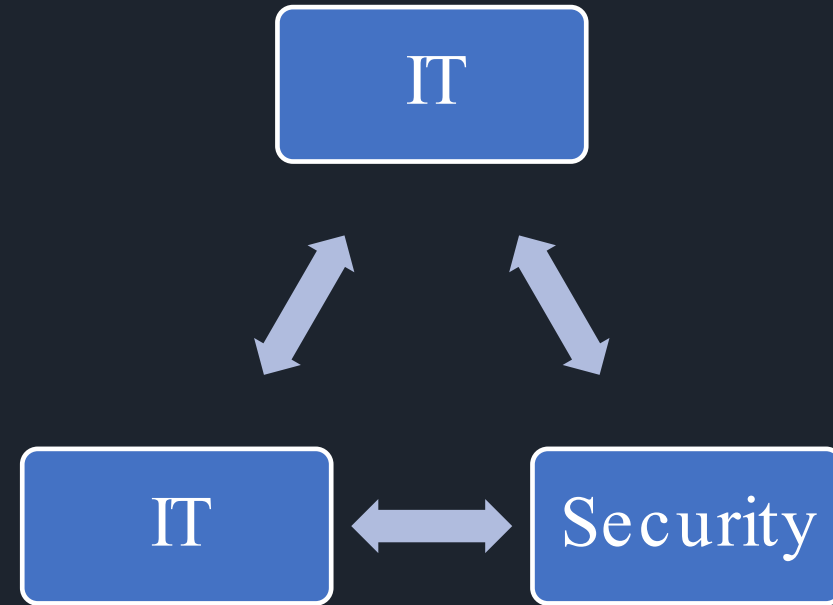
- Part man; Part machine
- Create focus groups of responsible parties
- Leverage tools like ITSM, CMDBs, and CASBs to set governance in motion

THE FUTURE OF CLOUD ENVIRONMENTS

- Speed, Speed, Speed
- Complex systems without a peek under the hood (LLMs)
- Higher need for delegated responsibilities



A PROPOSAL...



IT Engineers that report to security leadership that are integrated into ITSM workflow.

Resources dedicated/responsible for cloud environment changes

KEY TAKEAWAYS



- Cloud security is not a checkbox
- Cloud security is not a tool or service
- Creating conduits for security and technology teams to discuss cloud risks creates tangible benefits
- Standards = governance autonomy

THANK YOU



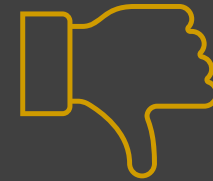
Connections

<https://linkedin/sethearby>



Contact

searby@forsynse.com



Concerns

devnull@skynet.gov