protiviti®
Face the Future with Confidence

# SEGREGATION OF DUTIES: THE INCREASING BURDEN OF PROOF

Vijan Patel
Protiviti

Houston IIA Conference - April 3, 2017

Protiviti Perspective provided by Brandon W., Houston

# WHY TALK ABOUT SEGREGATION OF DUTIES?

1. Not groundbreaking but still the best protection against fraud

2. Times are changing…

   - Companies are slimming down – especially in O&G
   - Regulators are concerned
   - External auditors are ratcheting up the bar
   - New technologies give unprecedented insight into the good, bad, and ugly

3. Given new scrutiny, pressures, and mountains of information, keeping on top of SOD has become a real challenge

# ACCESS IN THE NEWS – IS ANY PRESS GOOD PRESS?

**Controller embezzles $8.7 million over 3 years**

**VP of IT Defrauds company $8.2 Million over 3 years**

**Accountant embezzles $3.4 million**


**Disclosure of 3 Material Weaknesses, 7 Significant Deficiencies**

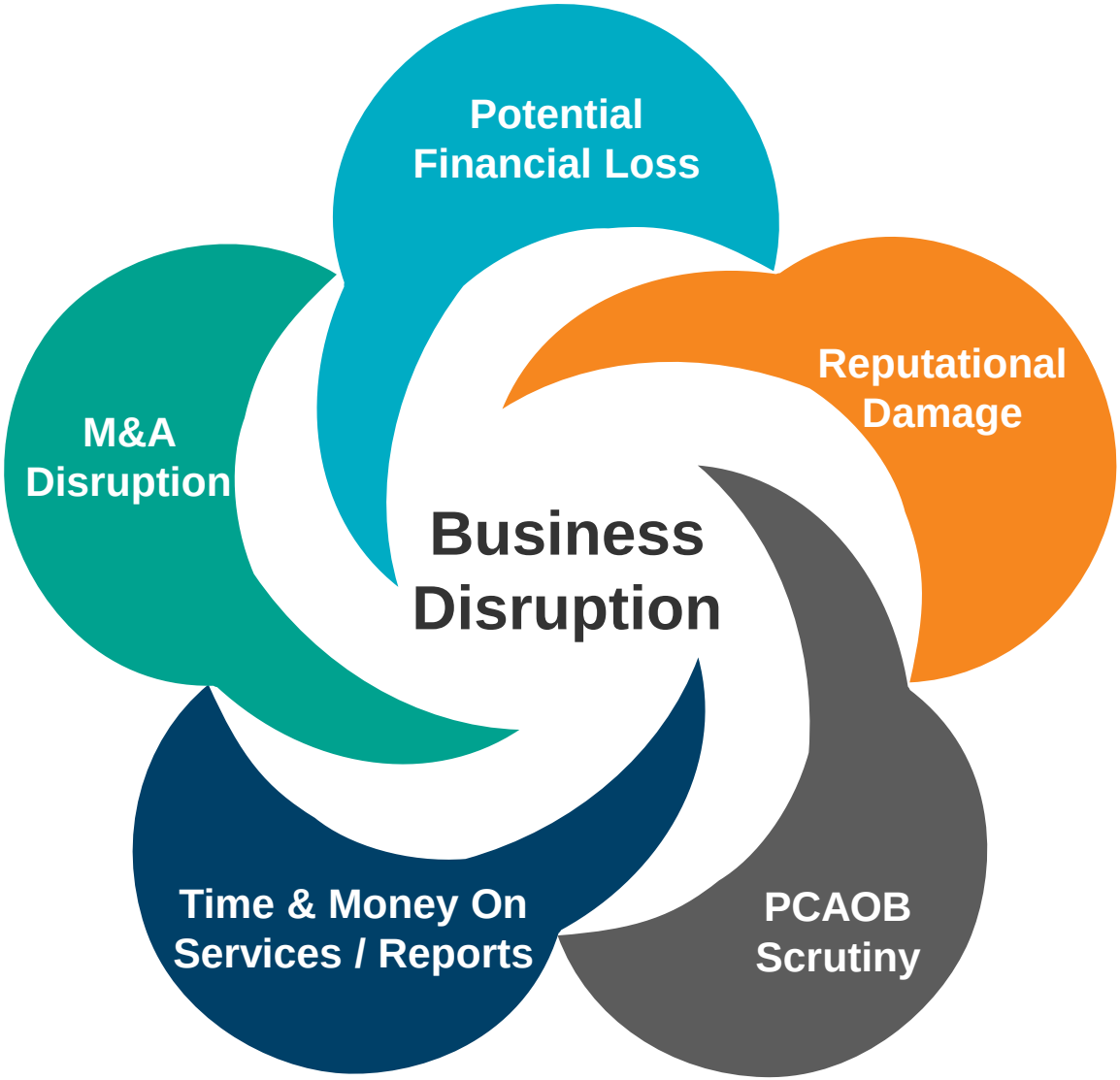
**Retraction of external and management conclusions over ICFR**





protiviti

# THE IMPACT OF MISMANAGEMENT

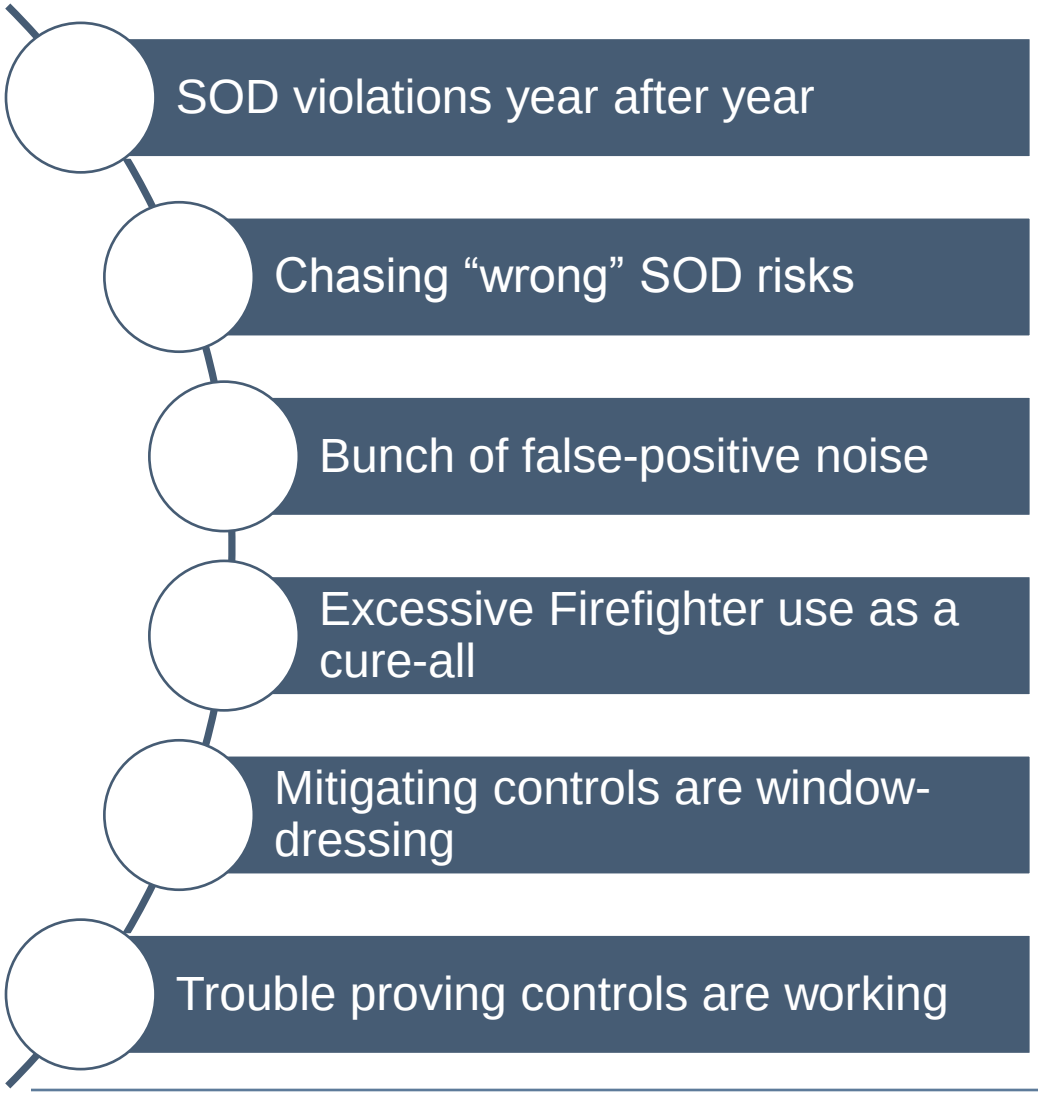







protiviti

# FRUSTRATIONS ARE COMMON



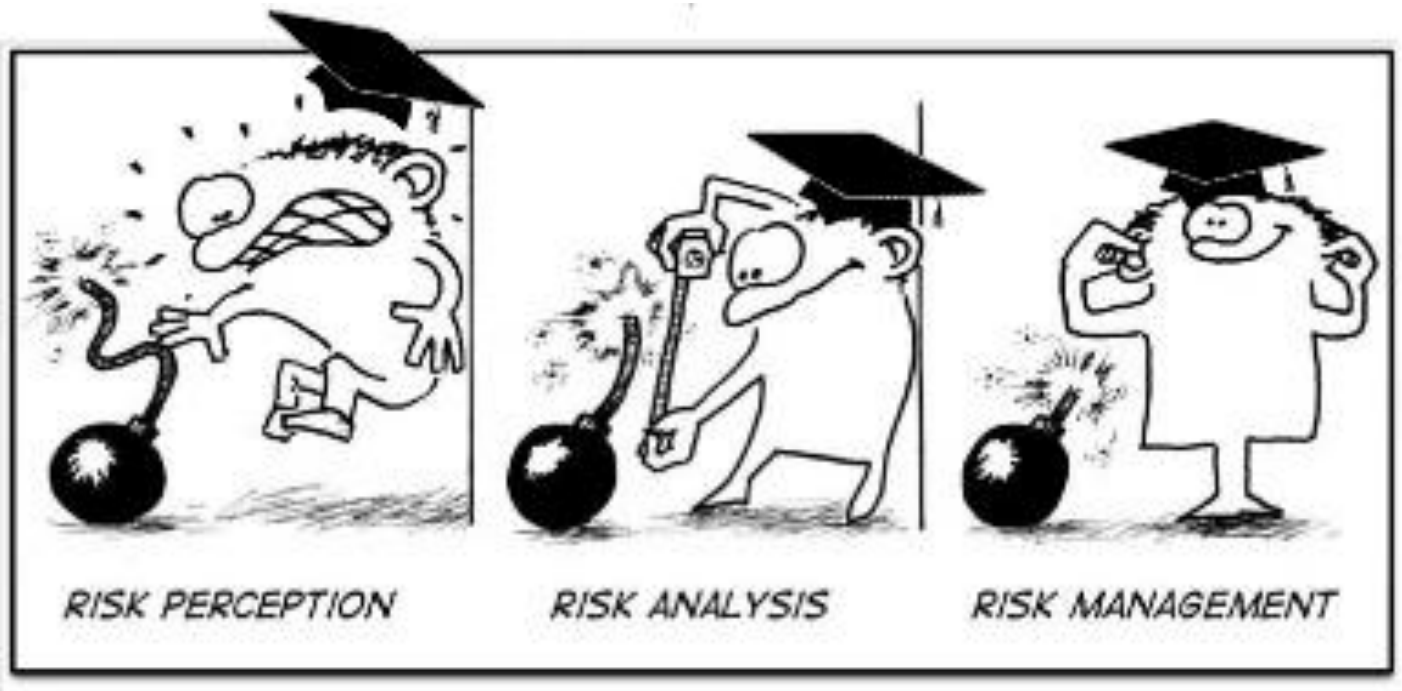

Do any of these sound familiar?





protiviti

# IS IGNORANCE BLISS?








protiviti

# IS THERE SUCH A THING AS TOO MUCH CONTROL?






protiviti

# ONE SIZE DOES NOT FIT ALL






protiviti

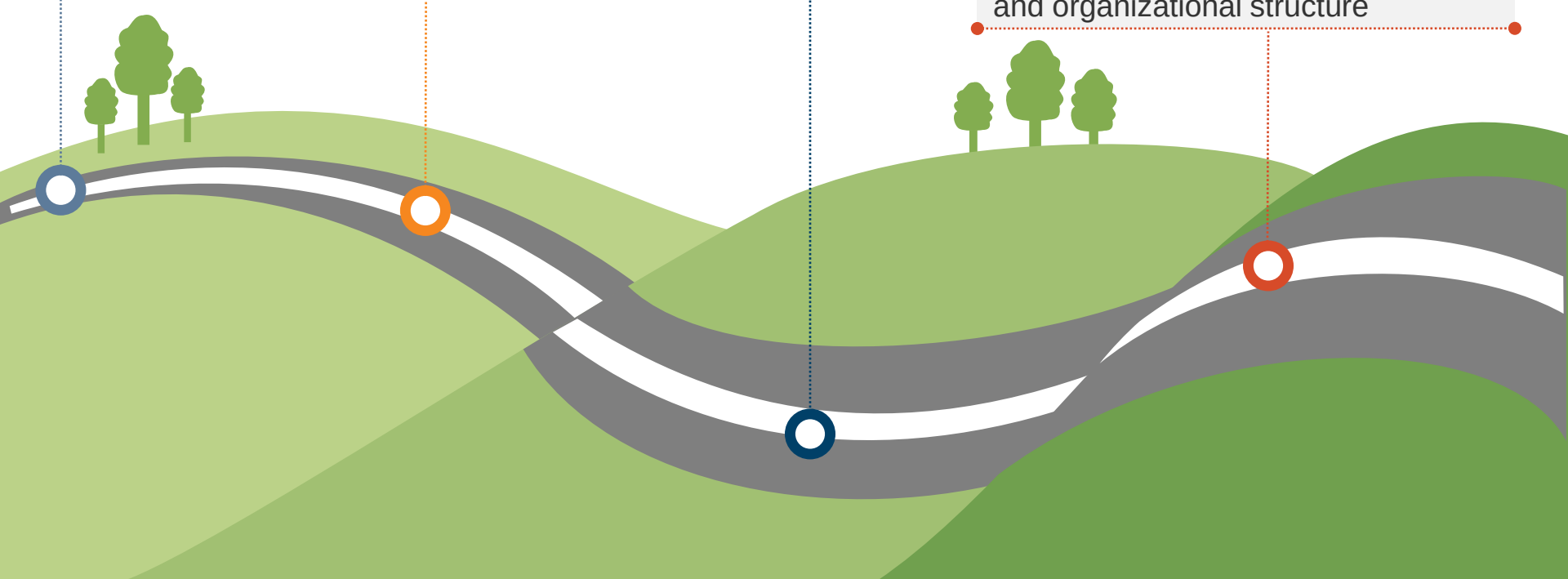
# THE HISTORICAL ROAD TO SOD MANAGEMENT

**Periodic Checks** – Limited manual analysis performed as part of annual SOX efforts

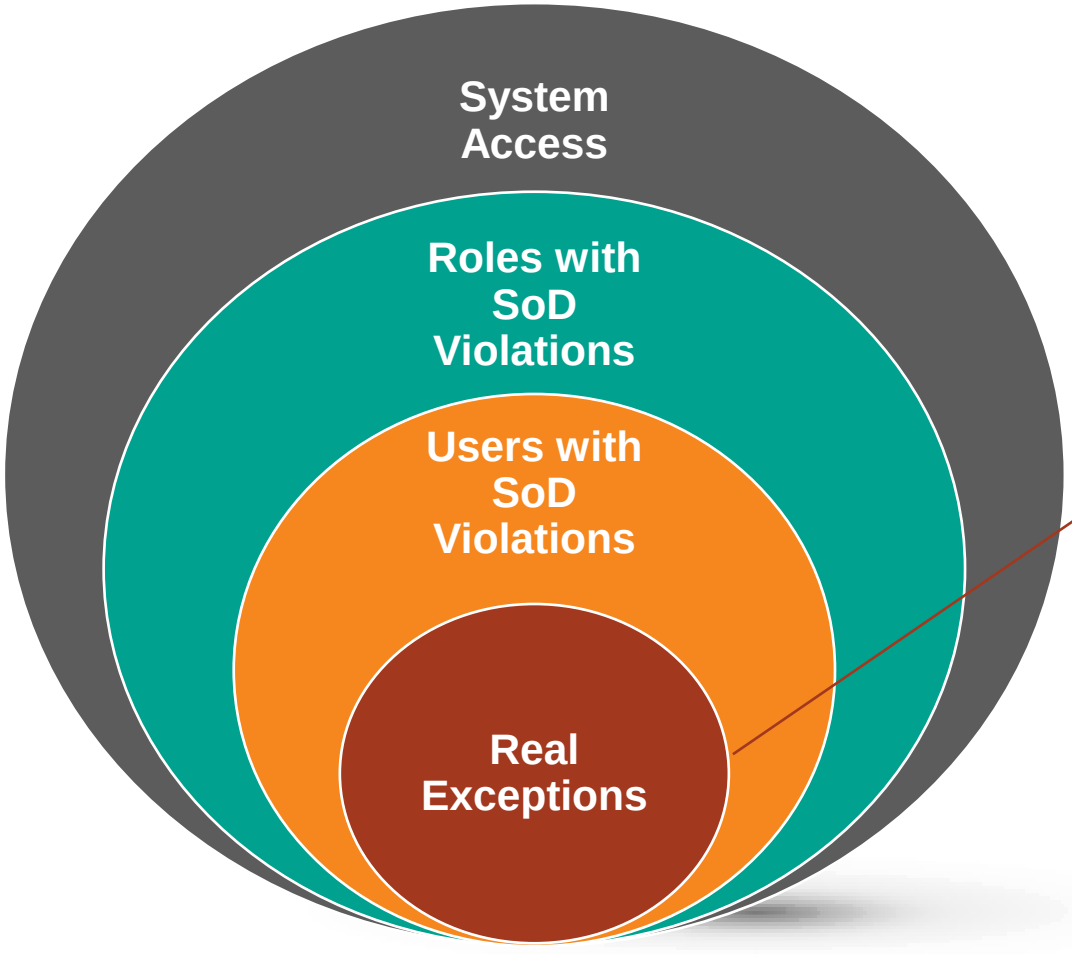
**Limited Analysis –** Intermittent SOD access review using out-of-the-box rules in a reporting tool

**Proactive Checks –** Custom SOD ruleset and access checks during provisioning process, including documentation of mitigating controls

**Optimized Security –** Roles/permissions are built inherently free of SOD conflicts and security assignments reflect responsibilities and organizational structure



# WHAT IS SOD QUANTIFICATION?




Why focus here?

- Identify *actual occurrences* of SOD violations
- Understand *who* did it, *how many* times, and for *how much*
- In the *absence of controls* at the above layers, true comfort can still be obtained





protiviti

# CASE STUDY #1

Fortune 500 Power Tools Manufacturer

# PROJECT OVERVIEW

**Company**

- Fortune 500 Company - Power Tools Manufacturer
- 2 SAP production environments

**Issue**

- Significant deficiency due to a large volume of SOD issues
- Opened the door to financial misstatement and fraud
- Difficult to determine how ‘material’ the deficiency really was

**Results**

- SOD quantification project contained the exposure
- Implemented a process to investigate, and follow up on actual violations
- Avoided escalation to material weakness




protiviti

# APPROACHES TO SOD QUANTIFICATION


- Point-in-time assessment (Defined time period)
- Detect actual SoD Violations
- Multiple point-in-time assessment tools available

- Ongoing Review
- Manage Financial Risk
- Process Improvements
- Requires developed tools

What Happened for the Past Quarter/Year?

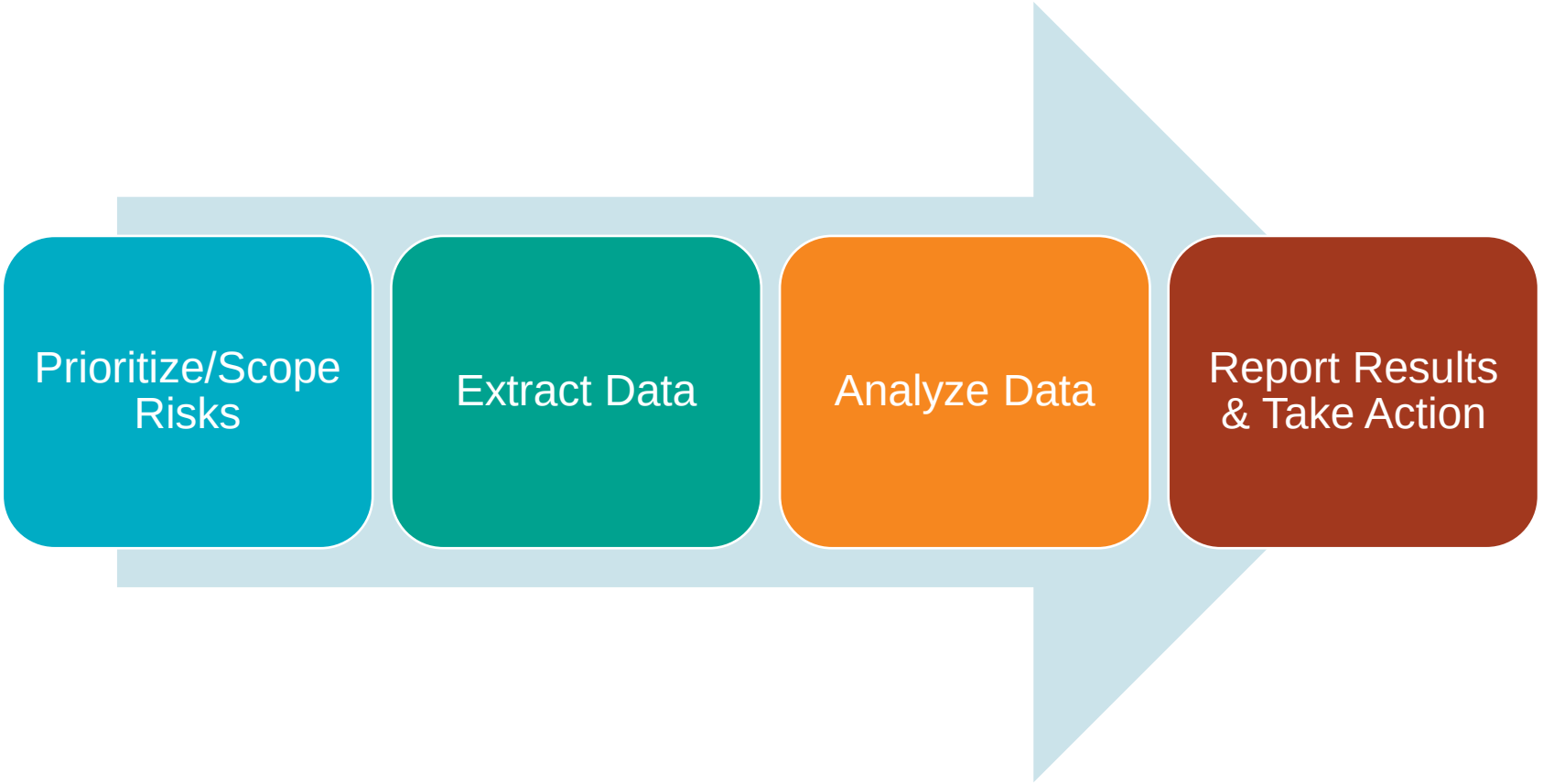
What is Happening Today? Am I Concerned?





protiviti

# MANUAL QUANTIFICATION APPROACH








protiviti

# SOD QUANTIFICATION RESULTS (EXCERPT)

| AC Risk | SoD Risk Description | Business Process | Potential SoD Violations reported in Access Control | | Individuals Executing Specific Transactions | | | Actual SoD Violations after Quantification Analysis | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | # Users | # Violations | # Users | Total # Transaction Occurrences | Total $ Value (US $) | # Users | Total # Transaction Occurrences | Total $ Value (US $) |
| **F001** | Create a fictitious GL account and generate Journal activity or hide activity via posting entries | General Ledger | 12 | 1,116 | N/A | 0 | N/A | 0 | 0 | $0 |
| **P001** | Maintain a fictitious vendor and enter a vendor invoice for automatic payment | Purchasing and Payables | 72 | 10,383 | 9 | 478 | $2,048,862 | 4 | 91 | $213,109 |
| | | | | | 6 | 354 | $646,230 | | | |

**What could happen** **What really happened**





protiviti

# MANUAL QUANTIFICATION CHALLENGES

## Manually Intensive

- Significant knowledge was required to understand details of security, business processes, SAP table structures, and organizational hierarchy
- A large team analyzed data over a 3-month period

## Extracting and Processing Large Volume of Data

- Tables' size reached 300 million line items
- Took days to extract all tables

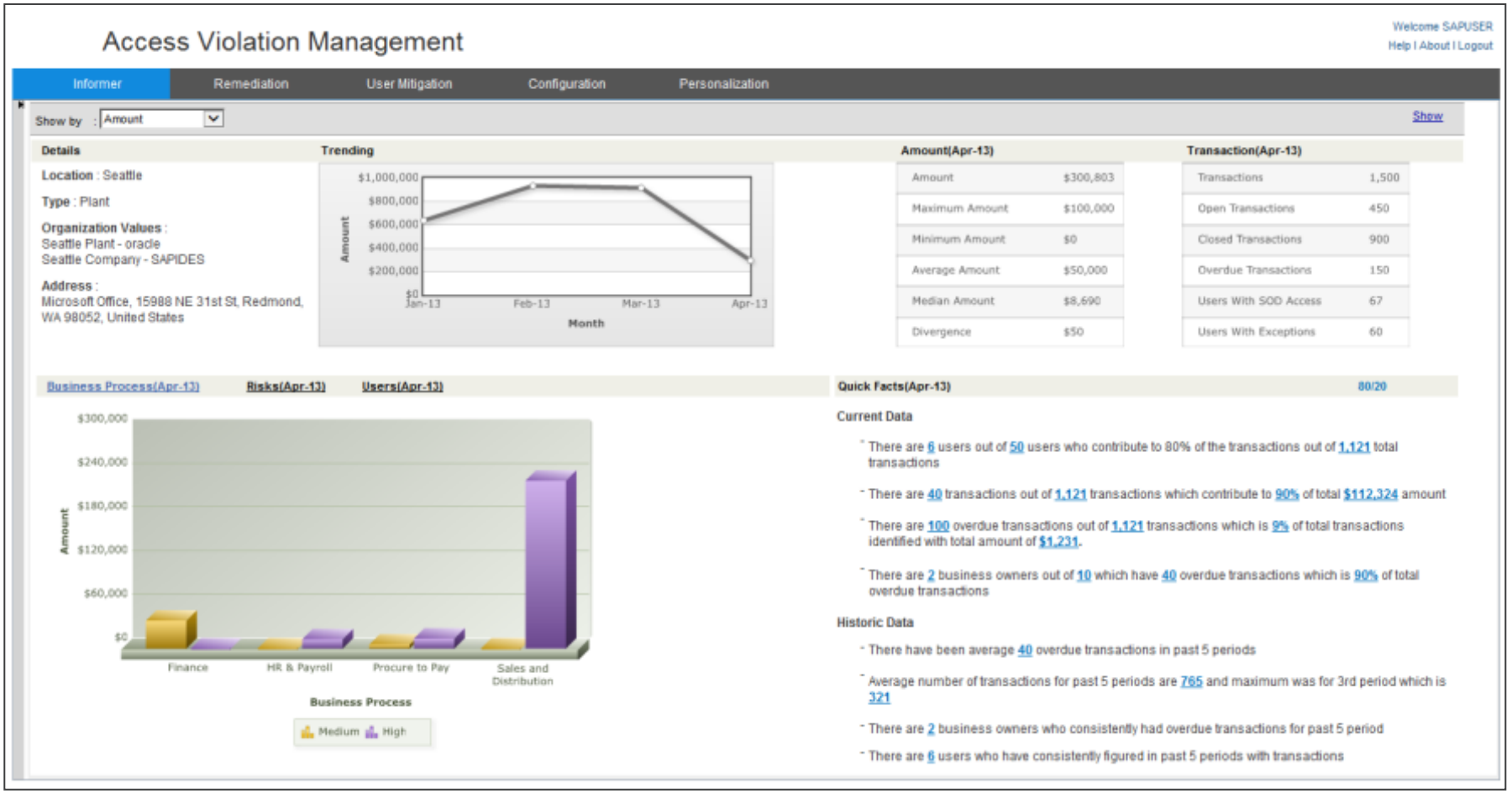
## Reliability of Results

- Timeliness of data could lead to less reliable conclusions (e.g., data could be months old)
- Manual processing of large volume and complexity of data can lead to errors

## Providing Meaningful Results

- SOD risk descriptions were vague and increased difficulty interpreting the actual transactions in the systems
- Mapping and scoping document types and transaction codes can be difficult and time consuming
- Currency conversion for multiple company codes

# NEXT STEP – AUTOMATED TOOL








protiviti

# NEXT STEP – AUTOMATED TOOL

**To:** Ben Jeffers
**Subject:** SOD Report: Mitigation risk exceptions requiring action

Dear Ben Jeffers,

Please check and confirm following mitigation risk exceptions assigned to you in Access Violation Management:

| Risk ID | Risk Description | User ID | User Name | System Name | Reported Date | Exception Count | Status |
|---|---|---|---|---|---|---|---|
| S528 | Create or Maintain Supplier & Process Supplier Invoices | AJITB | Allison Wiley | SAPIDES18 | 2014-15-03 | 3 | OPEN |
| S524 | Maintain Customer Master Records and Post Fraudulent Payments | SHARADS | Kendrick Woody | SAPIDES18 | 2014-15-03 | 2 | OPEN |
| **Total :** | | | | | | 5 | |

http://10.40.1.160:8085/LaserFocusApp/checkLogin.do

Regards,
AVM Automated Control Monitoring

This is an auto-generated Email. For any query regarding this, please get in touch with the SAP Team.

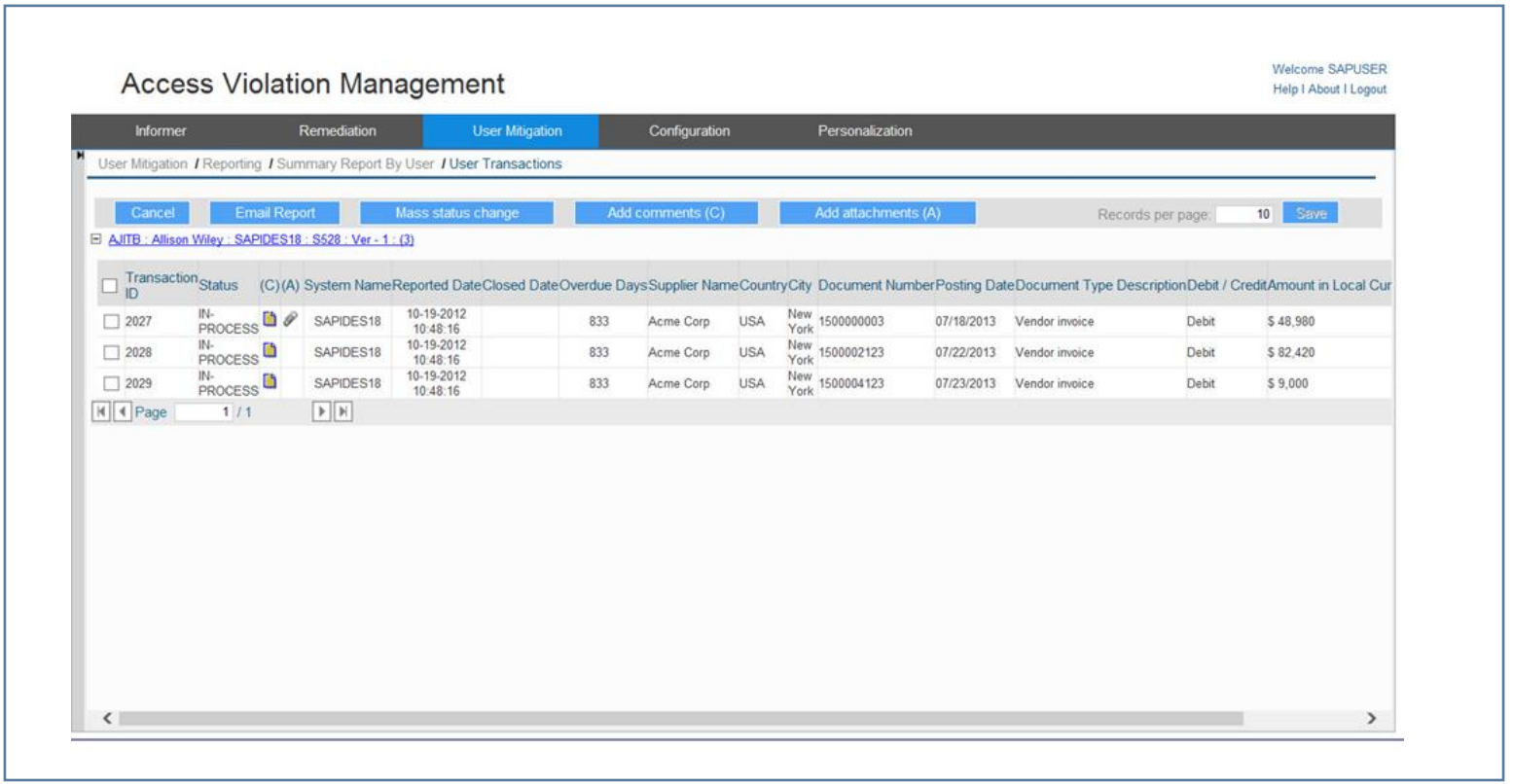






protiviti

# NEXT STEP – AUTOMATED TOOL








protiviti

# NEXT STEP – AUTOMATED TOOL

Potential SOD Exposure by Country






protiviti

# CASE STUDY #2

Bio-Medical Device Manufacturer

# PROJECT OVERVIEW

**Company**

- Bio-medical device manufacturer
- About $450MM in Revenues
- Utilizes Oracle eBusiness Suite (11i -> R12 version)

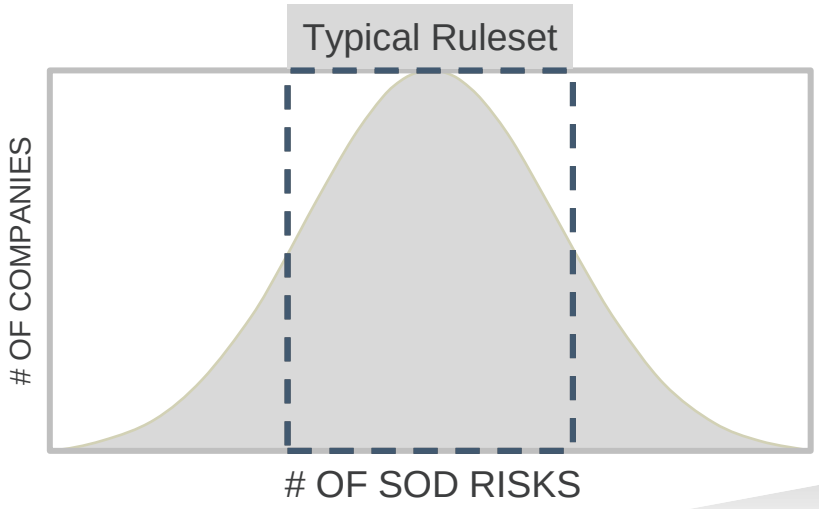
**Issue**

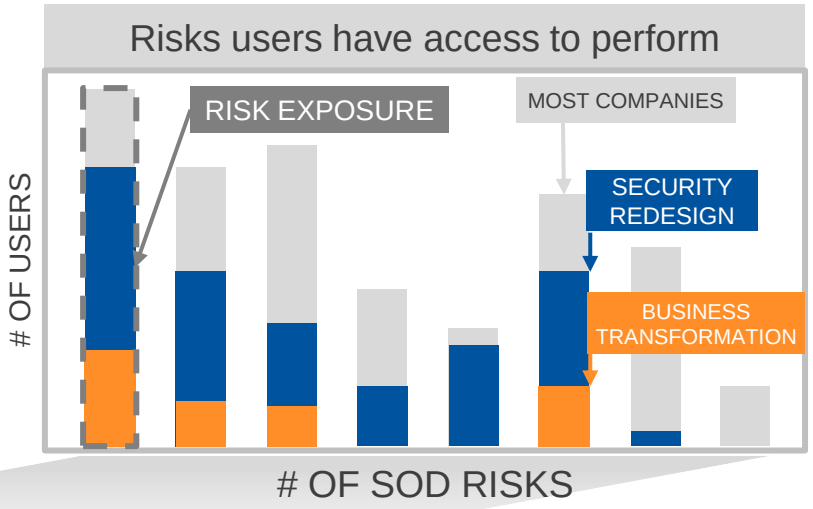
- An analyst accidently purged several critical tables in Oracle, raising alarm
- External audit also expressed concern as to lack of insight on SoD
- Many had access to shepherd transactions all the way through a cycle
- A significant deficiency was issued in the controls opinion

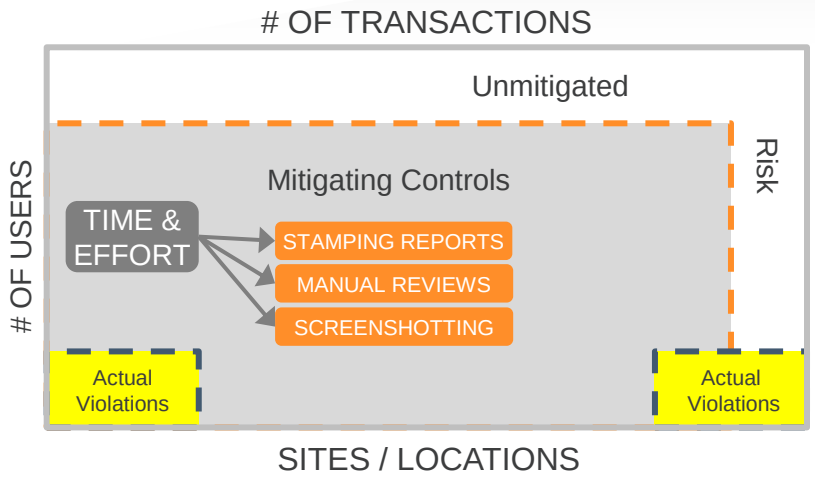
**Results**

- Forensics proved that very few actually used risky functions
- Business process / job duties / workflows were adjusted to insert SoDs
- The security model was to be overhauled for the new R12 environment

# THE GOAL: GET FROM 'POTENTIAL' TO 'ACTUAL' RISK




Only review the

- No m reports
- No m iolations

Actual Violations

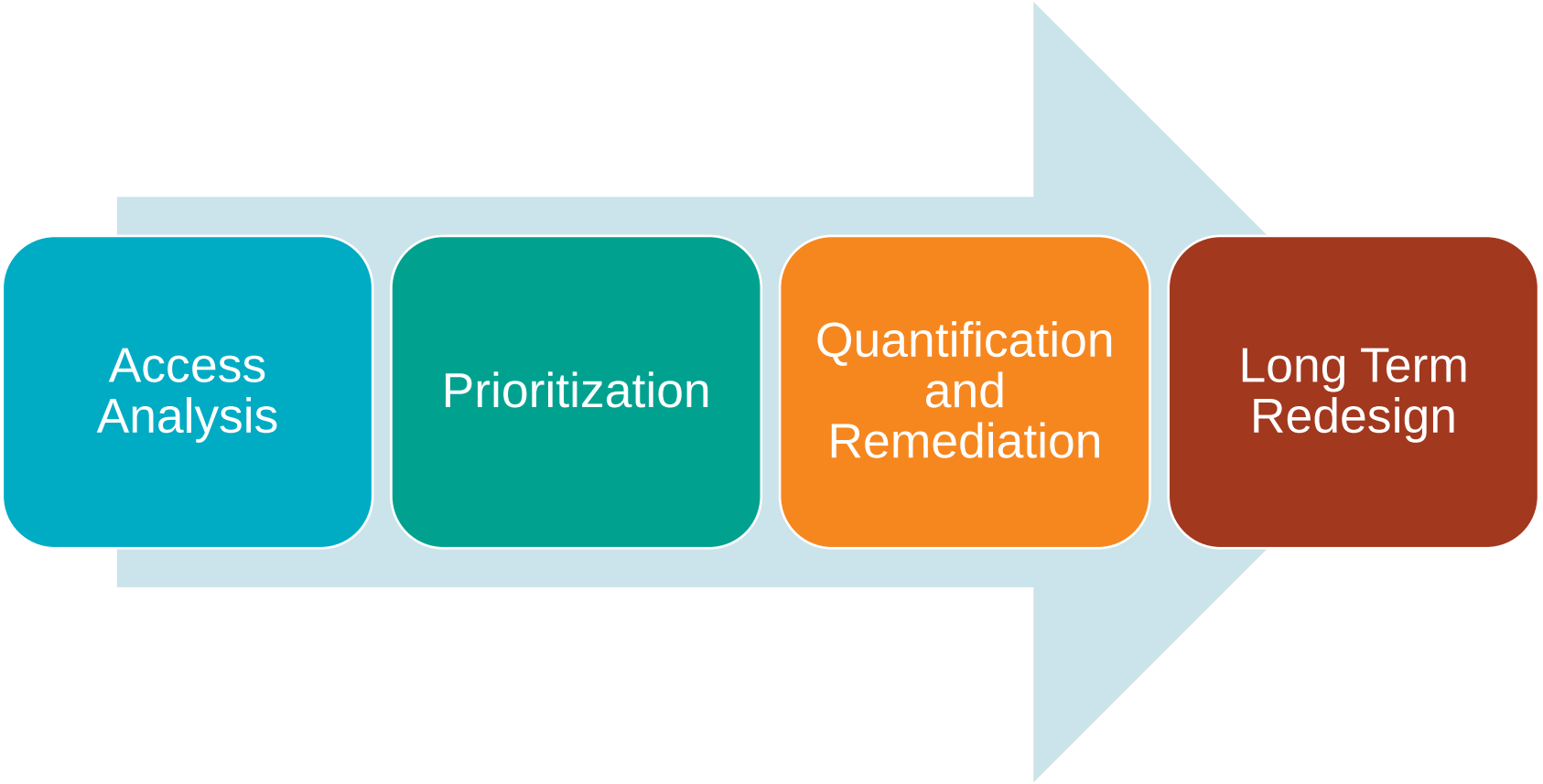
and investigate for misstatement or fraud





protiviti

# PROJECT APPROACH

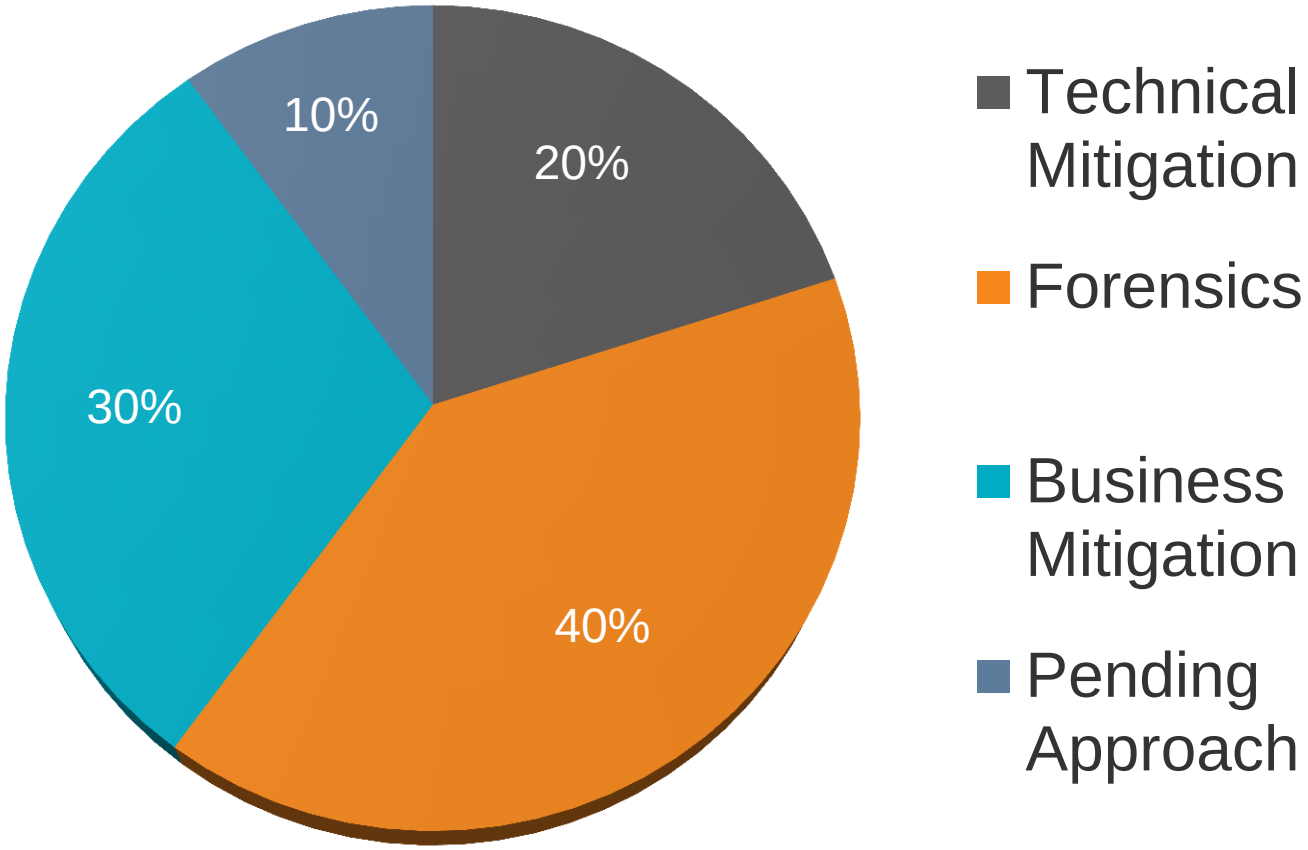







protiviti

# SOD RESPONSE APPROACH








protiviti

# CASE STUDY #3

Large Independent Oil & Gas Company

# PROJECT OVERVIEW

**Company**

- Large independent oil and gas company
- 17+ in-scope SOX systems

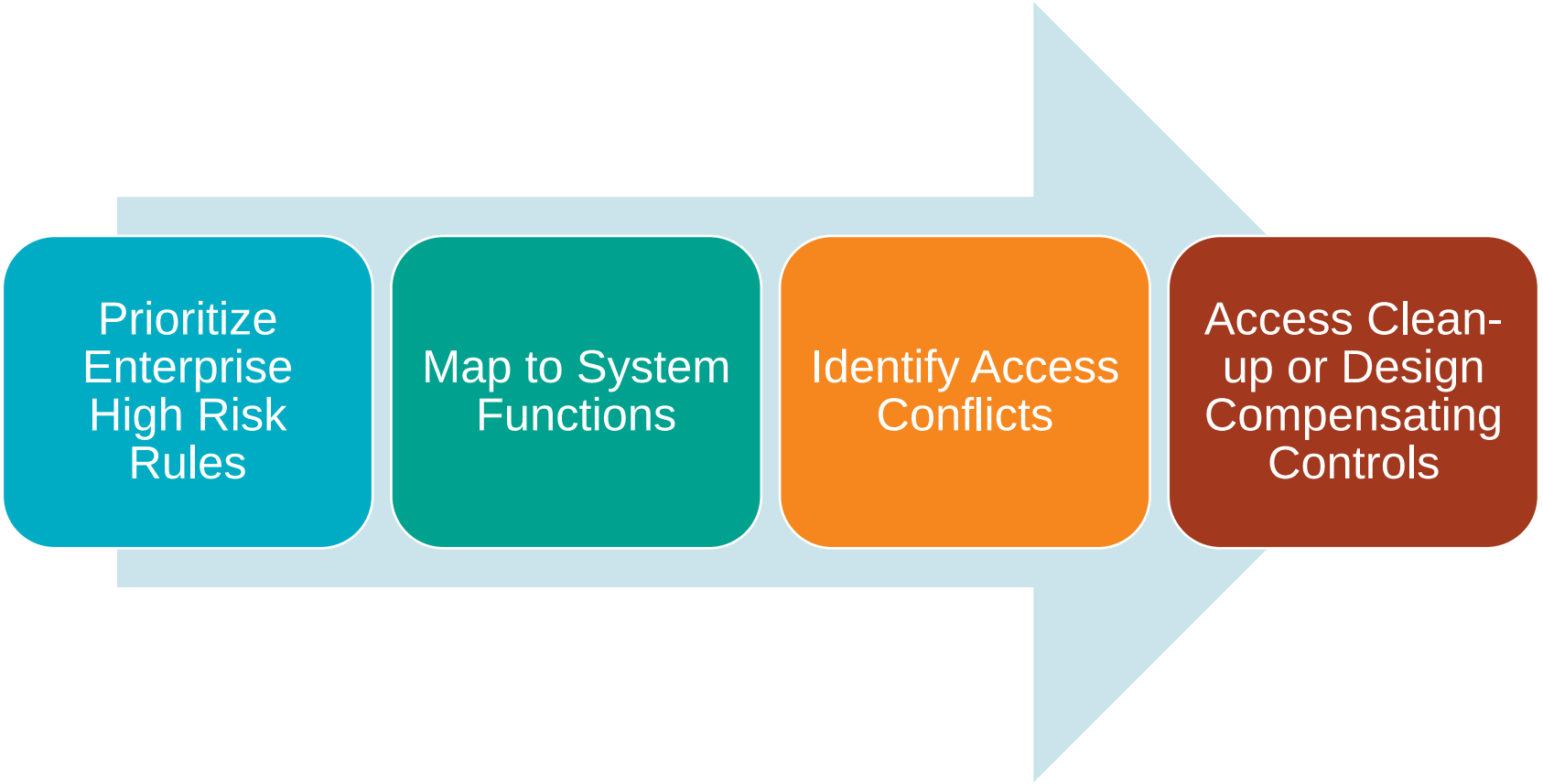
**Issue**

- External Audit forced a significant deficiency related to certain application access and SoD concerns
- Historically relied on business controls to compensate for SOD risks
- Many of the systems were custom built or difficult to query security

**Results**

- Process created to identify high risk conflicts, mitigating controls, and existing SOD conflicts within systems
- Reduced number of SOD violations in systems
- Added compensating controls to control environment to further mitigate risk

# PROJECT APPROACH





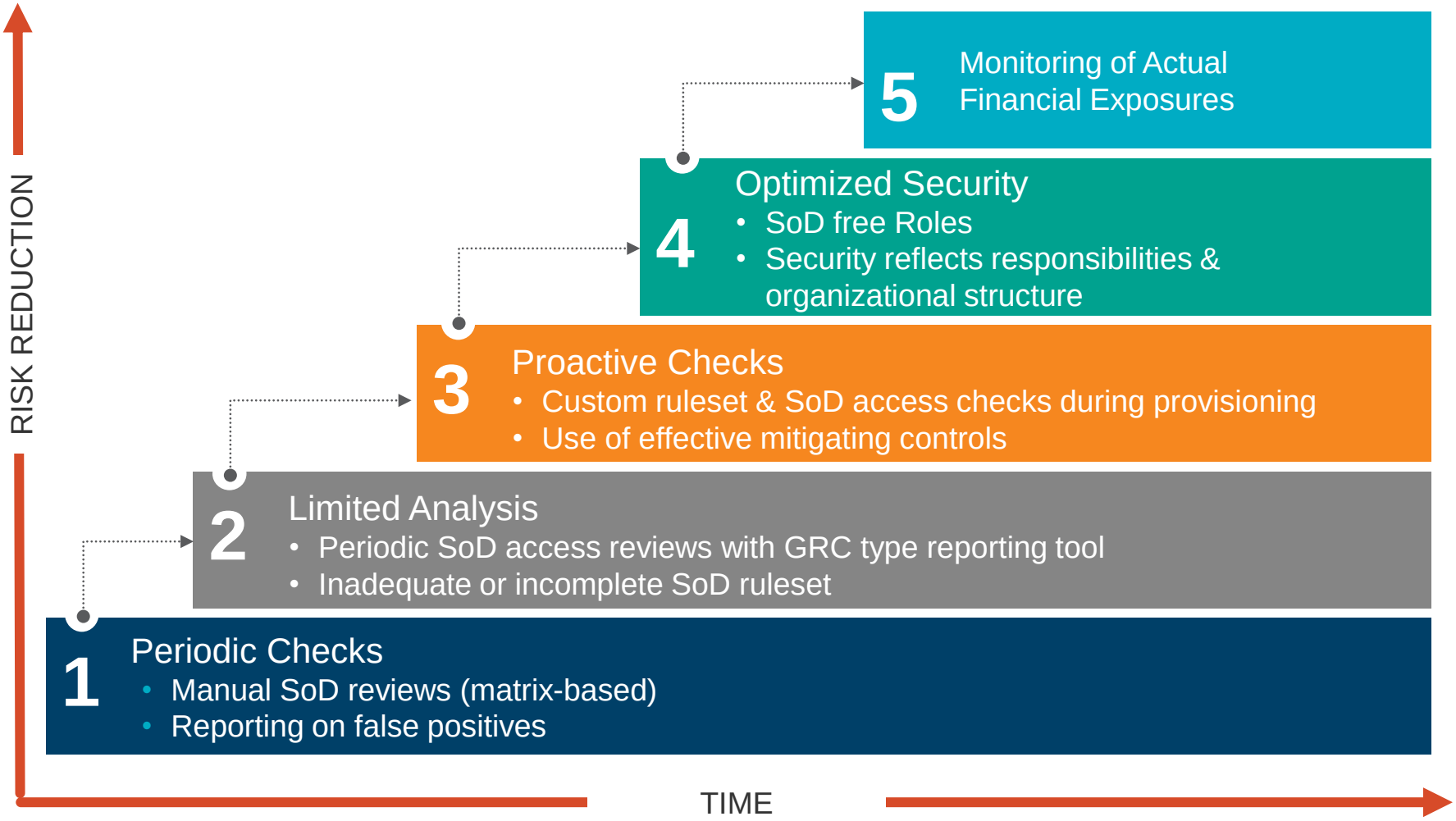



protiviti

# CASE SUCCESS FACTORS

- Risk prioritization was key
  - Impact
  - Likelihood
  - Inherent Mitigation
- Risk awareness by the business and IT was essential
- Mitigation / monitoring controls were only considered when:
  - A clear owner could be assigned to consistently action
  - The control would actually catch concerns
  - The control could be efficiently provable
- Clear goals, timeline, and accountability from IT, business, and IA/Compliance was needed to reach a clean baseline

# SOD RISK MANAGEMENT MATURITY – WHERE ARE YOU AND WHERE DO YOU WANT TO BE?








protiviti

# KEY TAKEAWAYS – BE **SMART**

| | |
|---|---|
| S | **S**crutiny is on the rise - Be proactive |
| M | **M**itigations must be able to truly catch abuse |
| A | **A**ccess should build up on least privilege principle |
| R | **R**eal **R**isk should drive remediation priorities |
| T | **T**echnology is key to sustainability |





protiviti

# QUESTIONS?


**Vijan Patel**

Associate Director

protiviti®

*Face the Future with Confidence*

Phone: 713.314.5120

vijan.patel@protiviti.com

Houston, Texas

***Powerful Insights. Proven Delivery.®***


## THANK YOU!

*Face the Future with Confidence*



protiviti®