ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Robotics for GRC

Meet Your New Tech Risk Manager

Nirma spearheads the Information Risk Management vertical at ANB. With more than 20 years of experience in Audits, IRM, Cyber Security and Consulting, she has lead teams in various engagements for large Banking & Financial Services companies, Telecom and other industries. She works with regulatory audits prescribed by RBI, NESA, MAS, etc.

She leads the Tech GRC automation vertical implementation for global clients and is actively involved in development of the 'Governance through Robotics' platform.

ARAC

Multi Locational

- Multi-locational servicing capability with offices in India, Dubai, London and Nairobi.
- Servicing clients in 25+ countries across SE Asia, Middle east and Africa.

Multi Industry expertise

- Telecom, Media and Technology
- Banking, Insurance and Financial Services
- IT and ITES
- Manufacturing, Pharma and others

Automation focused

- drut | Unified GRC automation platform enabling data collection, analytics and dashboarding
- Inherent OCR engine
- Low code BOT creator for connecting to different systems

Multi-skilled Team

- Multi skilled team comprising Chartered Accountants, Bankers, IT experts, MBAs, CISAs, Engineers, Lawyers, etc.
- Multilingual resources across various countries
- Resources with specific Industry/ domain expertise

UAE Internal Auditors Association
JOIN, LEARN & SHARE

enhanced expectations from the IA function

Internal auditing is an independent, objective assurance and consulting activity **designed to add value** and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The management now needs

- Enhanced assurance with 100% data validation
- Timely identification of red flags and newer risks
- Real time exception reports for timely action
- Frequent and effective reporting

How internal auditors are attempting to 'value add':

- Automated control monitoring
- Design adequacy review for transformational projects and digitization
- Identification of cost saving opportunities

AAAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Automation is Imperative

- Automation transforms legacy processes and drives digital transformation.
- RPA has been a main strategy for many business functions to drive efficiency at optimal costs including Governance, Risk, and Compliance (GRC).
- GRC is a diverse and inter-reliant function intended to manage regulatory requirements.
- RPA-based automation of GRC ensures efficiency and increase transparency and accountability.
- RPA-based GRC automation helps
  - assess assets,
  - manage policies,
  - proactively handles risks,
  - establish control mechanisms,
  - perform audits of all GRC activities.

Why Robotics for GRC?

Audit and Manage Risk Proactively

- Continuously risk assessments
- Monitoring the IT/IS operations

Effective Board Reporting

- Transparency to stakeholders
- Improved governance results

Incorporate Regulatory and Compliance issues

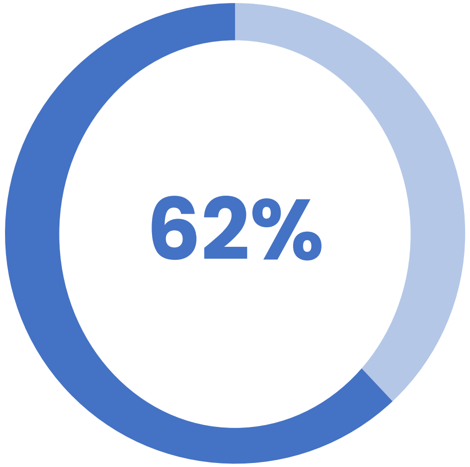
- Country / Industry specific security and privacy laws
- Compliance Frameworks

The average cost of compliance is $5.47 million versus an average of $14.82 million for noncompliance, which is an average difference of $9.35 million annually

Consistence Business Process

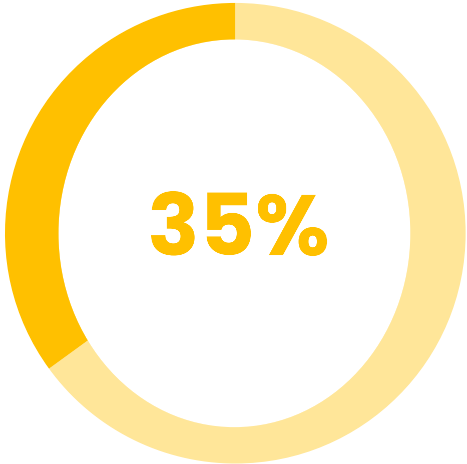
- Virtual execution across geographies
- Across functions, processes and applications

GRC Trends

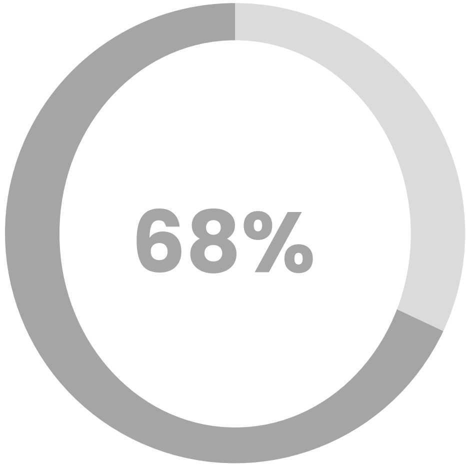


Organisation use software to monitors IT security controls

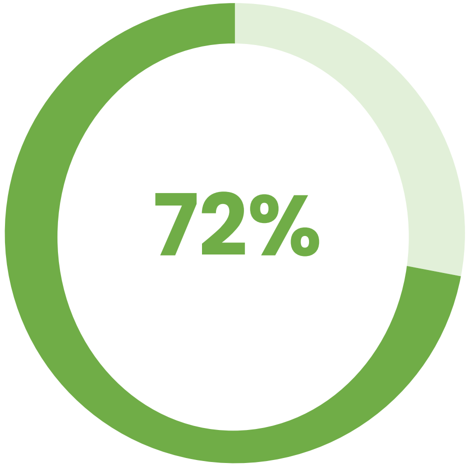
and reports on compliance posture



Organizations have evaluating software for risk and compliance monitoring in 2023



Organisation having integrated tools with both manual and automated processes did not experience a breach in 2022



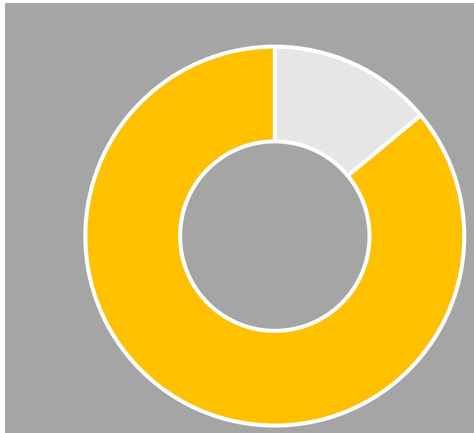
Organisation who had risk and compliance activities integrated together did not experience a breach

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

GRC Objectives Achieved

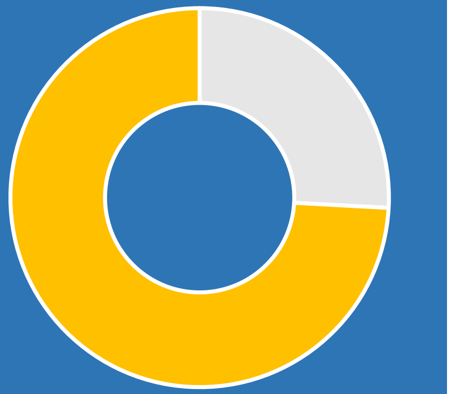
86 % Improved Productivity



More than 70% organization reported RPA opportunities in most business functions particularly technology

59 % Reduction in Cost

98 % Improvement in Compliance



AAAC

UAE Internal Auditors Association

JOIN, LEARN & SHARE

Challenges

data collection

- Manual and error prone extraction
- Time consuming for repeated follow ups
- Data integrity/ completeness issues

data analytics

- High manual involvement
- User expertise required for query building
- Single functionality querying capability

reporting

- High manual involvement
- Time consuming
- User dependent for every audit

Average time spent each week on Duplication of Task

USA
4 hr 55 mins

UK & Germany
5 hrs 58

Middle East
4 hr 48 mins

Japan
2 hr 56 mins

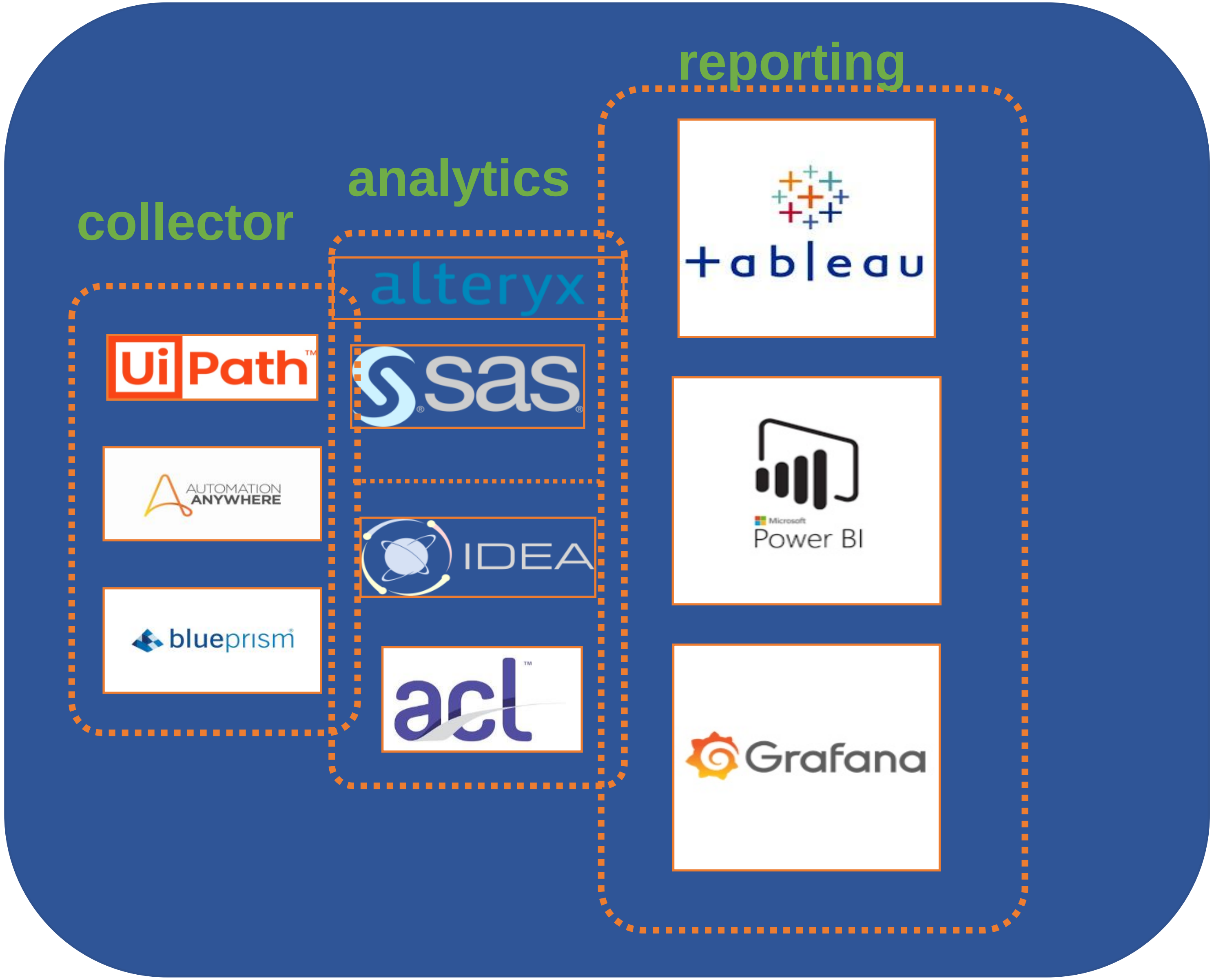
Australia and New Zealand
5 hr 87 mins

85 % of risk and compliance management team spends at least **1/3 or more of their time at work on repetitive tasks.**

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Single Stream – Integrated Platform



Unified Approach

data collection

- Customized system connectors for auto-extraction of standard reports
- Back-end generated data imported from shared path
- Connectors for all prominent systems
- One-time rule creation for data extraction

automated analytics

- One-time configuration of data processing rules and sequence
- Data processing rules can be set up through low code front-end query builder
- Complex data processing scenarios can be set up using Python, SQL etc.

reporting

- Auto-mailers of exceptions to stakeholders
- Updating exceptions in relevant application / BI
- Auto-generation of MIS for exceptions

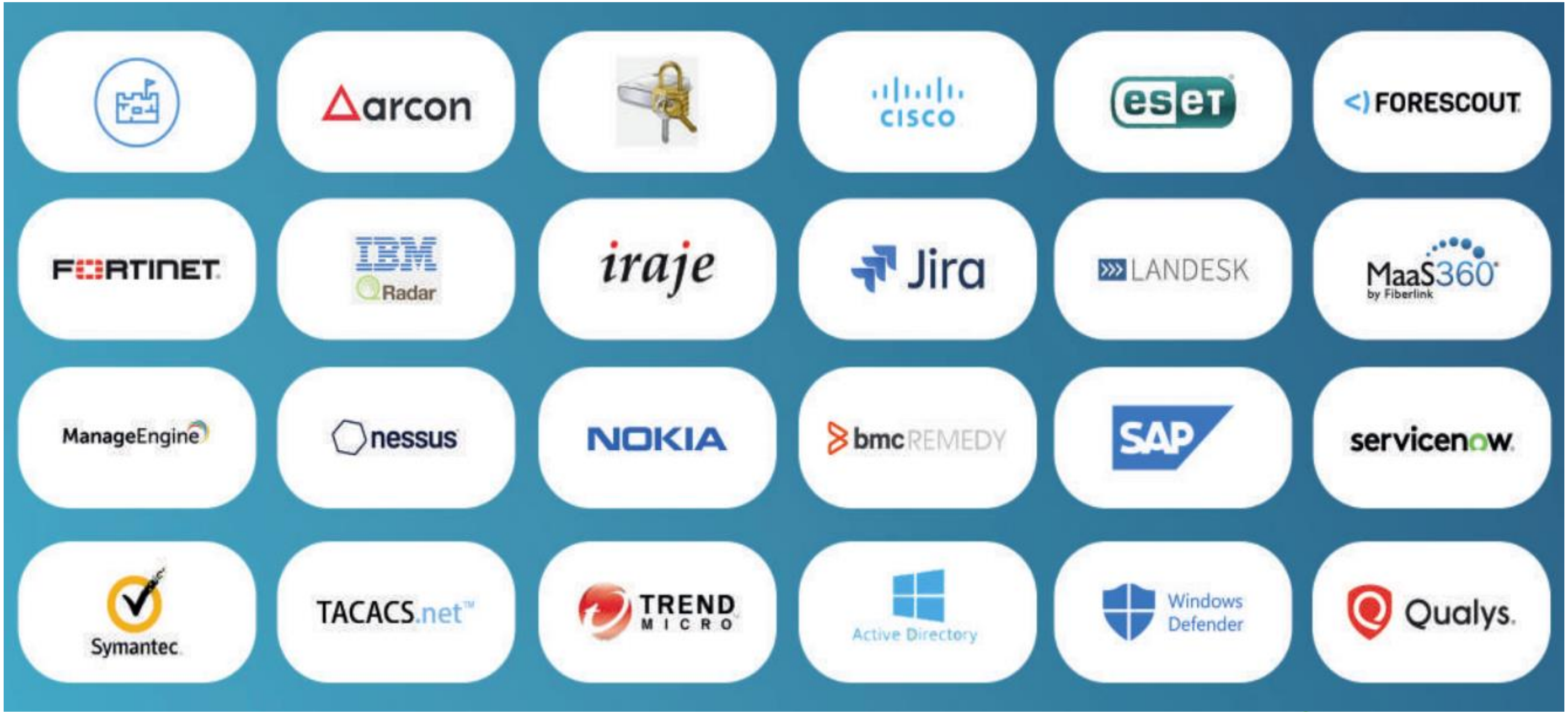
case management

- Exceptions validated and approved by the activity owner
- Approvals by process owner and auditor / reviewer
- Tracking of exceptions, closure timelines, and evidences through ‘open issue’ tracker

typical features

- Integrated system offering automated data collection, data processing and visualisation including Risk libraries
- Minimal coding required for BOT building for data collection and rule building for data processing
- Multiple dashboarding capabilities for visualisation of output

Deep Integrations



Deep Integrations – Controls Validated

DOMAIN	RCM	AUTOMATED CONTROLS	Drut. Works With
Access Management	16	11	Windows Active Directory
Antivirus Controls	14	14	Trend Micro, Symantec, Windows Defender, ESET
Asset Management	16	5	Manage Engine
Change Management Controls	27	11	Jira, Remedy, Manage Engine, Service Now
Endpoint Security	12	6	Bit Locker
Firewall Rule Review	10	8	Fortigate, Cisco, Nokia
Incident Management	14	6	Jira, Remedy, Manage Engine
Network Management	9	3	Forescout, TACACS
Mobile Device management	14	3	MAS 360
Patch Management	6	5	Landesk
Privileged User ID Management	21	5	ARCOS, IRAJE
SIEM Logging & Monitoring	4	2	AISAAC, IBM Qradar
Vulnerability Management	6	3	Nessus

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

Continuous Compliance Monitoring

- Companies are shifting their attention to improve their security postures by using various frameworks clearly the current security compliance posture
- Managing multiple frameworks is time-consuming, repetitive tasks
- Automation of GRC Technology allows management of multiple frameworks to be more streamlined and simplified,

PCI DSS COMPLIANT
GDPR
Saudi Arabian Monetary Authority
NIST National Institute of Standards and Technology
AICPA SOC 2
ISO
AICPA SOC 3
MAS

Tech Risk |Mapped to Compliances

Area	Controls	ISO 27001	NESA	ADHICS	PCI DSS
Access Control /Active Directory	Review of terminated/resigned users, active in the system	A.5.15	M 4.4.3	AC2.1	8.2.5
	Delay in disabling terminated / resigned users	A.5.16	T5.2.1	HR 4.1	8.2.5
	User Accounts with password never expires	A.5.17	T5.5.3		8.3.9
	Deviation in password change date from the policy	A.5.17	T5.5.3		8.3.9
	Rename Default Administration Account	A.8.9	T5.2.2		2.2.2
	Review of dormant accounts	A.5.16	T5.2.1	AC4.1	8.2.6
	User account configured without password	A.5.17	T5.5.3		8.3.9
Antivirus	Antivirus Installed on all systems	A.8.7	T3.4.1	OM4.1.2	
	Antvirus Updated on all systems	A.8.7	T3.4.1	OM4.1.3	5.3.1
	Antivirus Scan last run all systems/ deviation from policy	A.8.7	T3.4.1	OM 4.1.5	5.3.2
Patch Management	Patch Management solution installed on all system	A.8.8	T7.7.1	OM 6.5.1	6.3.3
	Patch Update on all system	A.8.8	T7.7.1	OM 6.5.3	6.3.2
Endpoint	Disk Encryption on all Laptops	A.8.1	T5.7.1		
	Network Access Control Solution Integration	A.8.1	T 5.4.3	CM 5.1.5	1.3
Incident Management	Each Incident is classified and has priority assigned	A.5.24	T8.2.3	IM 2.3	
	Each Closed Incident has an RCA	A.5.24	T8.2.2		
	Incident Escalation is done has be escalation matrix	A. 5.24	T8.2.1		
	Incident SLA/ TAT has maintained	A. 5.24	T8.2.1	3.11.2	12.10.1
SIEM /SOC	Intergration of all systems wih SIEM	A.8.15	T3.6.3	OM6.2	10.2.1
	System intergrated with SIEM but not sending logs	A.8.15	T3.6.3		

case study 1 | automation of firewall rules review

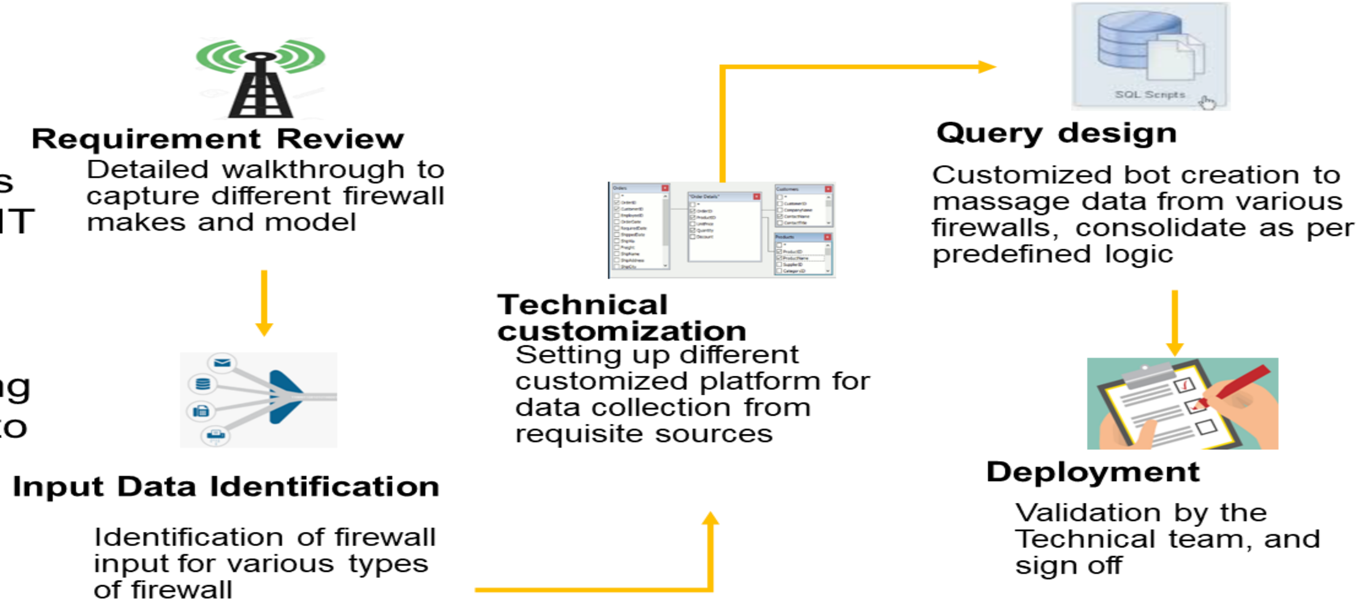
200 + Firewalls
10 controls each

0.2 Million + Firewall Rules Validated

1000+ man days saved annually

THE PROBLEM

- Different makes and models of IT and Telecom Firewalls
- Time consuming validation due to huge data size



Requirement Review
Detailed walkthrough to capture different firewall makes and model

Input Data Identification
Identification of firewall input for various types of firewall

Technical customization
Setting up different customized platform for data collection from requisite sources

Query design
Customized bot creation to massage data from various firewalls, consolidate as per predefined logic

Deployment
Validation by the Technical team, and sign off

THE SOLUTION

- 100% firewalls covered as opposed to 10- 20 sample firewall reviewed previously by client
- Entire implementation completed in three weeks and
- 3-4 mins per controls
- Limited manual intervention and accurate reporting

AAAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE

case study 2 | automation of security controls validation

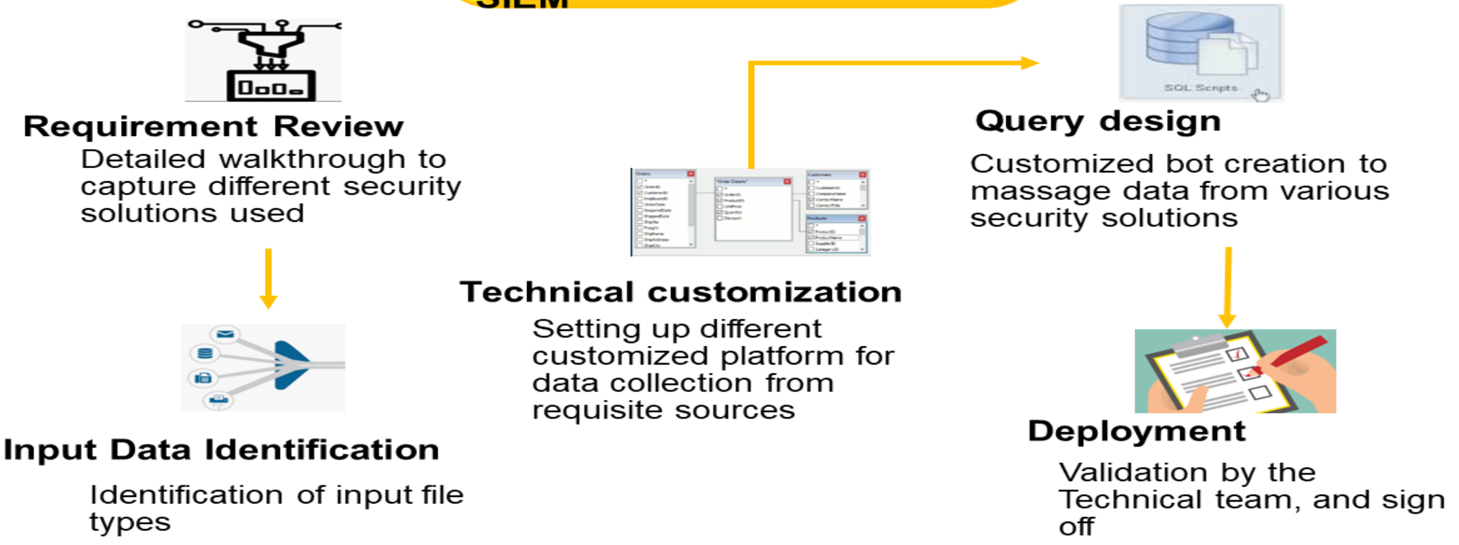
10+ Security Domains →

Patch Management
Access Controls
Antivirus
Endpoint Security
Incident Management
Network Access Controls
SIEM

→ **30+ Controls Validated**

THE PROBLEM

- Usage of various security solutions
- IT Control Testing within limited period of time
- IT Testing with Data Analytics was a challenge in the past



Requirement Review
Detailed walkthrough to capture different security solutions used

Input Data Identification
Identification of input file types

Technical customization
Setting up different customized platform for data collection from requisite sources

Query design
Customized bot creation to massage data from various security solutions

Deployment
Validation by the Technical team, and sign off

THE SOLUTION

- 100% coverage as opposed to 10- 20% sampling done in the past by client
- Overall Dashboard along with Domain wise view for Management
- Compliance status mapped to international and local regulations

ARAC

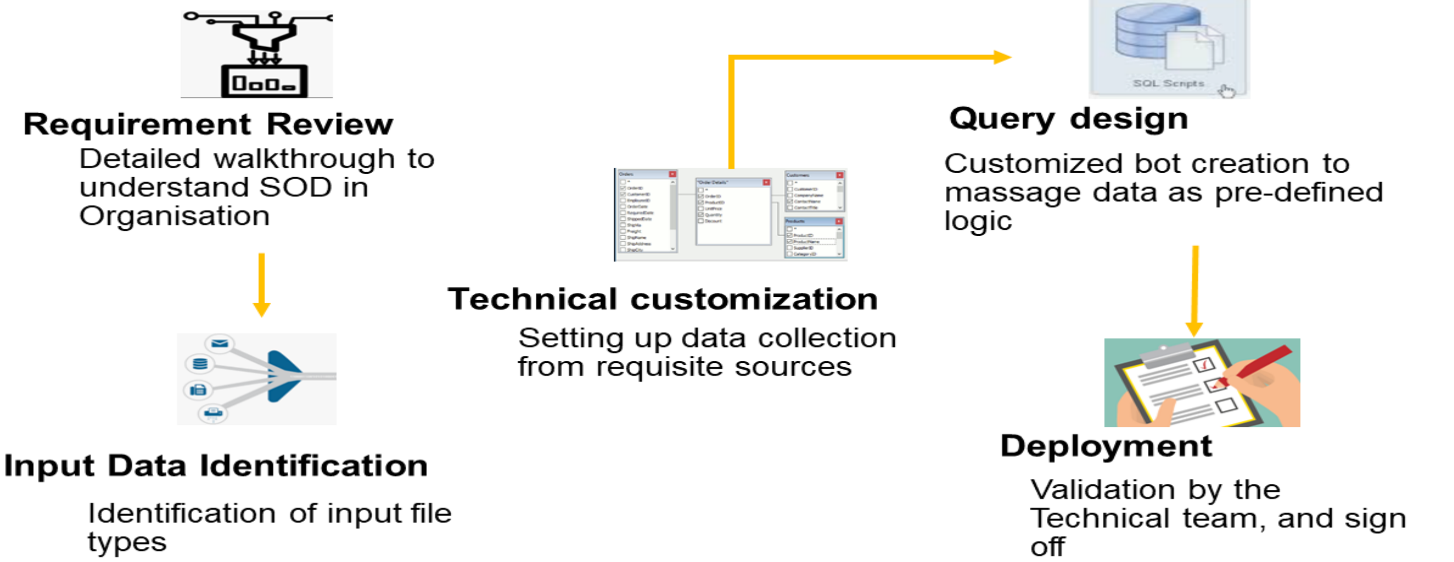
UAE Internal Auditors Association
JOIN, LEARN & SHARE

case study 3 | automation of SAP access & SOD controls

1500+ Users → **70 + Functions**
500+ Roles
200+ Custom T Codes → **152+ SOD Controls Validated**
50+ Exception

THE PROBLEM

- Complex Environment
- Time consuming validation due to huge data size
- Validation of SOD was a challenge in the past



Requirement Review
Detailed walkthrough to understand SOD in Organisation

Input Data Identification
Identification of input file types

Technical customization
Setting up data collection from requisite sources

Query design
Customized bot creation to massage data as pre-defined logic

Deployment
Validation by the Technical team, and sign off

THE SOLUTION

- 100% coverage as opposed to review of only sample critical SOD cases
- Identified policy violations, access to sensitive information

GRC Automation | what does it simply do

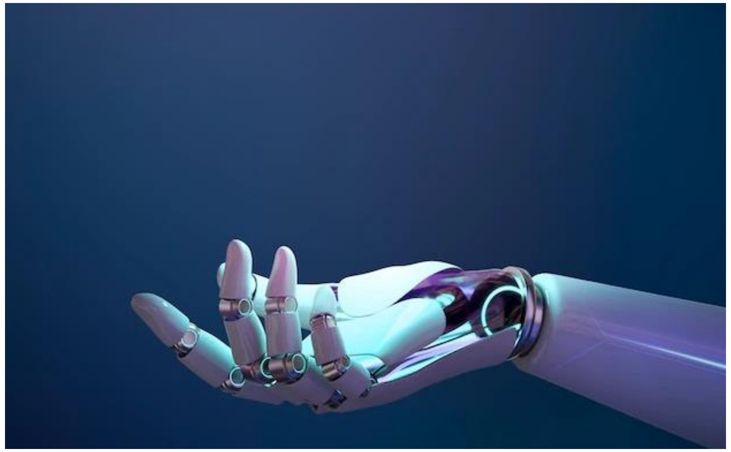
- Ensuring comprehensiveness of controls being monitored
- Factoring in any new and emerging risk scenarios
- Determining frequency of control monitoring as per evolving risks
- Sample testing of configuration accuracy on the automation platforms
- Auditing adequacy of action taken on the risk flags identified
- Continued focus on non-automatable controls

Establishment of RPA as a Centre of Excellence (CoE)

- 57% of organizations are expect to spend more time on risk compliance management.
- 63% of organisation are expect to spend more money on IT compliance and risk management
- 20% of companies will have more than 95% visibility of all their assets, which will be prioritized by risk and control coverage by implementing cyber asset attack surface management
- Popularity of RPA as a Service Model (RPAaaS)
- Marketplace in RPA for new technology and cyber risk
- Hyper-automated RPA tools

Connect with us

Nirma Varma
Director
Technology Risk& Cyber Security
Nirma.Varma@drut.com



drut.

Follow us on
www.drut.com
@drut.bot

Meet us @ Booth no 7

ARAC

UAE Internal Auditors Association
JOIN, LEARN & SHARE