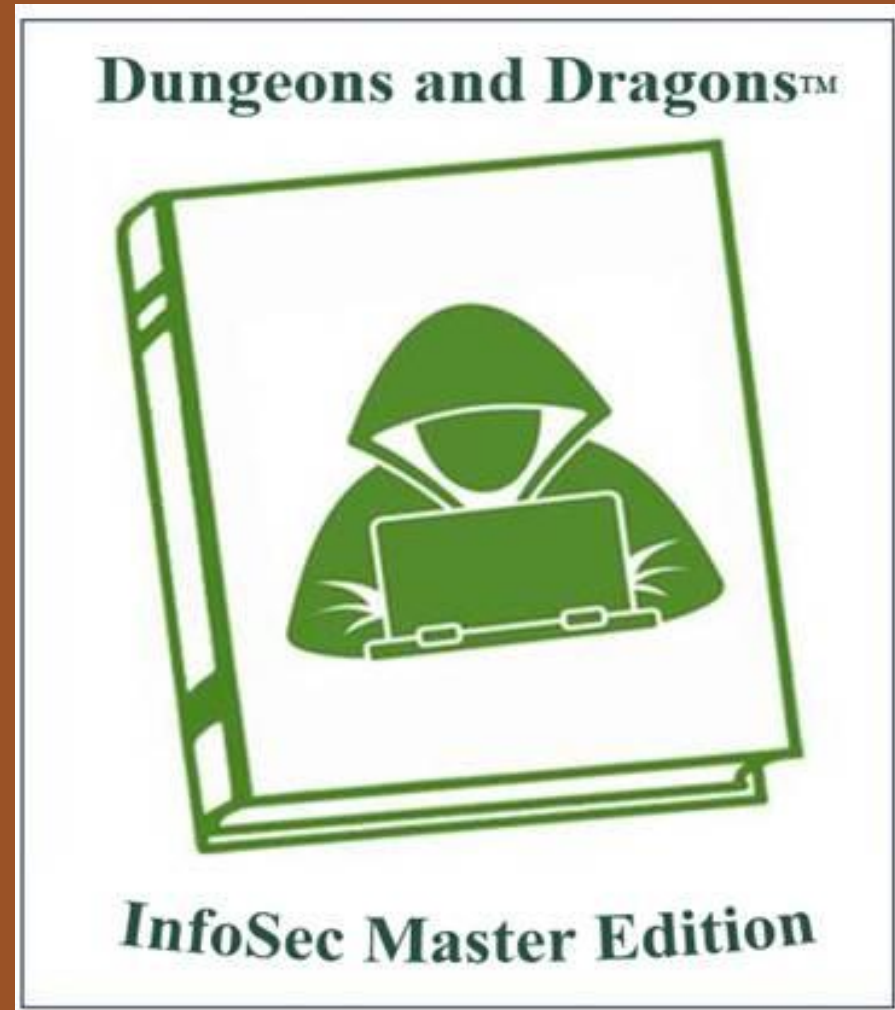


Welcome To The 10th Annual Hacking Conference



Welcome To The 10th Annual Hacking Conference

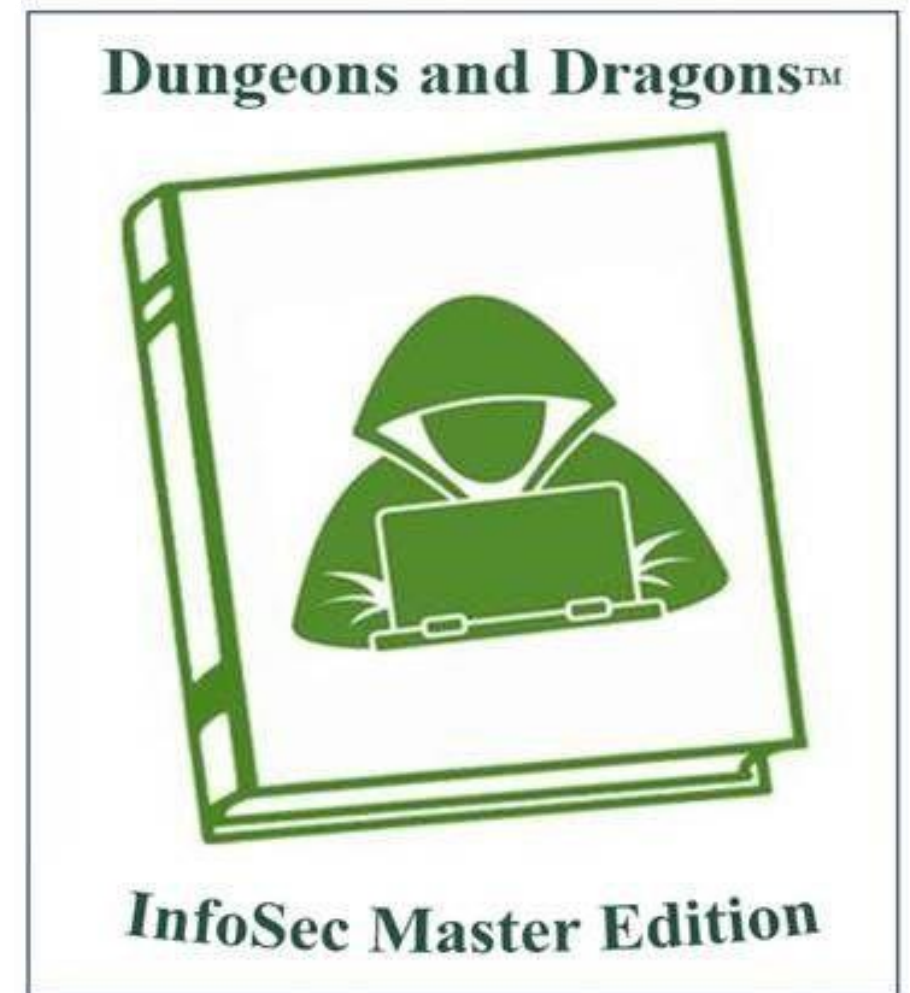
Remember to check-in to this session
on the app!



How to Develop your Own Security RPAs

The Journey of Identity-Based Solutions

Paul Hinds, CISM, CRISC, CDPSE, CISA
Founder/Managing Partner
Mitarbet Consulting Corp.

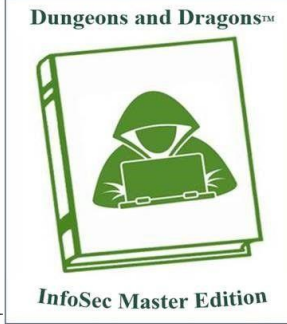


**Ways to eat monsters,
track rogues,
and avoid traps...**

INTRODUCTION

- Mitarbet Consulting – derived from the word “mitarbeit”
 1. Cooperation, Collaboration
 2. Assistance
- Broad cybersecurity, risk, privacy, and IT operations background
 - Big 4 and Tier 2 accounting and consulting firms
 - Industry experts
 - US and international development and support centers – India, Egypt, Israel, Turkey, etc.
- CISO/CIOs, Advisors, Board Members, ranging from high-tech, AI companies to global manufacturing, financial services, and healthcare clients.
- Addressing CMMC, Safeguards Rule, 800-171, ISO 27001, TISAX, etc.





STICKING WITH THE CONFERENCE THEME

The results of the party's choices and the overall story line for the game are determined by the Dungeon Master (DM) according to the rules of the game and the DM's interpretation of those rules.^{[29][30]} - **Your External Auditor**

The DM selects and describes the various non-player characters (NPCs) that the party encounters, the settings in which these interactions occur, and the outcomes of those encounters based on the players' choices and actions.^{[7][25]} - **Materiality, systems, and control requirements.**

Encounters often take the form of battles with "monsters" – a generic term used in D&D to describe potentially hostile beings such as animals, aberrant beings, or mythical creatures.^[29] - **People who perform the controls, the business area Control Owners, third-party contractors, and anyone else who has the evidence you need.**

In addition to jewels and gold coins, magic items form part of the treasure that the players often seek in a dungeon.^[31] Magic items are generally found in treasure hoards, or recovered from fallen opponents; sometimes, a powerful or important magic item is the object of a quest.^[32] - **good, clean, accurate, no confusion, no change, Control Evidence.**



STICKING WITH THE CONFERENCE THEME

The game's extensive rules – which cover diverse subjects such as social interactions,^[30] [magic use](#),^[33] combat,^[30] and the effect of the environment on Controls^[34] – allows the DM to deviate from the published rules^[30] or make up new ones if they feel it is necessary.^[35] – PCAOB, National Office, and other far-away gods who control the destiny of the DM.

This activity is performed through the verbal impersonation of the characters by the players, while employing a variety of social and other useful cognitive skills, such as logic, basic mathematics and imagination.^[27] A game often continues over a series of meetings to complete a single [adventure](#), and longer into a series of related gaming adventures, called a "[campaign](#)".^{[7][28][29]} – SOX Audit Season, Quarterly and Annual testing.

When working together as a group, the [player characters](#) (PCs) are often described as a "[party](#)" of adventurers, with each member often having their own area of specialty which contributes to the success of the whole.^{[25][26]} – Internal Audit, SOX Controls Team, IT first line controls tester.

QUESTION #1

- Which role do you perform in this game?
 - A) Internal Audit / SOX Control Team
 - B) IT Controls Owner / Tester
 - C) Financial Controls Owner / Tester
 - D) Third-party Auditor
 - E) Other



HISTORY LESSON

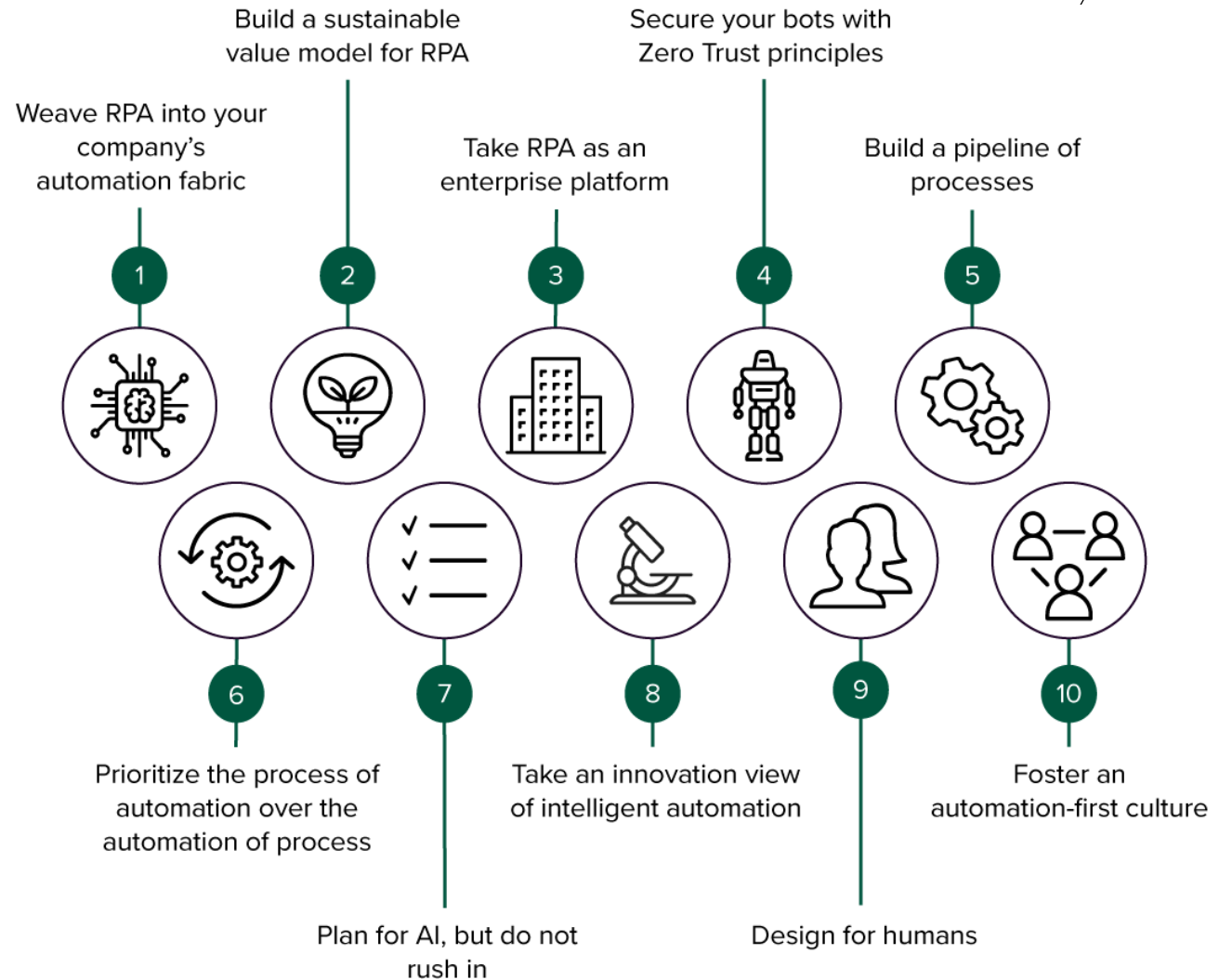
The term "Robotic Process Automation" (RPA) emerged in the early 2000s. The first RPA software was developed in the early 2000s. The term "RPA" was coined in 2012 by Phil Fersht, founder and lead analyst at HFS Research.

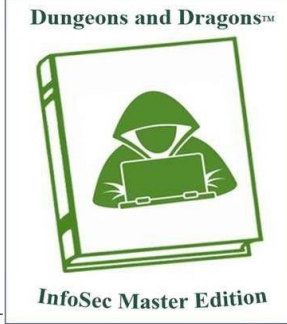
The initial development of RPA began after the 1990s. The first RPA product was released in 2003 by Blue Prism. UiPath and Automation Anywhere released their automation libraries around the same time.

RPA became officially recognized by large-scale businesses around 2012. The technology became more popular in 2018 as companies undertook digital transformation and RPA platform capabilities improved.

HISTORY LESSON

10 Golden Rules of RPA Success - Forrester.





HISTORY LESSON

Rule 2: Build A Sustainable Business Value Model For RPA

Enumerating the benefits of automating simple processes is easy enough. But as process complexity increases, it also becomes more difficult to calculate ROI because of the sheer number of factors and dependencies involved. The importance of structuring a robust and repeatable business case for every candidate automation cannot be overstated.

Unfortunately, we, the collective, have not the time, skills, or money to build our own solutions.

With the staffing shortages we face, taking on a new IT skillset is less than ideal.

We have reached the 20-year maturity, where the technology is now ready to be adapted into other technologies and services, and no longer a stand-alone project or set of solutions.

QUESTION #2

- What level of RPAs do you use?
 - A) We really don't use RPAs
 - B) We have a couple of RPAs in IT
 - C) We have a couple of RPAs in Financial Controls
 - D) We have RPAs in some IT and Financial Controls
 - E) We have several RPAs in both or either IT or Financial Controls – much better than everyone else

SOX COMPLIANCE COSTS – REASON TO RE-EVALUATE

Protiviti Survey

The average cost to test SOX controls is between \$1 million and \$2 million. The average SOX budget is \$1,725,500, and internal audit teams spend an average of 5,000 to 10,000 hours on SOX programs annually.

The average cost to test SOX controls varies by company size:

- Small firms: Less than \$25 million in revenue, average cost is \$181,300
- Companies with \$500 million or less: Average cost is \$651,000
- Companies with \$10 billion or more: Average cost is \$1.8 million

A single compliance test of a control could cost \$10,000 in external audit time.

Larger companies and global companies spend \$2 million or more. Organizations from industries including insurance and telecommunications also spend \$2 million or more per year.

SOX COMPLIANCE COSTS – REASON TO RE-EVALUATE

AuditBoard Article

While we no longer question the effectiveness of SOX, concerns over the rising costs and resource burdens of compliance continue to plague companies. As reported by Protiviti, SOX hours have risen by more than 10% for 68% of publicly held companies, and a staggering 82% of private companies preparing for IPO. External audit fees are also on the rise as companies struggle to meet increasingly stringent regulatory requirements.

This begs the following questions: How can a CFO get more out of their Internal Audit function? What are the ways CAEs can reduce SOX spend and decrease hours spent, as well as perform more value-add audits? Below, we take a closer look at the industry statistics.

Current State of SOX

A company's average SOX budget is between one million to two million dollars, and Internal Audit teams spend an average of 5,000 to 10,000 hours on SOX programs annually. But 70% of those hours are actually spent on administrative tasks - mainly, reconciling and managing spreadsheets.

SOX COMPLIANCE COSTS – REASON TO RE-EVALUATE

The Spreadsheet Problem

Today, over 95% of companies still manage their SOX programs manually on spreadsheets. While spreadsheets are useful in some contexts for organizing data, they are not ideal for managing SOX data for several reasons:

- Spreadsheets volume. For each documented control, there are five to six spreadsheets, including individual test sheets, PBC listings, RCMs and status sheets. SOX involves anywhere from 1,000 to 3,000 spreadsheets and documents.
- High user volume. Anywhere from 10 to 300 total users can be handling the RCM and data spread across multiple spreadsheets and documents.
- SOX requirements are dynamic. This means frequent changes to reports, test sheets and the overall structure of the SOX environment.
- SOX is highly cross functional. It requires real-time collaboration between multiple departments and teams.

SOX COMPLIANCE COSTS – REASON TO RE-EVALUATE

What about the existing GRCs and SOX software?

When SOX first passed, technology companies were not sufficiently savvy enough in SOX to design solutions that could effectively meet its pain points. As a result, the tools that initially entered the market were over-engineered to the extent that they complicated the process instead of streamlining it.

Many large GRC solutions introduced “all-in-one” solutions that were clunky and ill-suited for SOX. Other companies who initially built solutions for other purposes, such as financial reporting, attempted unsuccessfully to repackage their technology to meet SOX requirements.

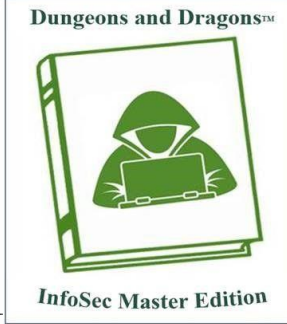
Many public companies that experienced a failed GRC implementation became disillusioned and jaded, and eventually returned to Excel to manage SOX manually.

SOX COMPLIANCE COSTS – REASON TO RE-EVALUATE

How can the industry move forward more cost effectively?

The key to maximizing SOX resources lies in leveraging technology to automate manual enterprise-wide processes. Other enterprise accounting and finance teams have already tapped into automation to drive process efficiencies. While many SOX teams have yet to fully embrace this technology, forward-thinking SOX teams are quickly seeing the return of SOX automation software. Several benefits of automation include:

- Reduced administrative hours and efforts spent on SOX
- Internal Audit teams are freed to perform more value-add audits
- Improved visibility into SOX environments
- Increased quality of internal controls
- Reduced number of financial restatements
- Improved external auditor collaboration and reliance



SOX COMPLIANCE COSTS – REASON TO RE-EVALUATE

Protiviti Survey

The time spent on SOX compliance increased across the board.

	SOX compliance hours increased	SOX compliance hours decreased
SOX filer status		
Large accelerated filer	68%	9%
Accelerated filer	55%	13%
Non-accelerated filer	39%	29%
Size of organization		
\$10 billion or greater	73%	6%
\$5 billion to \$9.99 billion	65%	14%
\$1 billion to \$4.99 billion	57%	12%
\$500 million to \$999.99 million	38%	29%
Less than \$500 million	59%	10%

SOX COMPLIANCE COSTS – REASON TO RE-EVALUATE

Protiviti Survey

The Protiviti survey of 564 SOX compliance professionals also found that 74 percent of respondents want to improve the automation of their SOX compliance program, but numerous practical obstacles make that ambition difficult to achieve.

*Which of the following represent the challenges keeping you from automating your control testing?
(Multiple responses permitted)*

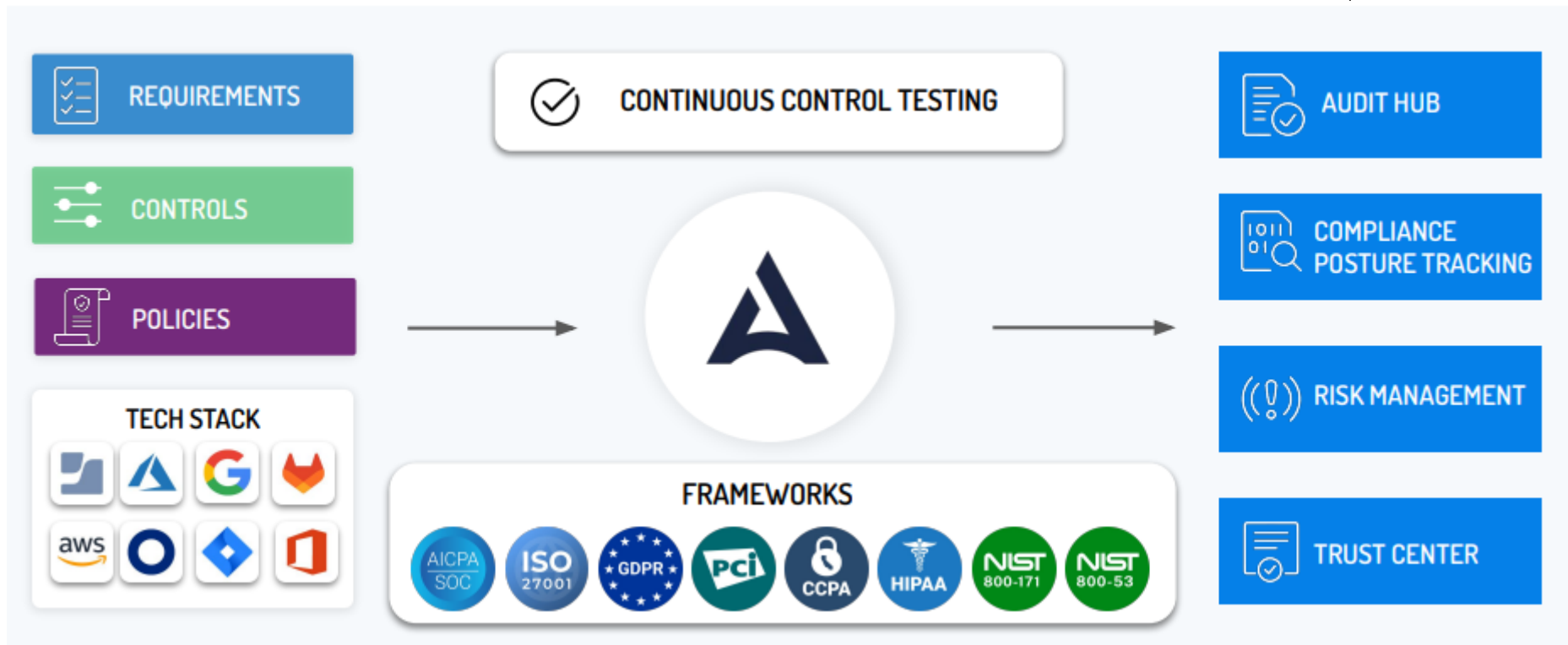
Many areas of the SOX control environment are not conducive to automation	47%
Lack of time to spend exploring automation due to other priorities	39%
Level of effort to implement, train, govern and maintain	34%
Lack of funding and/or executive support for automation	31%
Lack of talent/skilled resources to manage an automation program	31%
Lack of knowledge on available tools and technology	29%
Other	2%
None of the above	3%

QUESTION #3

- Define your SOX Maturity/Stability
 - A) We have limited changes in our SOX program year to year
 - B) We have some changes, but pretty limited due to system changes or small M&As
 - C) We have a lot of M&As or system changes every year and spend less than 25% of our budget on new work
 - D) We have a lot of M&As or system changes every year and spend over 25% of our budget on new work

WE ARE ENTERING A PERIOD OF RADICAL TRANSFORMATION

Technology solutions are now not unique to each client but are being developed to be shared across clients. We all have similar controls. No more the issue of having to justify your own GRC tools, your own RPA tool, and your own development costs.



WE ARE ENTERING A PERIOD OF RADICAL TRANSFORMATION

ISO 27001 – 110 control requirement – for multi-million-dollar technology companies, achieving ISO certification in 6 months or less.

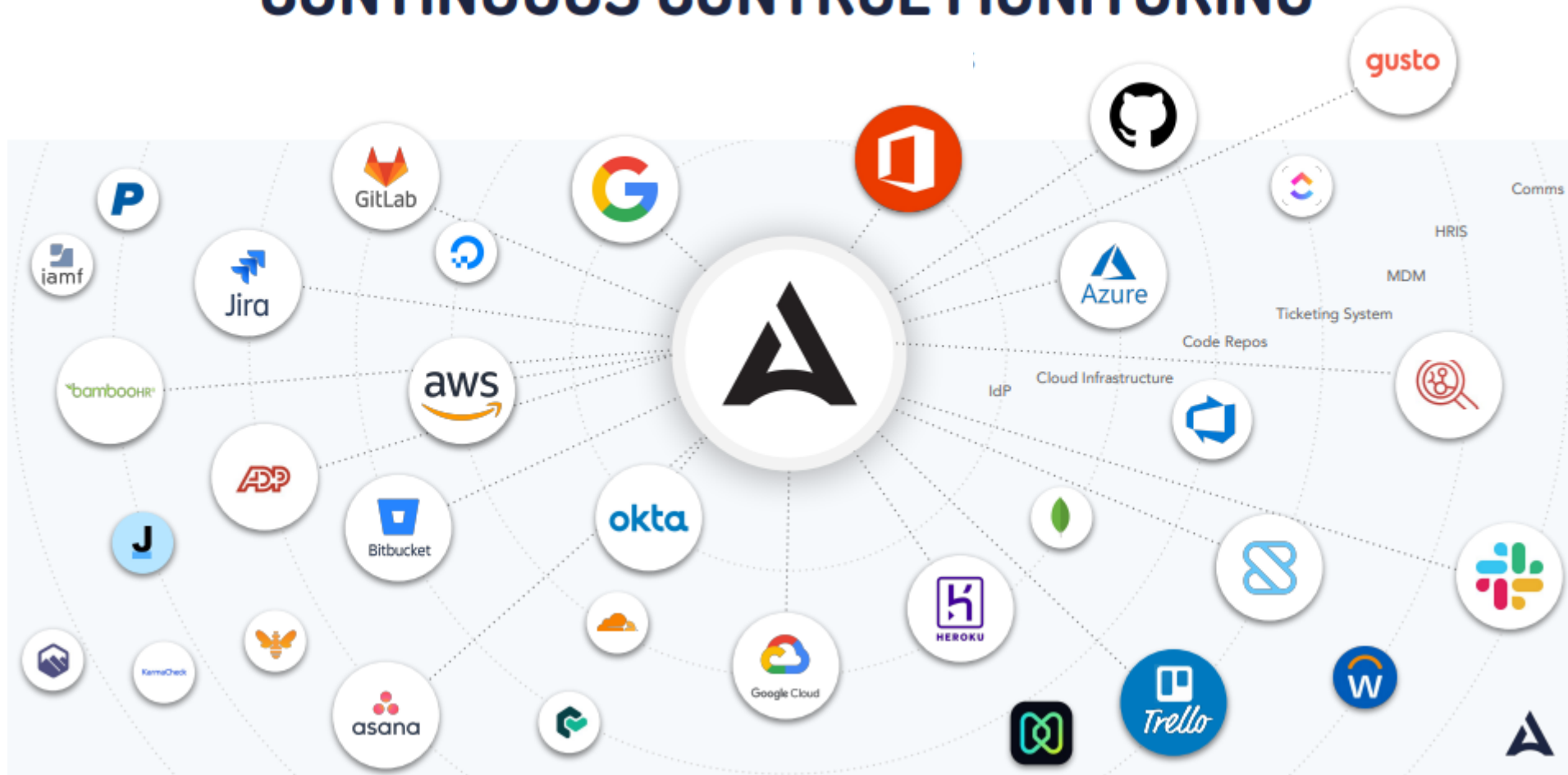


We drive ITGC testing time and costs down by 40% over three years. And are more adaptable to new systems and controls, saving you more money in the long-term.

- Video capture and marketing testimonial company (60% reduction in US based certification costs)
- AI financial services customer support and newsletter company (certification in 6 months, 40% reduced original consulting proposal)

WE ARE ENTERING A PERIOD OF RADICAL TRANSFORMATION

CONTINUOUS CONTROL MONITORING



WE ARE ENTERING A PERIOD OF RADICAL TRANSFORMATION



Few of us have only one control framework we must follow. Leveraging 350 controls, mapped to over 10 top frameworks, you can test and monitor against all your requirements in one dashboard.



WE ARE ENTERING A PERIOD OF RADICAL TRANSFORMATION

Custom Frameworks

- Create custom frameworks with custom controls
- Map any controls to Drata's automated tests without sacrificing automation
- Share controls between frameworks to reduce duplicative efforts
- Track progress of your custom framework in the Readiness Dashboard along with your other supported frameworks, allowing you to manage your entire security program in one central solution



Custom Frameworks made it easy for us to take the controls we had worked on with our auditors and drop them directly into Drata while mapping them against the other controls that the team is already tracking in the platform.

Tom Conklin, CISO
Fivetran

**Cut Audit Time
by 50%**



WE ARE ENTERING A PERIOD OF RADICAL TRANSFORMATION

CUSTOM RPA DEVELOPMENT FOR THOSE LEGACY UNIQUE SYSTEMS

Should you have legacy platforms and controls that are not currently addressed by the portfolio of RPAs that are available, many of these can still be developed at a significant discount because many of these can be used by other organizations looking for the same solution.

Development teams in India, Israel, US, and other international locations.

NEW TOOLS LEAD TO NEW SOLUTIONS





MITARBET
CONSULTING

QUESTIONS?

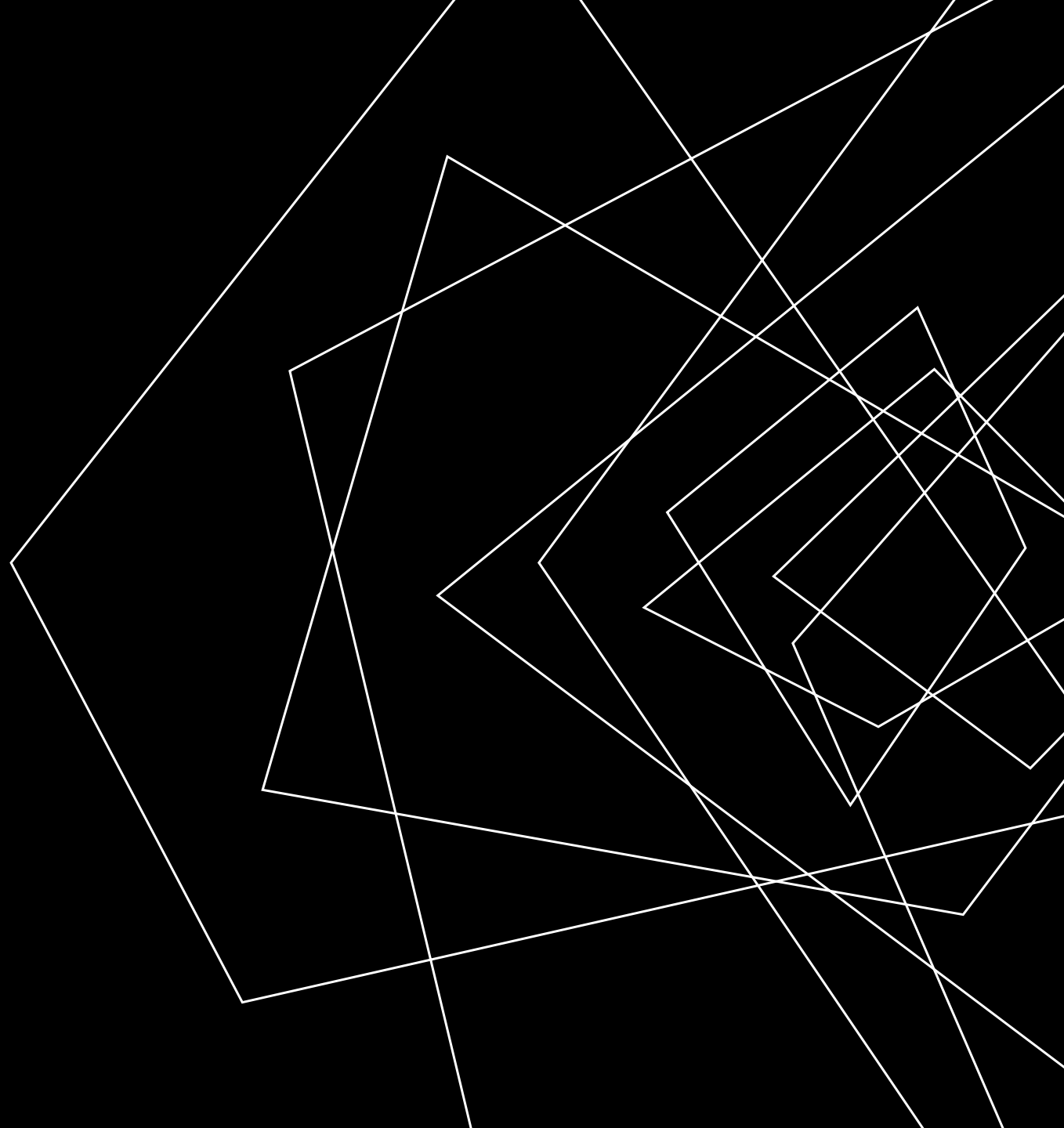
Paul Hinds

Founder/Managing Partner

Mitarbet Consulting Corp.

(224) 723-4817

paul.hinds@mitarbetconsulting.com



Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session
on the app!

