
13TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY SUMMIT
cybersecuritysummit.org
RESILIENCE UNLOCKED
TITLE SPONSOR
Island
#cybersecuritysummit #css13

Modernizing your Governance, Risk and Compliance Program in the age of Technological Innovation

Michael V. Siegrist

Cloud Manager | GRC and Security Assurance

OneTrust

PRIVACY, SECURITY & GOVERNANCE

Michael V. Siegrist

- 12 Years in GRC, TPRM and ESG Software Solutions
  - ServiceNow-GRC, ITRM and ESG Specialty Team
  - RSA Archer- EMC-Dell Solution Transition
  - LockPath (Navex)
- Corporate counsel-Gaming, healthcare and finance.
- DFW Based

Agenda

1. Introduction and Current Challenges
2. Foundational Elements to Drive Enterprise Wide Collaboration
3. Refining your Risk Assessment Processes to include considerations for Artificial Intelligence
4. Modernize your Control Testing Program to Drive Efficiency and Reduce errors

Internal and external pressures on IT risk & compliance

Expansion of **Cloud Services**

Jira aws CROWDSTRIKE snyk DATADOG

Evolving **compliance requirements**

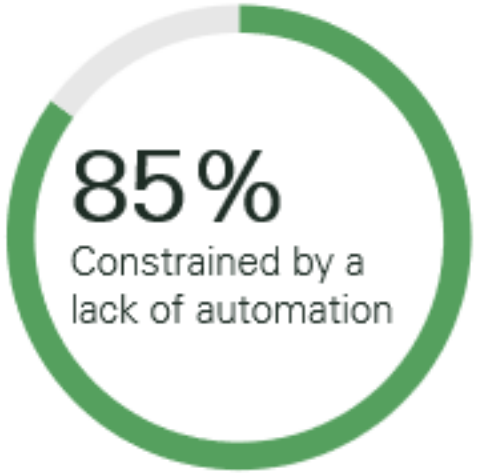
Proliferation of **data**

Changing dynamics and internal **complexity**

Various **stakeholders** to engage and educate

Tech challenges for program insights

Organizations that are not managing GRC processes in a unified ecosystem face significant barriers to efficient reporting.



The Surprising Sate of GRC Reporting
OCEG, 2022

Siloed GRC practices in flight/ operation

Redundancy, time and opportunities for error

- **Static data sources and varying priorities** create shadow workflow processes.
  - *i.e. SharePoint, spreadsheets, e-mail*
- **Repeat information gathering and manual evaluation** create opportunities for error and points of failure.
- Inconsistencies lead to **poor adoption for casual users** and program contributors.

CISO's need a better way to orchestrate risk and compliance

Siloed administration → Resource-intensive maintenance → Trust by design

Orchestrating trust through risk ownership

Guidance

Extended Stakeholders

Integration & Automation

Content & Program Req's

Capabilities

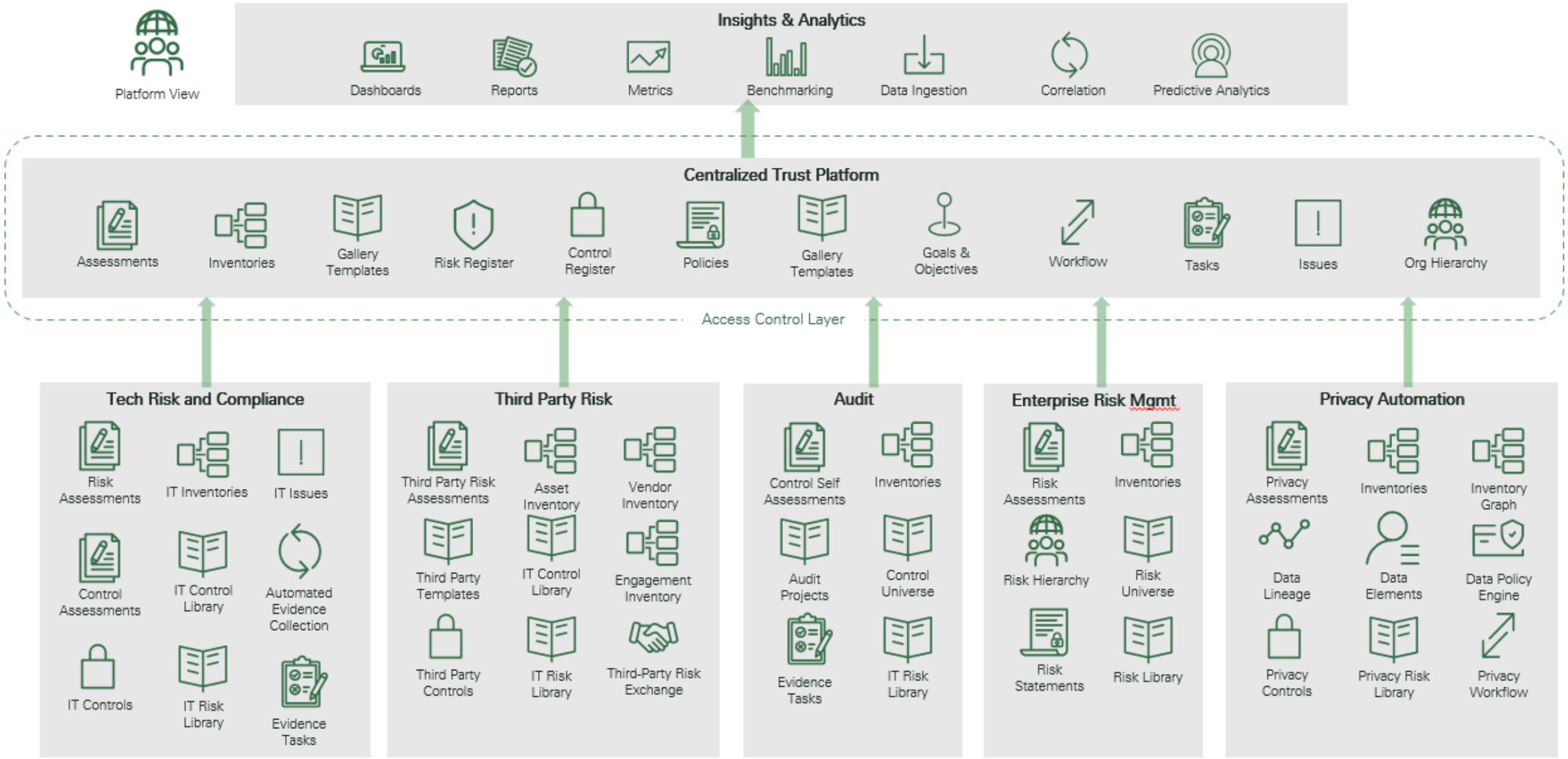
User Experience

Integrations & Automation

Capabilities

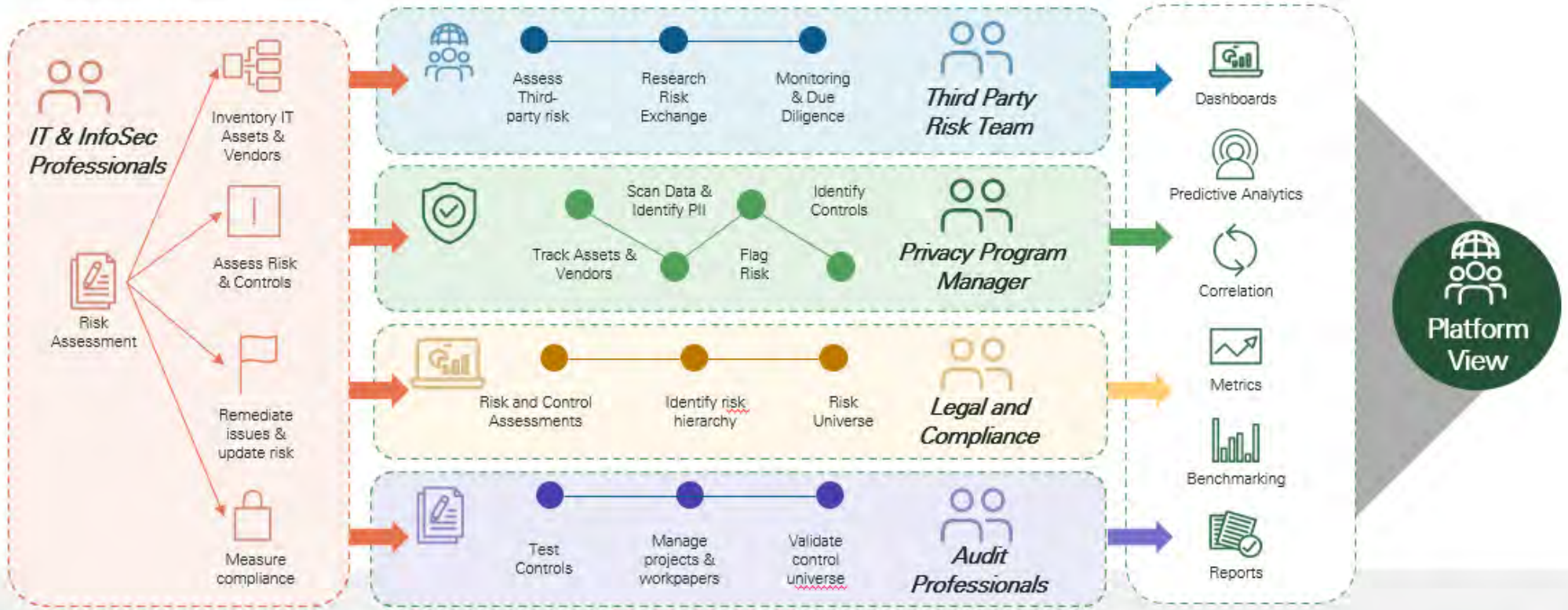
Content & Guidance

Foundational Elements to Drive Enterprise Wide Collaboration


Platform View
Insights & Analytics
Dashboards
Reports
Metrics
Benchmarking
Data Ingestion
Correlation
Predictive Analytics
Centralized Trust Platform
Assessments
Inventories
Gallery Templates
Risk Register
Control Register
Policies
Gallery Templates
Goals & Objectives
Workflow
Tasks
Issues
Org Hierarchy
Access Control Layer
Tech Risk and Compliance
Risk Assessments
IT Inventories
IT Issues
Control Assessments
IT Control Library
Automated Evidence Collection
IT Controls
IT Risk Library
Evidence Tasks
Third Party Risk
Third Party Risk Assessments
Asset Inventory
Vendor Inventory
Third Party Templates
IT Control Library
Engagement Inventory
Third Party Controls
IT Risk Library
Third-Party Risk Exchange
Audit
Control Self Assessments
Inventories
Audit Projects
Control Universe
Evidence Tasks
IT Risk Library
Enterprise Risk Mgmt
Risk Assessments
Inventories
Risk Hierarchy
Risk Universe
Risk Statements
Risk Library
Privacy Automation
Privacy Assessments
Inventories
Inventory Graph
Data Lineage
Data Elements
Data Policy Engine
Privacy Controls
Privacy Risk Library
Privacy Workflow

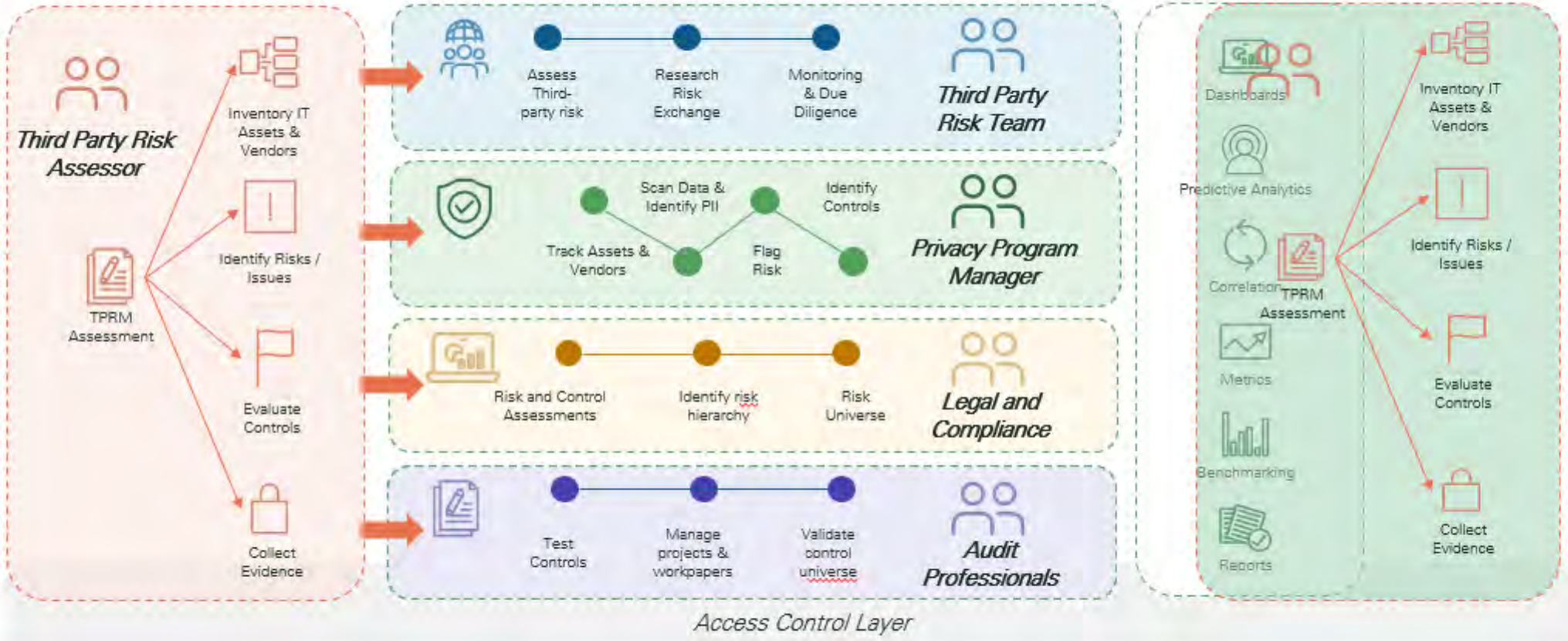
Unify workstreams across Risk and Compliance

Platform Lifecycle Overview



Scenario-Other Teams May Trigger Processes

Platform Lifecycle Overview



Refining Your Risk Assessment Processes to include considerations for Artificial Intelligence

AI is at an inflection point

Driven by:

Lower barrier to entry to adopt AI tools

83%

Number of AI-related GitHub projects grew 83% in the last 5 years

A rise in AI incidents

26X

The number of AI incidents and controversies has increased 26X since 2021

Lack of organizational preparedness

33%

Only 33% of business leaders have aligned AI risk management with their organizations broader risk management program

The era of unregulated AI is coming to an end

6.5X

Mentions of AI in global legislative proceeds have increased nearly 6.5 times since 2016

AI Index 2023 Annual Report Tech Jury 2023

AI presents new and unforeseen risk

Raising questions to ask and answer

What data is needed?	What must users know?	Where is third-party AI used?	Can we re-use existing work?
Data surge	**Black boxes**	**Third-parties**	**Legal**
AI incentivizes data collection & secondary use	Systems often lack transparency needed to govern their use	AI complicates third party risk management	AI reinforces existing obligations and introduces new ones

AI laws and frameworks snapshot

EU AI Act

	Company A	Company B
TYPE	User	Provider
DESCRIPTION	Uses vendors and service providers of AI systems	Develops AI systems embedded in the products/services they offer
EXAMPLE AI SYSTEMS	Third-party software *eg. HR hiring system*	OCR (optical character recognition) system *eg. Resume scanner*

Examples of Requirements from EU AI Act

Conformity Assessments

Documentation

Transparency

Building bridges

Risk-based approach fundamentals

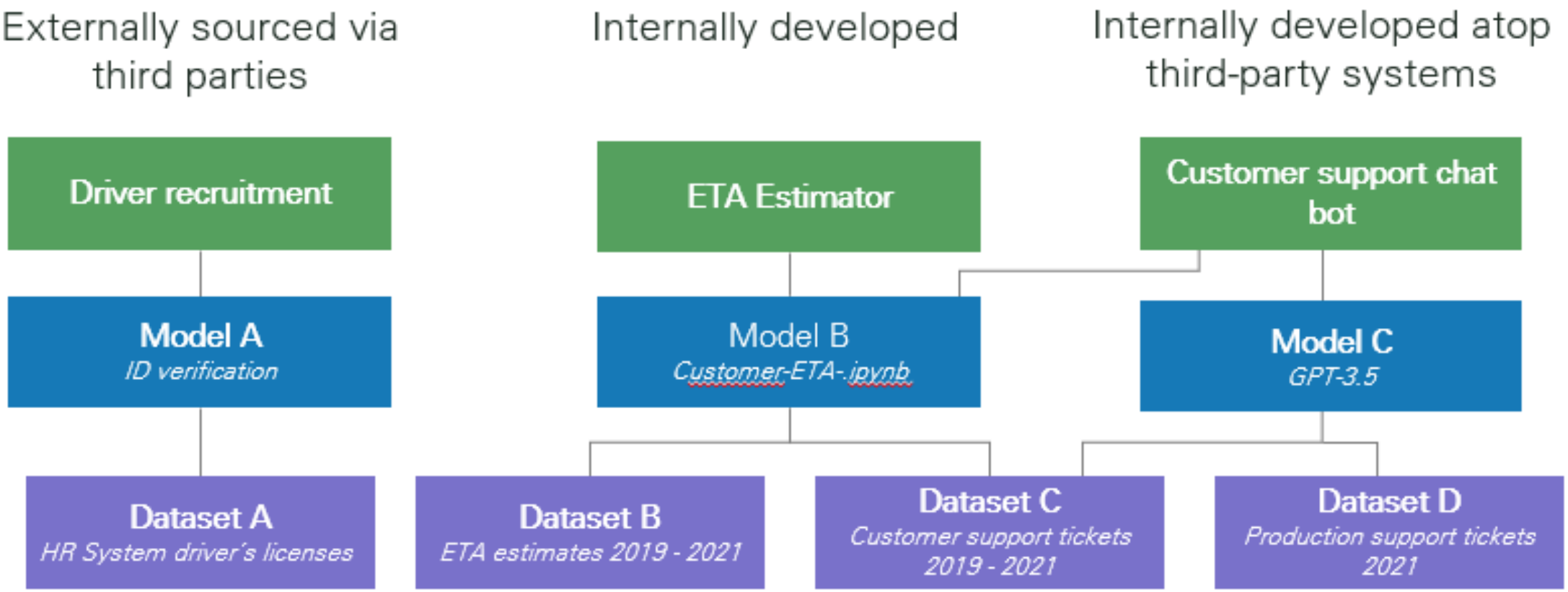
Technology

Oversight

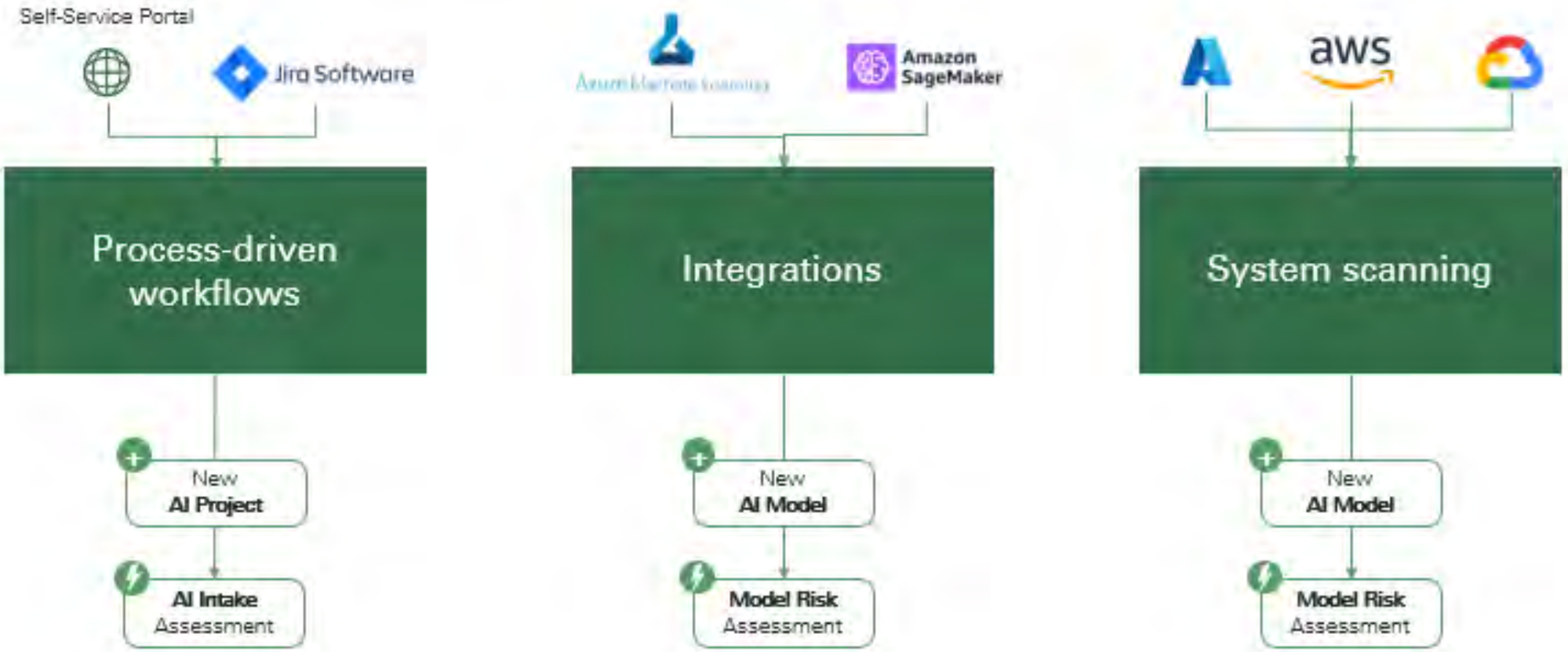
1. Inventory
2. Assess
3. Mitigate
4. Monitor

System components can be interrelated

Example: A ride sharing app



Detecting AI use across the business



Before you grant access…

Considerations

- What stakeholders must be involved?
- What are the inputs?
- What are the outcomes?
- What new/existing controls are required?

Scenario 1

A bank utilizing a service provider for optical character recognition

What stakeholders must be involved?	*Marketing, Sales, Development, Information Security, Privacy, Procurement, Legal & Compliance, Ethics*
What are the inputs?	*Contact information, financial data*
What are the outcomes?	*Remote deposit fulfillment; loan approval**
What new/existing controls are required?	*Bias & fairness monitoring, access controls*

Scenario 2

A retailer building a chat bot for product recommendations

What stakeholders must be involved?	*Marketing, Sales, Development, Information Security, Privacy, Legal & Compliance, Procurement*
What are the inputs?	*Product descriptions, customer queries, customer contact information, payment information*
What are the outcomes?	*Product recommendations; order fulfillment*
What new/existing controls are required?	*Opt-out of automated decision-making*

Future-proof your data across its lifecycle for responsible use in AI systems

Collect or create

Capture first-party data with consent and purpose to respect choice, regulatory requirements, and business policies

Process, share, and use

Understand and assess risk for how data are used by internal and external individuals, systems, and AI models.

Store and dispose

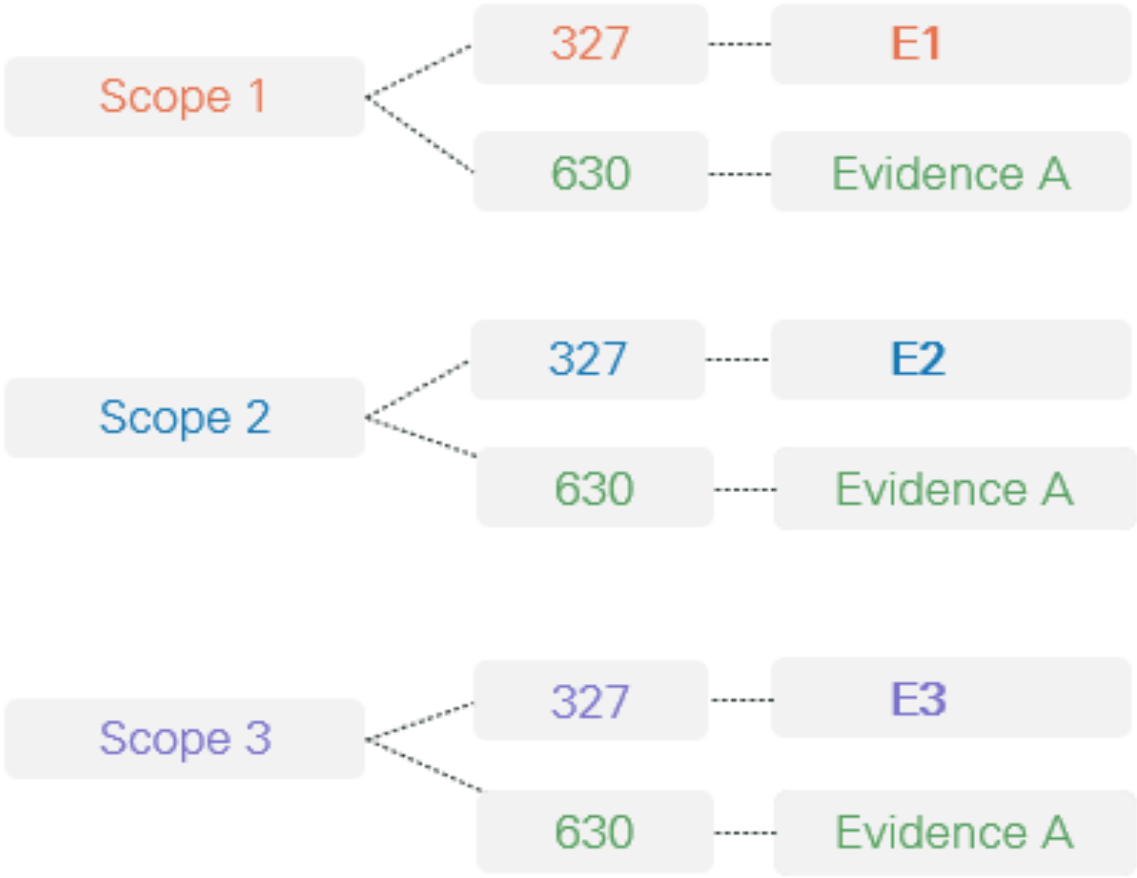
Ensure data visibility and protection, with appropriate access, risk mitigation, and retention period enforcement.

Modernize your Control Testing Program to Drive Efficiency and Reduce errors

Standardize compliance requirements

Scope your program to scale with a flexible data model to reduce deviations and reinforce consistency across control implementations with common objectives.

Leverage a consistent compliance baseline to evaluate control maturity and risk based on your business objectives.



Standardize compliance requirements

Scope your program to scale with a flexible data model to reduce deviations and reinforce consistency across control implementations with common objectives.

Leverage a consistent compliance baseline to evaluate control maturity and risk based on your business objectives.

Standardize compliance requirements

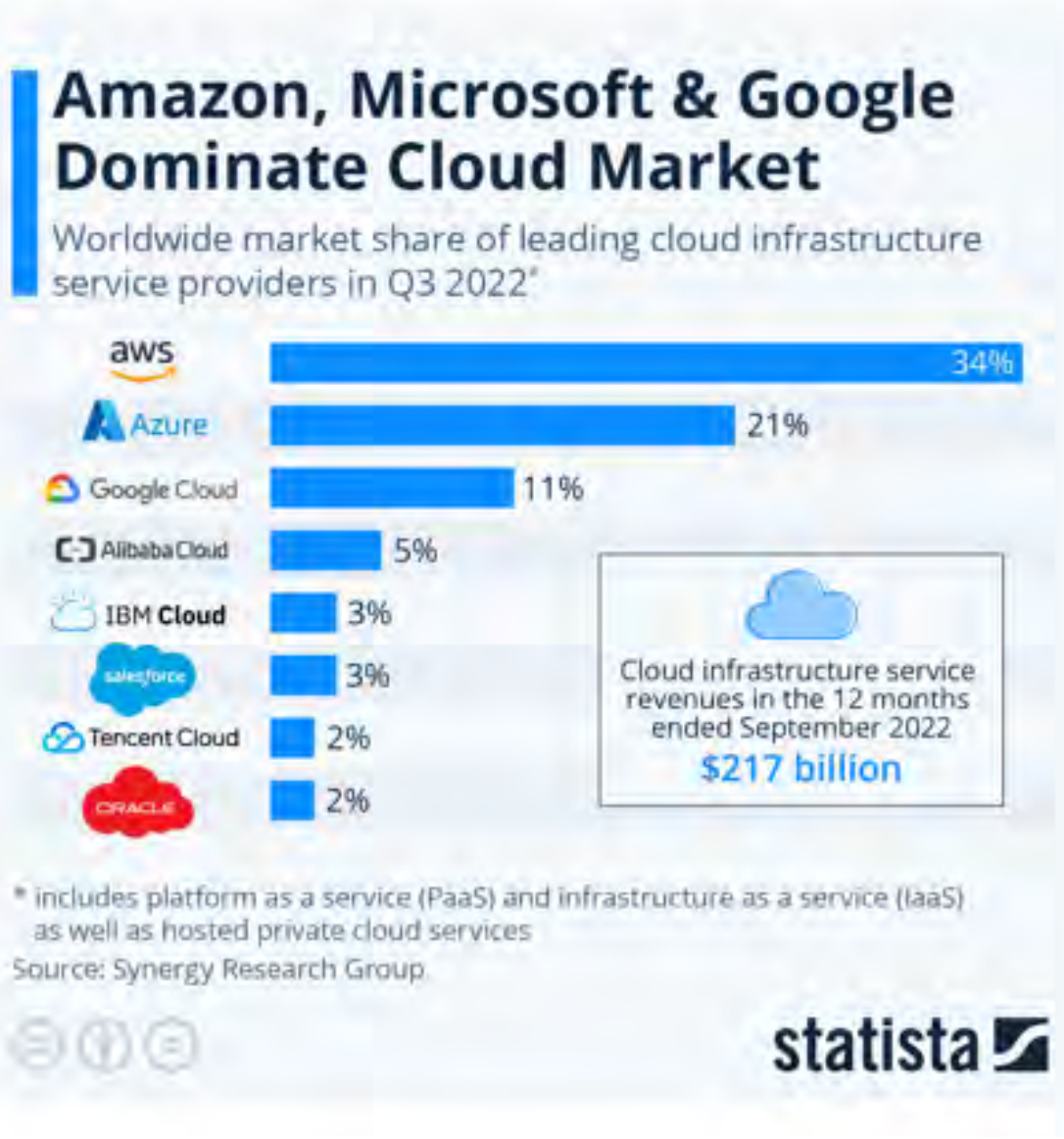
Scope your program to scale with a flexible data model to reduce deviations and reinforce consistency across control implementations with common objectives.

Leverage a consistent compliance baseline to evaluate control maturity and risk based on your business objectives.

Translate to the business & SecOps tech

Alleviate the burden of maintaining APIs across your tech stack for internal applications.

Use-case specific integrations connect directly into business operating systems and functions.



Collect evidence on time, and in scope

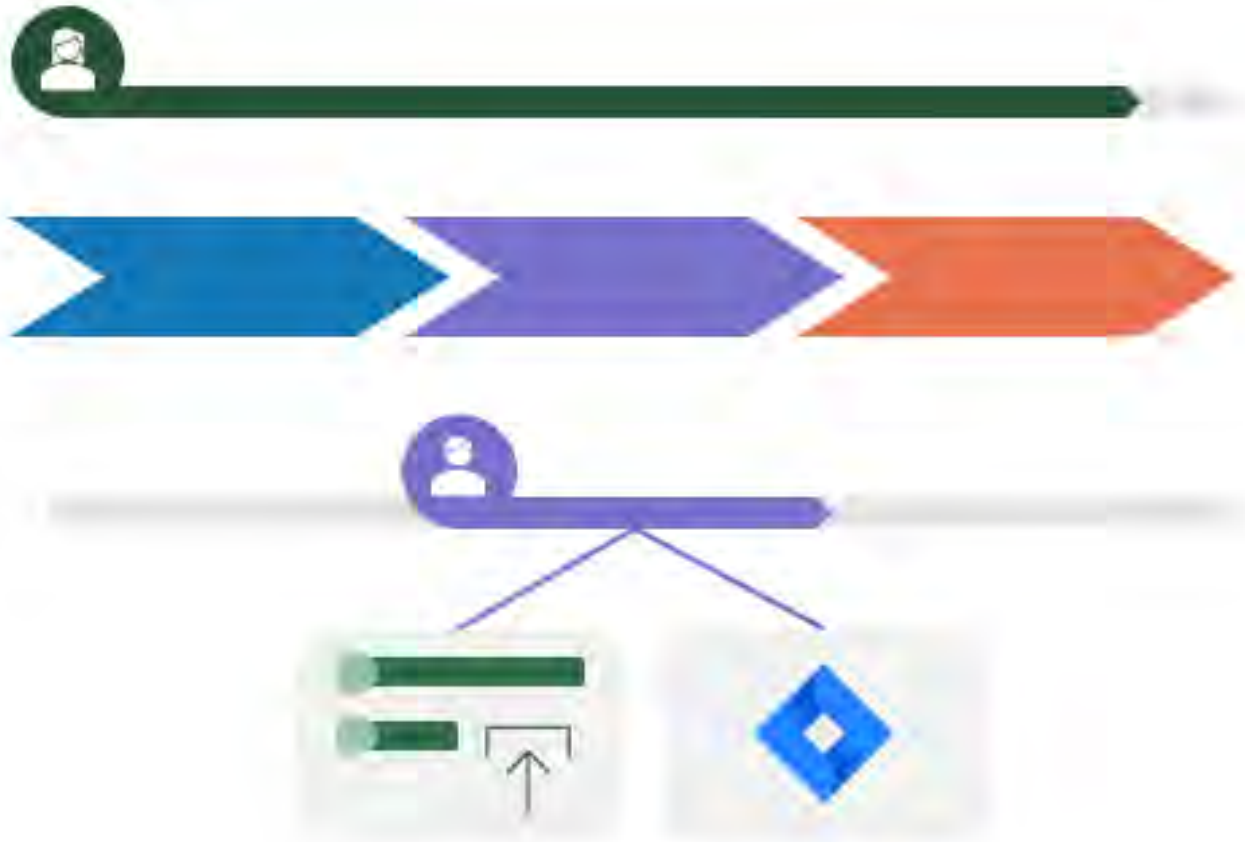
Scan systems an application in cadence with your IT audits and risk lifecycle.

Automatically collect and verify evidence to be continuously compliant.

Optimise business engagements

Connect your compliance capabilities with tailored experiences to engage stakeholders.

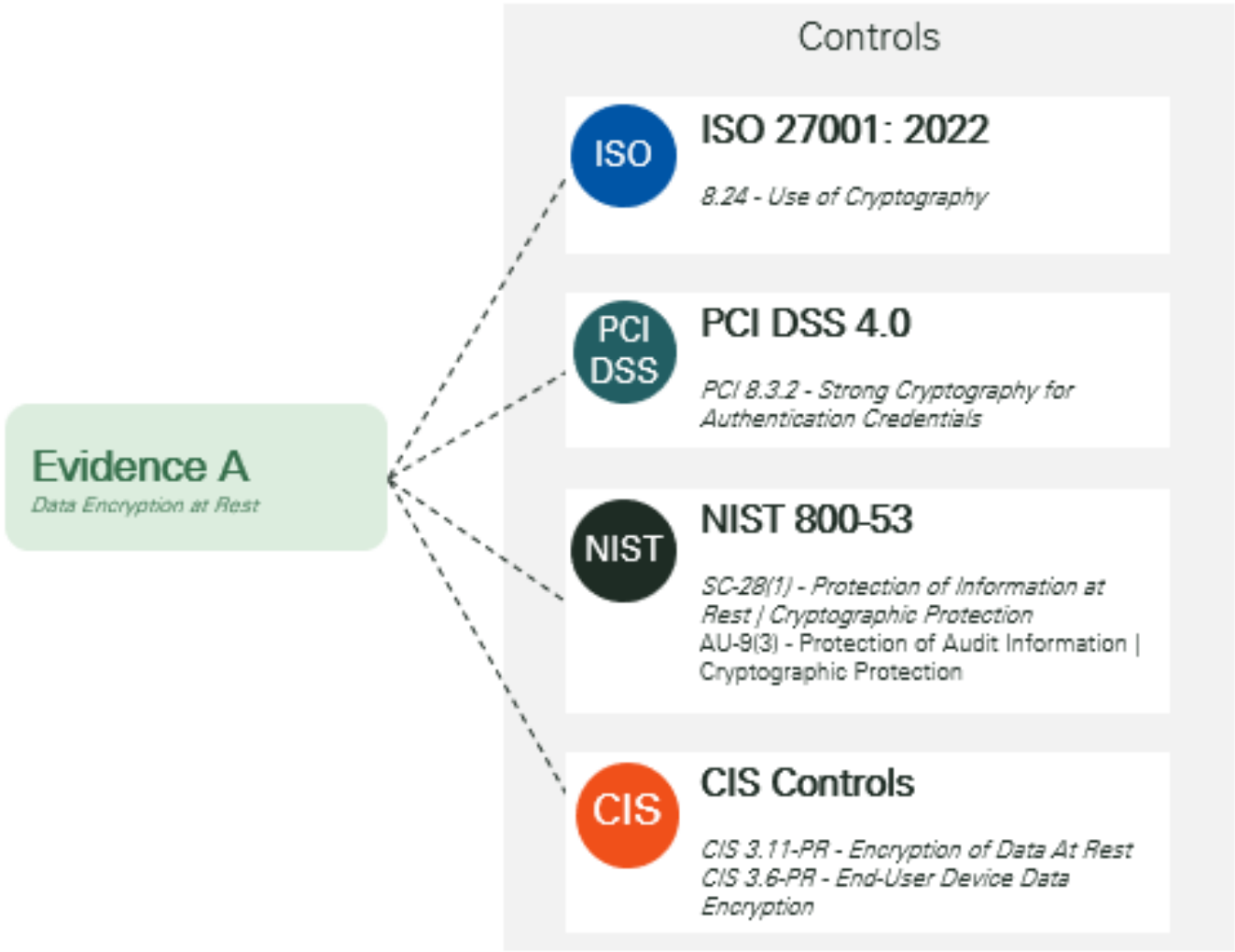
- Intuitive, role-based user experience
- Guide and engage stakeholders who are removed from risk
- Streamline cross-functional collaboration by integrating where the business operates.



Test once, comply many

Keeping pace with the rate of change across external compliance requirements.

Operationalized **content** across leading frameworks with standardized evidence requirements, mapped across controls to report into different auditable scopes.



Key areas prime for better automation

1 Standardize evidence requirements

- Leverage regulatory, standard, and framework intelligence to maintain controls.
- Identify specific data points (SecOps data, configuration, or evidence) that meet repeatable compliance requirements.

2 Translating to your Tech Stack

- Pre-scoped (purpose-built) technology paths
- Focus data exchanges to meet specific (std) evidence obligations
- Coordinate data to avoid manual touchpoints

3 Collect evidence in scope, and on time

- Scan systems an application in cadence with your IT audits and risk lifecycle
- Validate evidence against scope and notify stakeholders

4 Optimize business engagements

- Intuitive, role-based user experience
- Guide and engage stakeholders who are removed from risk
- Integrate with collaboration tools

5 Test once, comply many

- Map evidence to common controls across different compliance scopes
- Report evidence across overlapping framework requirements; Test once, comply many

Key Takeaways

1. Risk and Compliance will only become more complex as IT systems adopt the cloud, AI and other technologies.
2. To keep up, consider:
    1. Driving enterprise-wide collaboration
    2. Incorporating AI considerations into your risk assessment process
    3. Automate control testing to ensure accuracy and timely compliance reporting

Thank you!