SECONIZE

Compliance Audit Automation

https://seconize.co/compliance-management/

Challenges in Internal Audit

1. CISOs must go thorough their compliance with cybersecurity frameworks

2. Companies need to re-align frameworks with business strategies and risk profiles

3. Adaptation to robust cybersecurity is needed to enable business growth

Seconize – DeRisk Center   Cloud Oriented | Automated | Holistic | *Continuous* | *Contextual*

Impact Based

Near Real Time

Unified

Automated

Security Compliance Management with data driven approach
- Automated Evidence Collection
- Analysis of the evidence collected

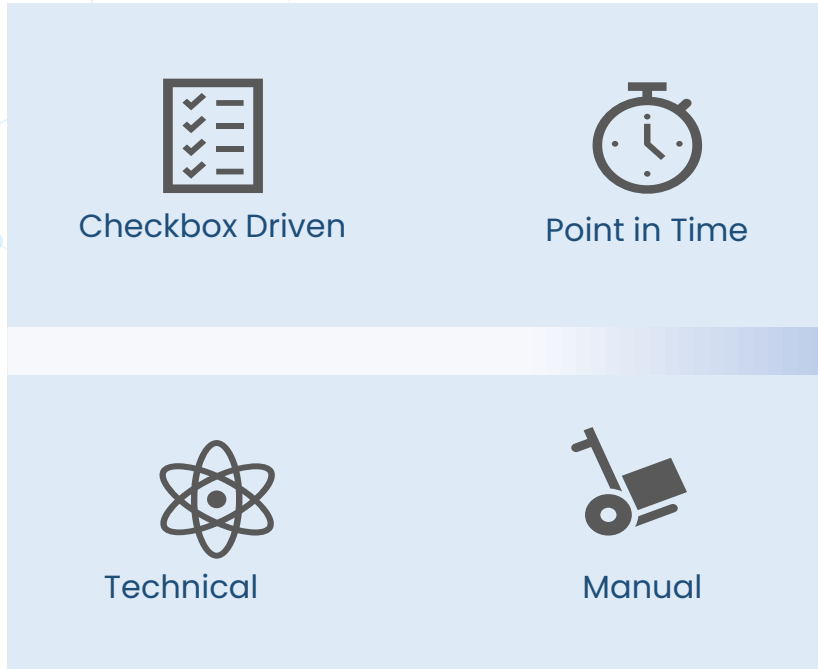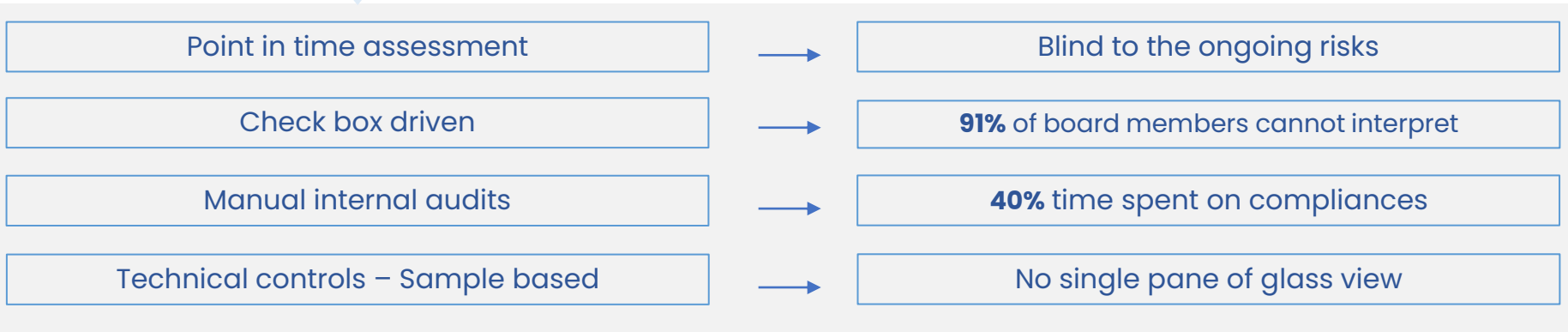**Traditional Compliance Management**   Manual   Time & Effort   Tedious   Regulatory Frameworks

Compliance Management

Traditional Management

Seconize – DeRisk Center

Checkbox Driven Point in Time

Impact Based Near real time

Technical Manual

Risk based Automated

Point in time assessment	→	Blind to the ongoing risks
Check box driven	→	**91%** of board members cannot interpret
Manual internal audits	→	**40%** time spent on compliances
Technical controls – Sample based	→	No single pane of glass view

to reduce risk

- CISOs must go well beyond annual compliance audit and ascertain compliance risk on a continuous basis

- Automate the compliance management
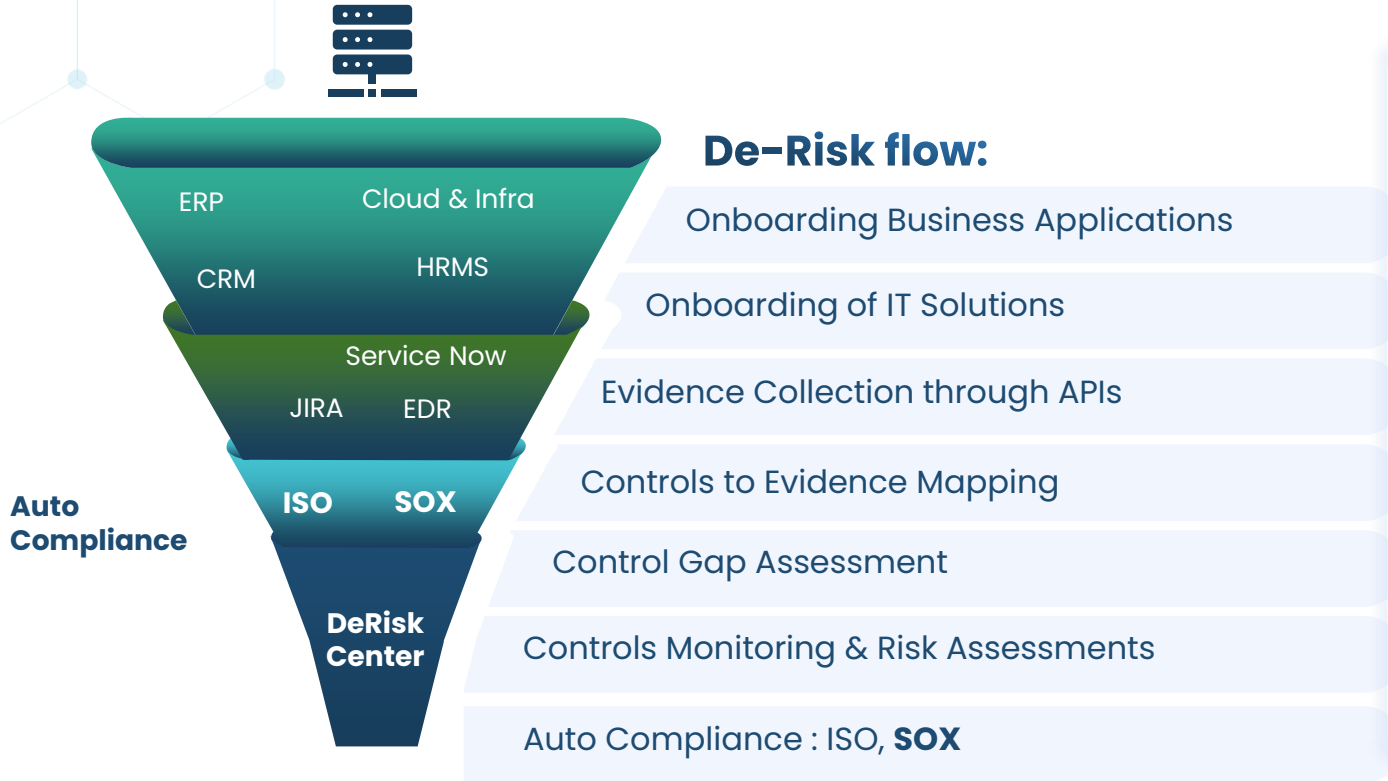
- Business Enabler

Current Challenges

➢ Standards such ITGC–SOX , SOC2, ISO 27001:2013 are intensive efforts

➢ Regulatory bodies like **GDPR, CCPA, SEBI, RBI, IRDAI, NBFC** are mandating

    ➢ Increase in compliance requirements
    ➢ Comprehensive & Overlapping Controls
    ➢ Tedious Manual Evidence Collection Processes
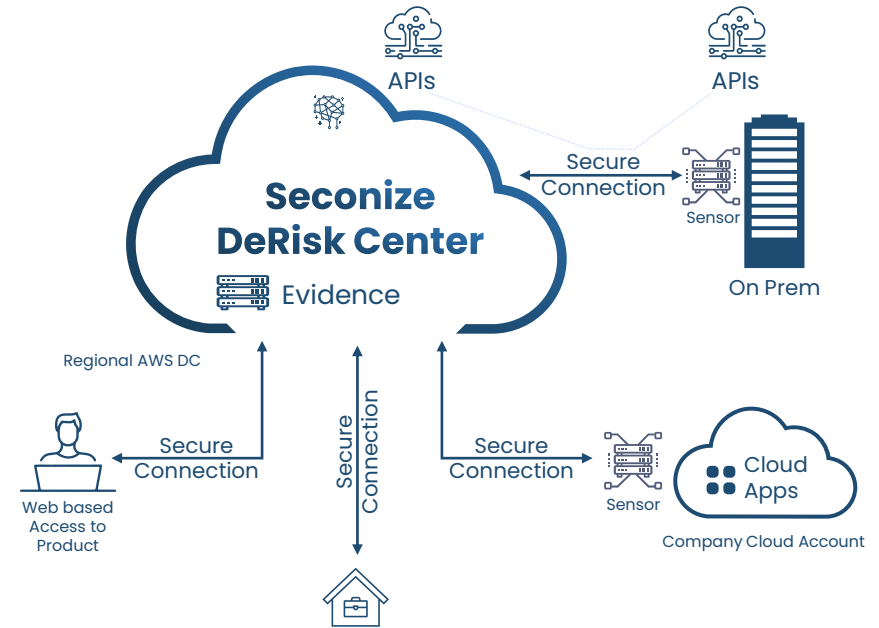   ➢ Frequent assessments vs earlier annual assessments

Goals

➢ Meet the compliance without laborious manual efforts

➢ Have an overall visibility at organization level to manage Compliance

➢ Automate the overall Controls and Cyber compliance requirements, by collecting evidence.

Seconize DeRisk Center

Assessments are based on industry-wide standards like
ISO 27001-2013, SOX, NIST CSF , PCI DSS , CCM

De-Risk flow:

Auto Compliance

Funnel labels: ERP, Cloud & Infra, CRM, HRMS, Service Now, JIRA, EDR, ISO, SOX, DeRisk Center

- Onboarding Business Applications
- Onboarding of IT Solutions
- Evidence Collection through APIs
- Controls to Evidence Mapping
- Control Gap Assessment
- Controls Monitoring & Risk Assessments
- Auto Compliance : ISO, **SOX**

Serving Across On-Prem, Cloud,

APIs   APIs

Seconize DeRisk Center   Evidence

Secure Connection   Sensor   On Prem

Regional AWS DC

Web based Access to Product   Secure Connection   Secure Connection   Secure Connection   Sensor   Cloud Apps

Company Cloud Account

Compliance gap assessment; Automated technology gaps; Workflows for manual inputs; Internal audit report

Salient Points: Deployed in customer region, Security and privacy, Best practices, Hybrid deployment, Cloud Management, Sensors on premises

SEC●NIZE   Confidential

Compliance Management

- Automate Compliance Gap Assessments to Drive Security
- Compliance is about defining, measuring, and mitigating risk
- Periodically assess networks for compliance with internal and regulatory security controls
- Audits reduce risks by identifying gaps between the desired state of configurations and processes and those that exist in the infrastructure

Automated Compliance Gap Assessment

- Generic Compliance Framework
- Automate technology gap assessment
- Workflows for manual inputs
- Internal audit report
- Data Driven
- View multiple compliance at the same time
- Maintain Continuous Visibility Over Compliance

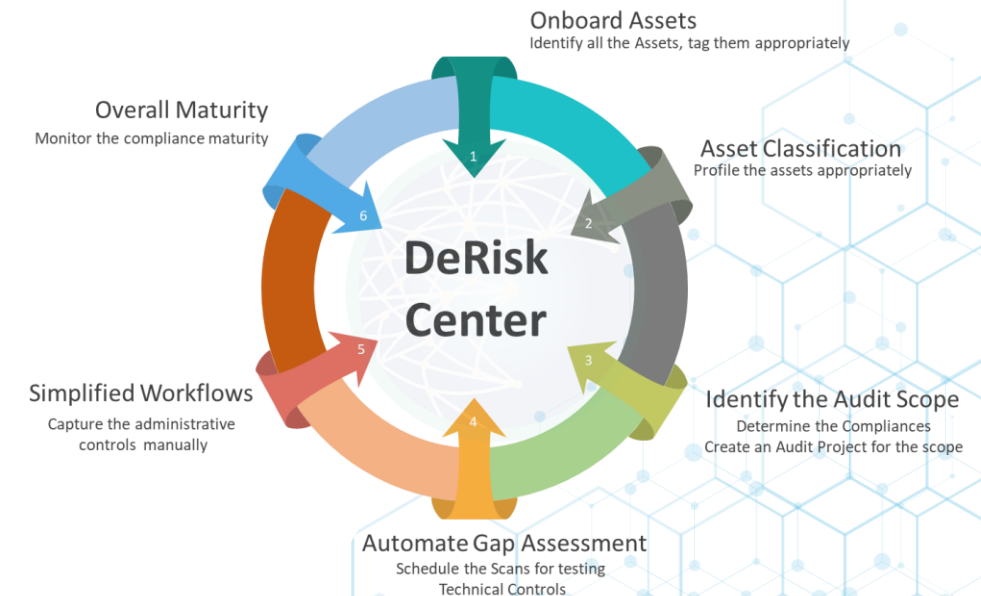### Automated Controls Assessment

- Out of box testing of Technical Controls
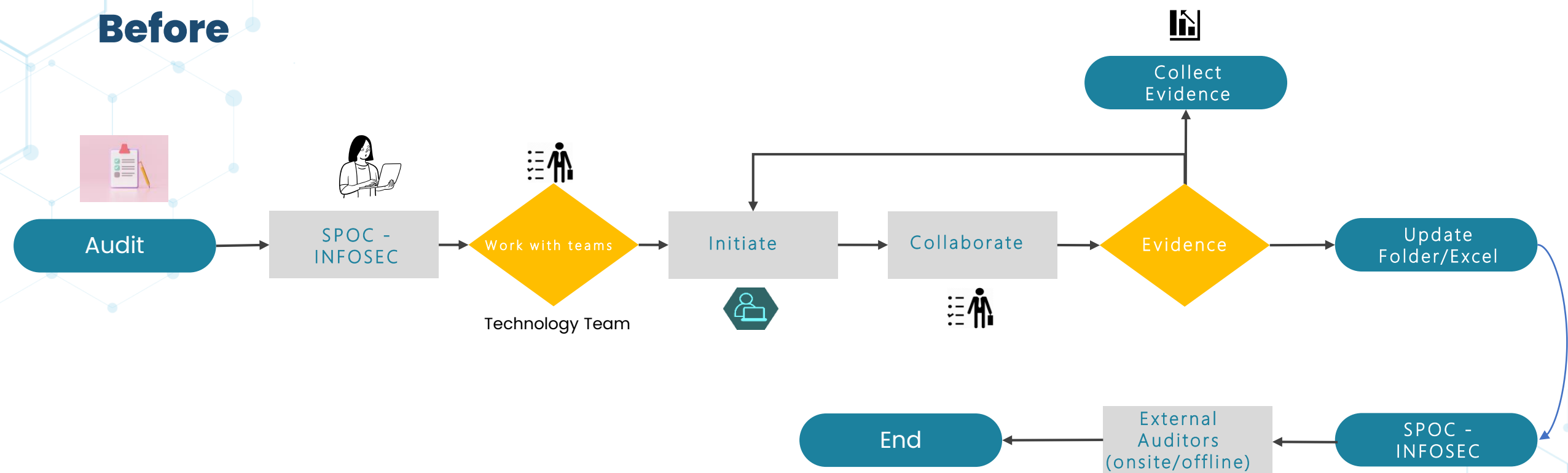- Flexible framework for custom plugins

Automated Mapping

- Maps to numerous regional and global standards and regulations
- ISO 27001:2013, GDPR, PCI DSS , NIST, RBI framework, IT GC SOX
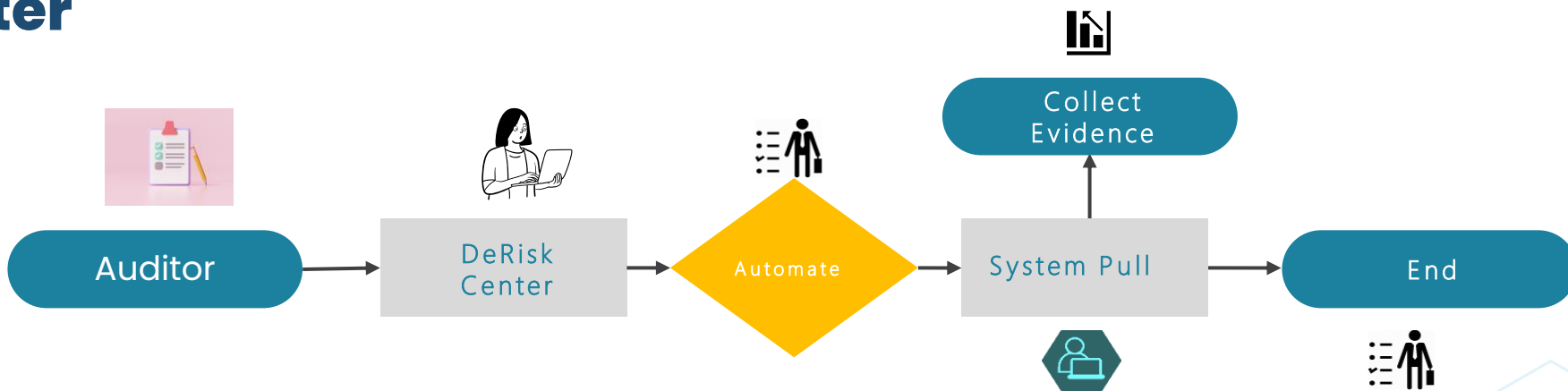
Simplified Workflows

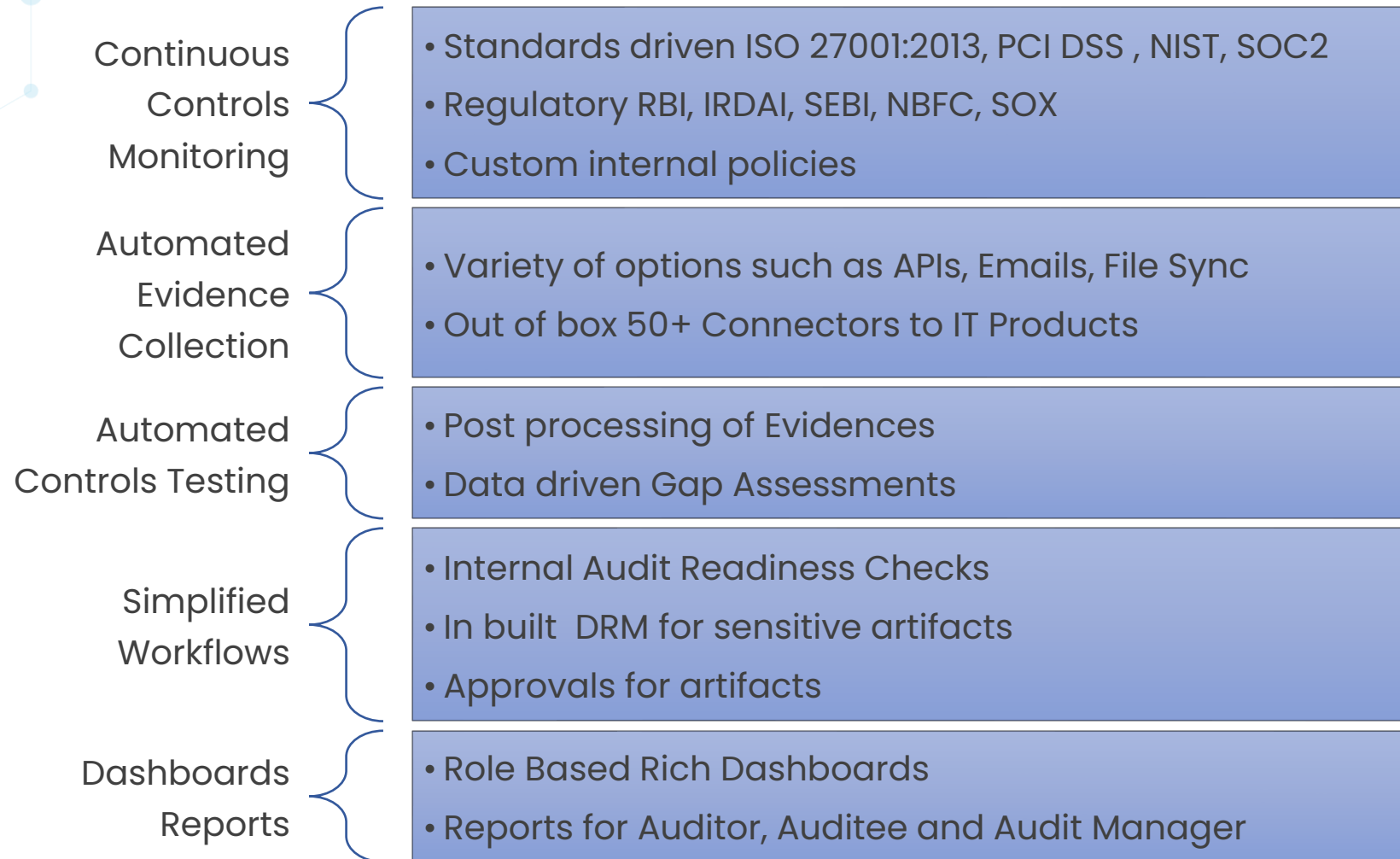- For capturing administrative Controls

Onboard Assets
Identify all the Assets, tag them appropriately

Asset Classification
Profile the assets appropriately

Identify the Audit Scope
Determine the Compliances
Create an Audit Project for the scope

Automate Gap Assessment
Schedule the Scans for testing Technical Controls

Simplified Workflows
Capture the administrative controls manually

Overall Maturity
Monitor the compliance maturity

DeRisk Center

Before

Audit → SPOC - INFOSEC → Work with teams (Technology Team) → Initiate → Collaborate → Evidence → Update Folder/Excel

Collect Evidence

SPOC - INFOSEC → External Auditors (onsite/offline) → End

After

Auditor → DeRisk Center → Automate → System Pull → End

Collect Evidence

Compliance Management

Continuous Controls Monitoring
- Standards driven ISO 27001:2013, PCI DSS , NIST, SOC2
- Regulatory RBI, IRDAI, SEBI, NBFC, SOX
- Custom internal policies

Automated Evidence Collection
- Variety of options such as APIs, Emails, File Sync
- Out of box 50+ Connectors to IT Products

Automated Controls Testing
- Post processing of Evidences
- Data driven Gap Assessments

Simplified Workflows
- Internal Audit Readiness Checks
- In built DRM for sensitive artifacts
- Approvals for artifacts

Dashboards Reports
- Role Based Rich Dashboards
- Reports for Auditor, Auditee and Audit Manager

BEFORE

- Evidences are collected manually from respectively stake holders

- To & fro conversations are a plenty between infosec SPOC and teams for evidence collection

- Evidences collected are provided in a separate Desktop for Onsite audits or Laptop used be shipped for Offline audits to protect the artifacts

AFTER

- Evidences collection is automated using REST APIS, Scripts, Email Integrations

- Less Number of back and forth conversations due to Seconize DeRisk Centre

- Evidences collected are shown as "read-only" mode without any download option via Seconize DeRisk Centre.
  - No operational complexity of sending laptops or allocating desktops without compromise on evidence protection

Product Visualization – Compliance Mgmt

Compliance Dashboard

Compliance Details

Control Details

stg.seconize.co/cm/audits

Incognito

Welcome, Chethan

ACME

Compliance Mgmt / Audits

Compliance

Year
2023

All Filters

Search by Audits

+ Audit

2023

☑ Audit Period   ☑ Assessment Period

8	8	0	0
Total	Open	Completed	Overdue

Policies

Evidences

Audits

Approvals

| Audits	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
ISO27017_2015-Audit												
IRDAI_TEST_2023_1												
IRDAI_2023_Audit												
SOC-Audit-001												
RBI_Audit												
IRDAI_Audit												
SEBI-Cyber_Audit												
ISO_Audit												

15   8 of 8

11
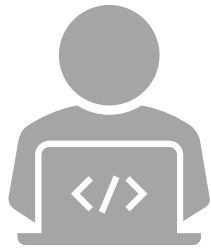
Challenges

Complexity of regulations and standards

Compliance requirements can be complex and difficult to interpret, making it challenging to develop automated audit processes.
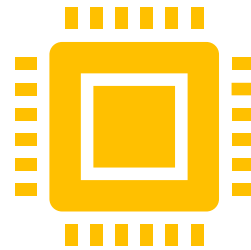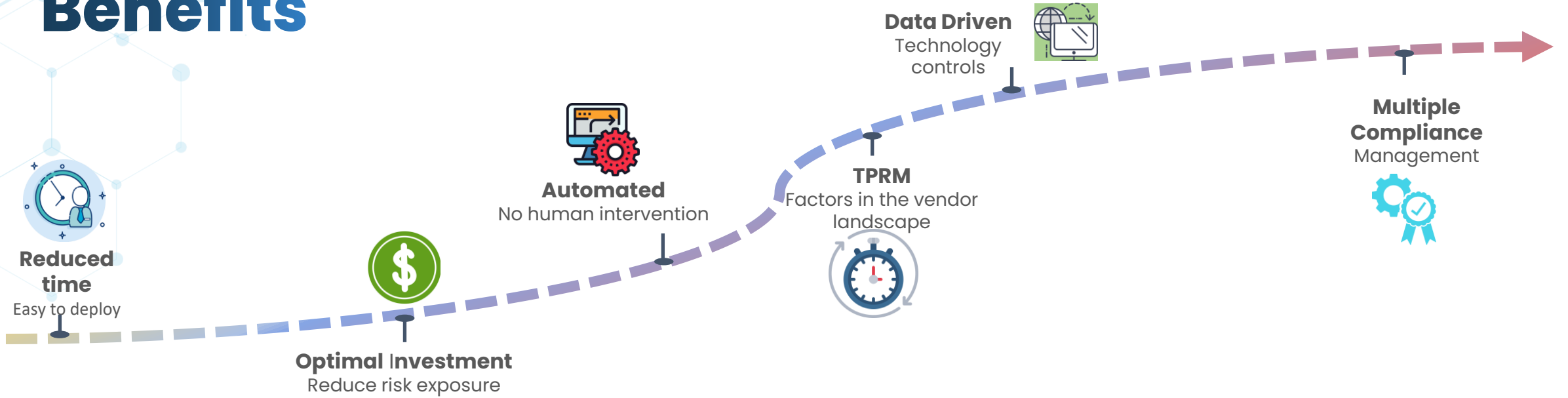
Integration with existing systems

Integrating compliance audit automation with existing systems can be difficult, particularly if those systems are outdated or not designed with automation in mind.
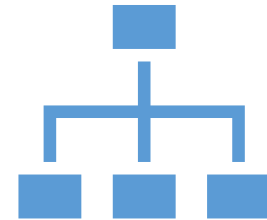
Training and adoption

Educating and training the internal audit teams of the change in approach from manual to automation. Helping the external auditors to adapt to the new system.

Benefits

Data Driven
Technology controls

Multiple Compliance
Management

Automated
No human intervention

TPRM
Factors in the vendor landscape

Reduced time
Easy to deploy

Optimal Investment
Reduce risk exposure

Easy to deploy	Cloud based SaaS product	**Compliance Dashboards**	Actionable reporting for informed decision making
Effort Reduction	From months to minutes	**Data Driven**	The technology aspects of the compliance are auto populated
Manage multiple compliances	Maps one compliance to another	**Customizable Workflows**	Tailor the system to your unique business processes
Maintain Confidentiality	Evidence can be viewed and not downloaded	**Regulatory Updates**	Stay ahead with automated updates on evolving compliance standards

Case Study

Leading Financial Services company

Customer Profile

Customer is a well-established Mutual Fund company. Have existing investments in Cybersecurity. SEBI compliance audits becoming stringent is taking away too much of their time

Customer Situation

- Has existing scanners
- Regulated by SEBI
- Audits are being done manually, which is taking them 3 months at a time, and significant effort
- Skeletal IT Security staff

Seconize Solution

- Ingesting the feeds from the existing scanners
- Compliance automation for SEBI Cyber and SEBI Controls
- Connectors to IT Systems to automate evidence management
- Roadmap to increase the automation coverage
- Comprehensive and exhaustive dashboards for efficient operation

Benefits & Key Outcomes

- Improved productivity as employees were spending less time with external auditors for interviews and filling questionnaires.
- Reduced "Cost-To-Comply" due to automation

India Top 10, Conglomerate

Customer Profile

Customer is a top 10 company out of India. Customized compliance framework built, enforcing it and monitoring from the parent company is a challenge.

Customer Situation

- Customized compliance, derived from ISO 27001 and NIST
- Manual audits across 17 group companies,
- Want to enforce the custom compliance across all group companies

Seconize Solution

- Ingesting the feeds from the existing scanners
- Compliance automation for customized compliance
- Connectors to IT Systems to automate evidence management
- Comprehensive and exhaustive dashboards for efficient operation
- Manager of manager system to manage all group companies

Benefits & Key Outcomes

- The parent company able to roll out customized compliance across all the group companies and manage them.
- Reduced "Cost-To-Comply" due to automation and better security posture.
- Ease of reporting to management and board.

Fortune 500 Company

Customer Profile

Customer is a fortune 500 company HQ out of US. Is regulated and has to comply to ITGC SOX compliance. Multiple teams assigned to the task and increasing complexity.

Customer Situation

- ITGC SOX is being done manually
- Multiple teams across globe involved in the internal audit
- Challenging to do the internal audit across teams

Seconize Solution

- Compliance automation for ITGC SOX
- Connectors to IT Systems to automate evidence management
- Collecting evidence from legacy systems
- Comprehensive and exhaustive dashboards for efficient operation
- Controls testing in place

Benefits & Key Outcomes

- The onerous task of internal audit is automated
- Reduced "Cost-To-Comply" due to automation and better security posture.
- Work with the external auditors directly
- Bringing in more applications to be audited

Competitors & Differentiation

Seconize has upper-hand!

Differentiators:

- ✓ Data Driven
- ✓ Integrates with Enterprise systems
- ✓ Evidence Collection
- ✓ Factual data reports
- ✓ Continuous
- ✓ Product roadmap
- ✓ Compliance regulated

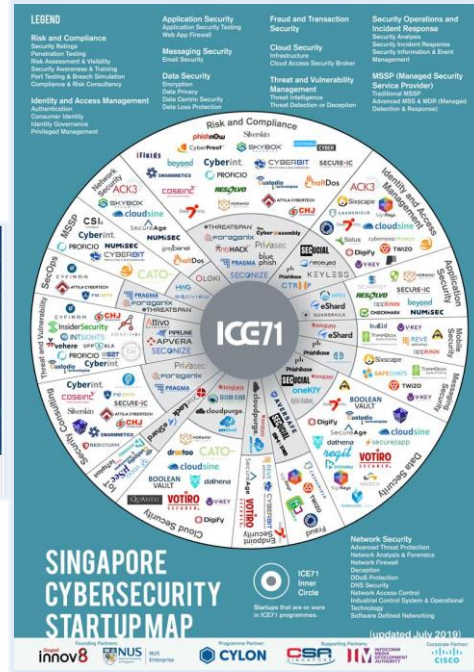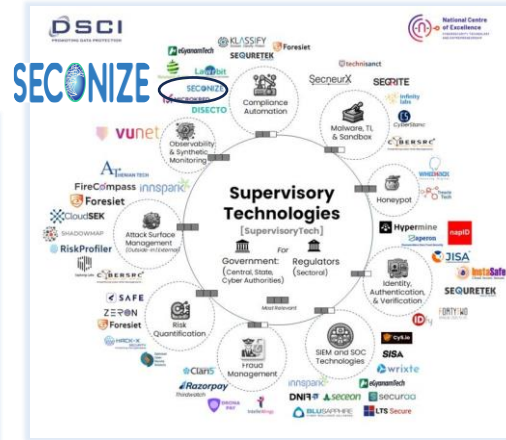|	Feature	Hyper Proof	Audit Board	RSA Archer	Service Now	SEC❂NIZE
Continuous Controls Monitoring	*Standards driven*	✓	✓	✓	✓	✓
	Regulatory driven	✓	✓	✓	✓	✓
	Custom Policies	✓				✓
Automated Evidence Collection	*Out of Box Connectors*	✓		✓		✓
	Legacy Systems					✓
Automated Controls Testing	*Post Processing of Evidences*					✓
	Data backed Gap Assessments					✓
Simplified Workflows	*Internal Audit Readiness*	✓	✓	✓	✓	✓
	Inbuilt DRM for Sensitive Artifacts					✓
	Audit Observations Tracking	✓	✓		✓	✓

Recognition

DSCI – India
Cybersecurity Product
Of the year 2021

Top 5 Startups to watch out for in 2020

iDEX Defence Award Winner, 2023

DSCI
《 **Product Companies**

Globe – 100 Startups to look out for in 2021

MVP Stage – Winner

Emerge 50 – Top 50 Deep Tech startups

Singapore – Cybersecurity map
Top 5 cybersecurity

Thank You

SECONIZE

De-Risking Cyber