Unify Third-Party Risk and Cybersecurity for Sustainable Resiliency

ProcessUnity

Today’s Presenter

Brad McAdams
Pre-Sales Manager
ProcessUnity

The ProcessUnity Platform

50+ Use Cases

- Third-Party Risk Management
- Cybersecurity Risk Management
- Anti-Bribery & Corruption

Key Features

- ✓ Hands-Free Automation
- ✓ Enterprise Integration
- ✓ No-Code Configuration
- ✓ Real-Time Reporting

Our Customers

50% CPO

50% CISO
CCO
CRO

Named a **Leader** in the Forrester Wave for Third-Party Risk Management

800+ years of risk experience

The Boston Globe
TOP PLACES TO WORK 2022
MASSACHUSETTS

SHARED ASSESSMENTS

Crowe

REFINITIV

BITSIGHT
The Standard in SECURITY RATINGS

Global partner network

Cyber and Procurement Share Two Goals

Reduce Risk

Internal and external risk management

Reduce Costs

Eliminate process and workflow redundancy

Collaboration Drives Cost and Risk Reduction

Procurement

Sources and onboards external partners

Cybersecurity

Sets internal and external cyber standards

Consolidate Services & Technologies

Eliminate Process & Workflow Redundancy

Manage Risks, Not Incidents

Challenges to Unifying Cyber and Procurement

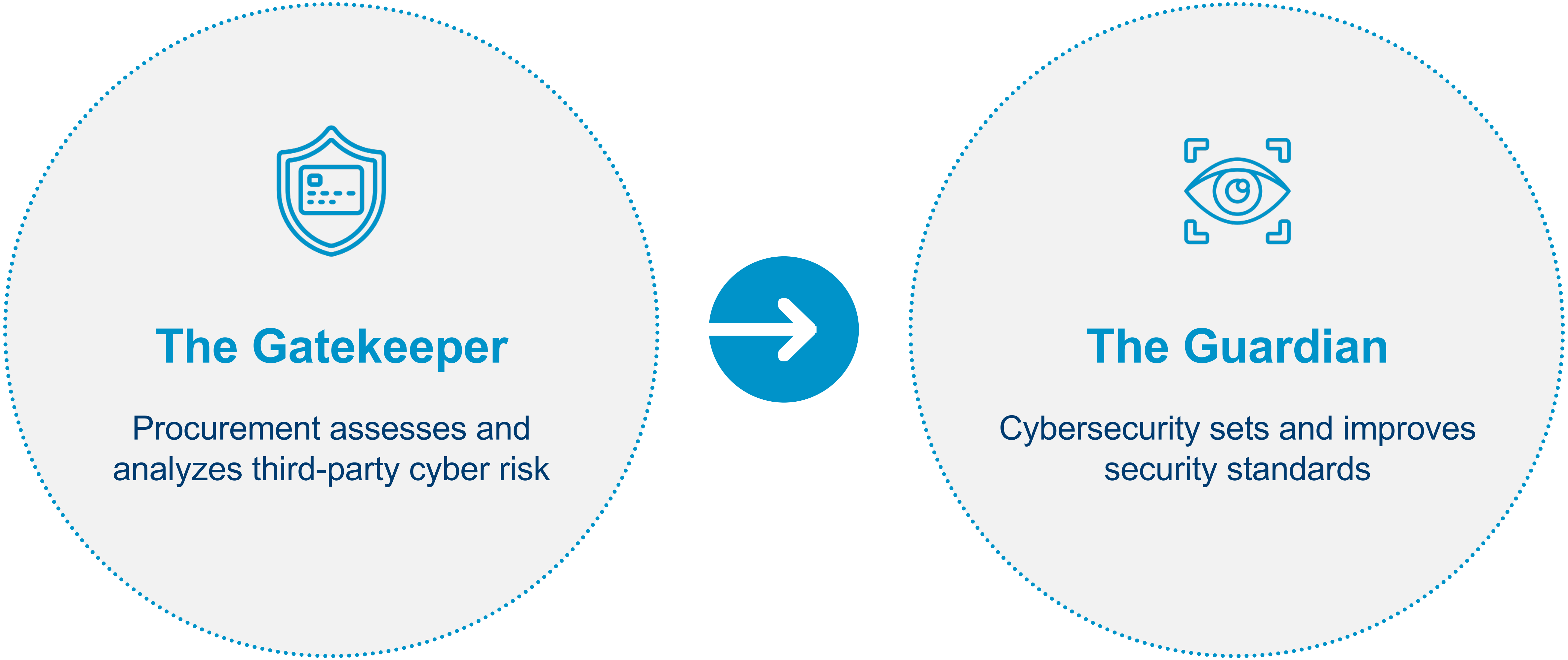
Limited visibility between teams

Duplicate work

Security gaps in the third-party network

Lack of centralized control framework

Partnership Decreases Vulnerability



The Gatekeeper

Procurement assesses and analyzes third-party cyber risk

The Guardian

Cybersecurity sets and improves security standards

Risk Unification is the Key to a Strong Defense

Cybersecurity

- Continuous control improvements
- Internal and external risk monitoring
- Faster, informed incident response

Shared Data

Assessments

Regulatory Changes

Security Events

Procurement

- Better due diligence questionnaires
- Deeper vendor risk analysis
- Security worked into vendor contracts

Steps to Unifying Cybersecurity and Third-Party Risk Management

1. Establish your enterprise controls
2. Scope questionnaires based on controls
3. Relate third-party responses to your controls
4. Evaluate control effectiveness and remediate gaps

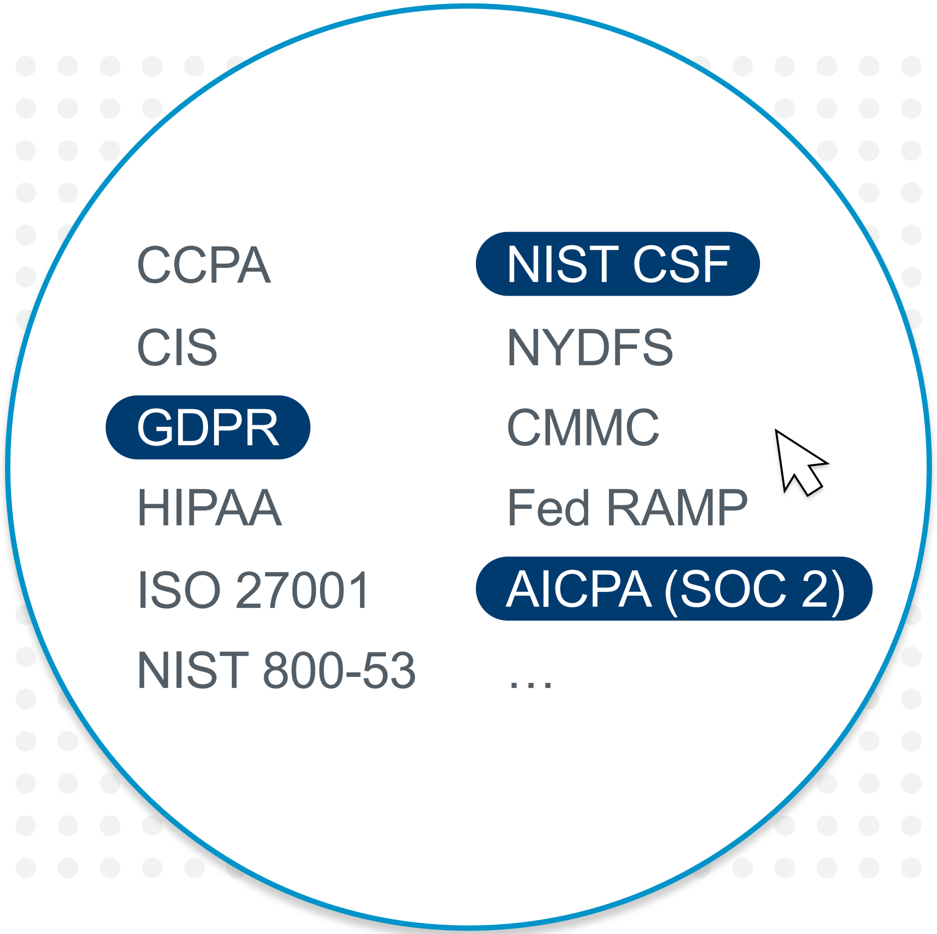
Step 1: Establish Your Enterprise Controls

ProcessUnity

Step 1: Get Your House in Order

META-FRAMEWORK ARCHITECT SPEEDS CONTROL LIBRARY CREATION

Select all applicable regulations and standards:



CCPA

CIS

GDPR

HIPAA

ISO 27001

NIST 800-53

NIST CSF

NYDFS

CMMC

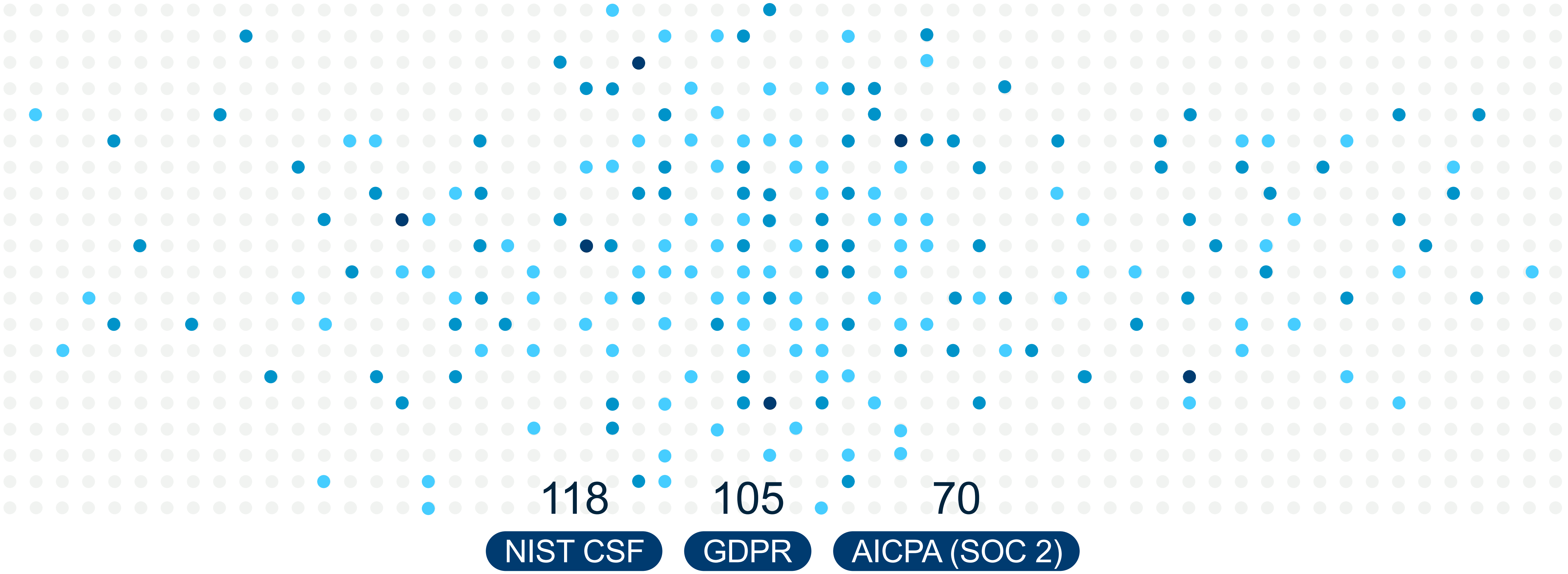
Fed RAMP

AICPA (SOC 2)

…

Step 1: Get Your House in Order

META-FRAMEWORK ARCHITECT SPEEDS CONTROL LIBRARY CREATION



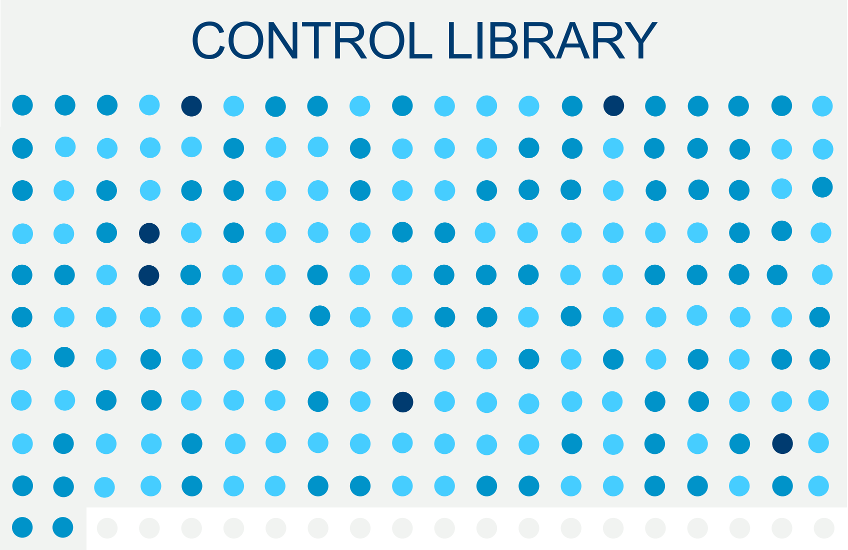
Step 1: Get Your House in Order

META-FRAMEWORK ARCHITECT SPEEDS CONTROL LIBRARY CREATION

293 Total controls

91 Shared

202 Identified Controls



118 NIST CSF

105 GDPR

70 AICPA (SOC 2)

30%

Reduction of control redundancy in a simple click of a button

Step 2: Scope Questionnaires Based on Controls

ProcessUnity

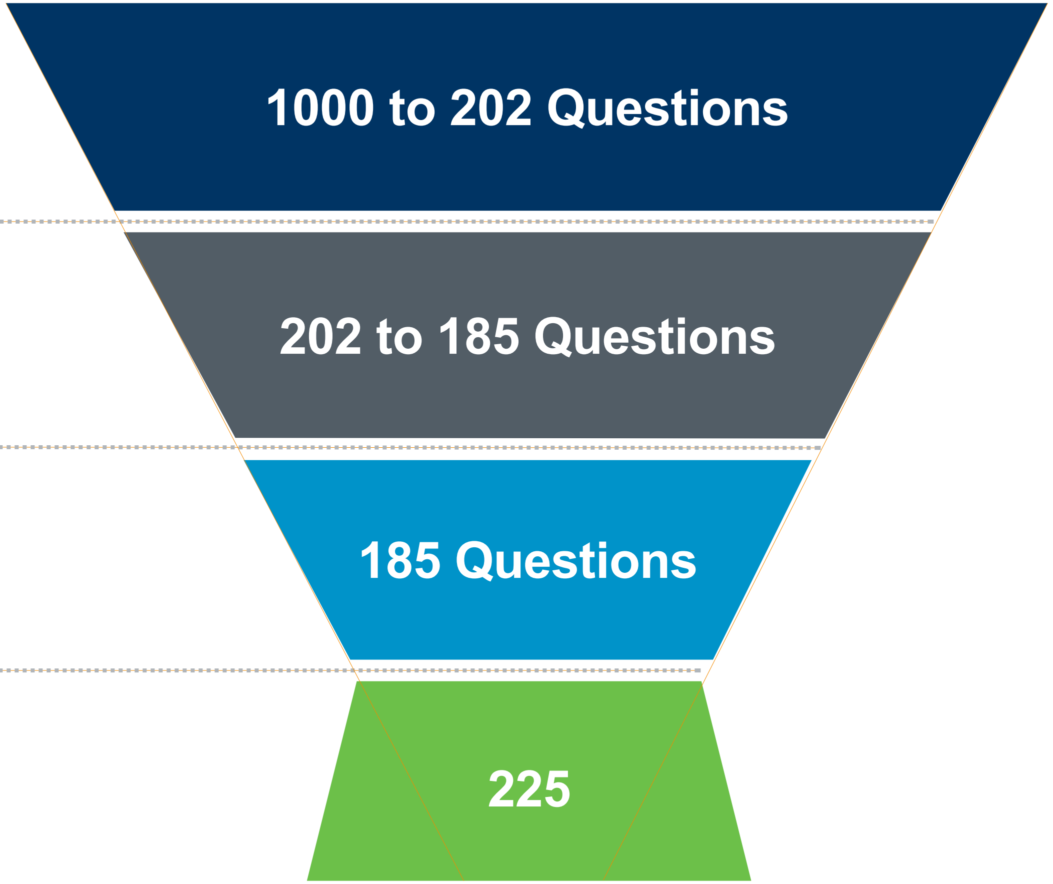
Develop Questionnaires Based on Hybrid Model

- Select relevant questions / sections from an industry-standard questionnaire
- Augment with your own propriety questions / sections
- Allow vendors to submit their completed industry-standard questionnaire
- Ask the vendor to respond only to the questions not covered in the industry-standard questionnaire
- Speeds response times, helps ensure completeness

Step 2: Scope Questionnaires Based on Controls

AUTOMATICALLY SCOPE QUESTIONS BASED ON CONTROLS & VENDOR CHARACTERISTICS

Step 1: Align Questions to Your Standard(s)	Aligns to NIST CSF, SOC II, GDPR
Step 2: Scope Access to Data Questions	Third party has no data access
Step 3: Scope Regulation Questions	N/A: Data regulation questions scoped out already
Step 4: Scope Additional Risk Domain Questions	In scope for ABAC and ESG



1000 to 202 Questions

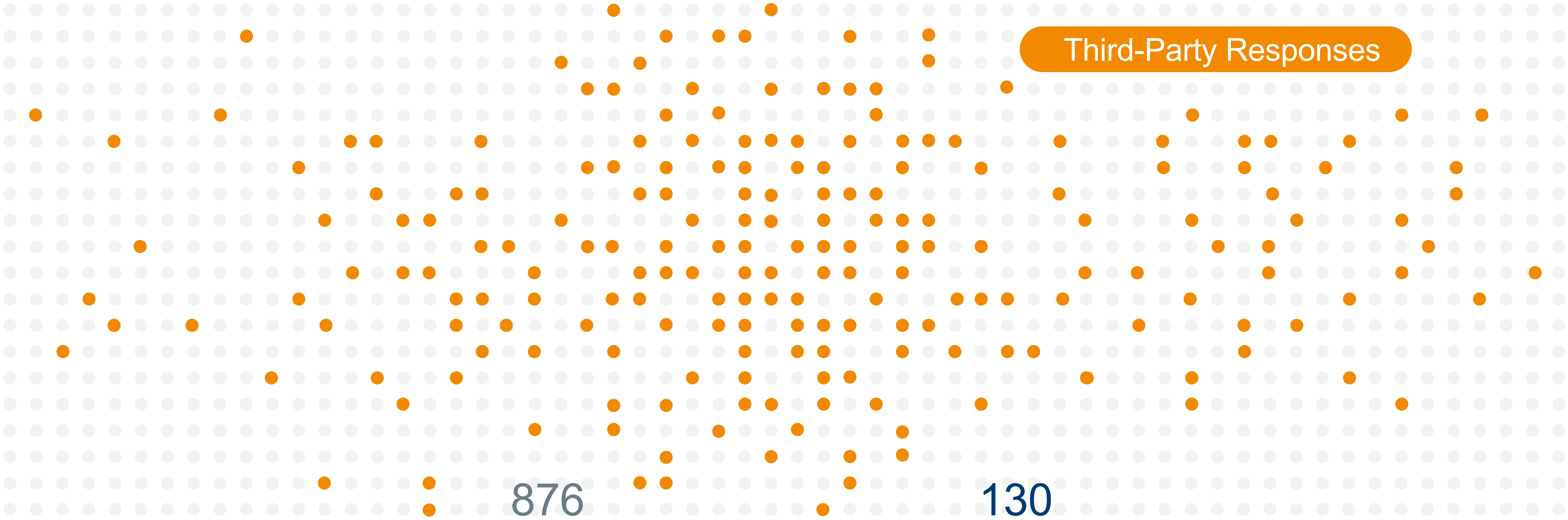
202 to 185 Questions

185 Questions

225

Conditional Question Scoping

Scope External Control Review



Third-Party Responses

876

Total Questions in Library

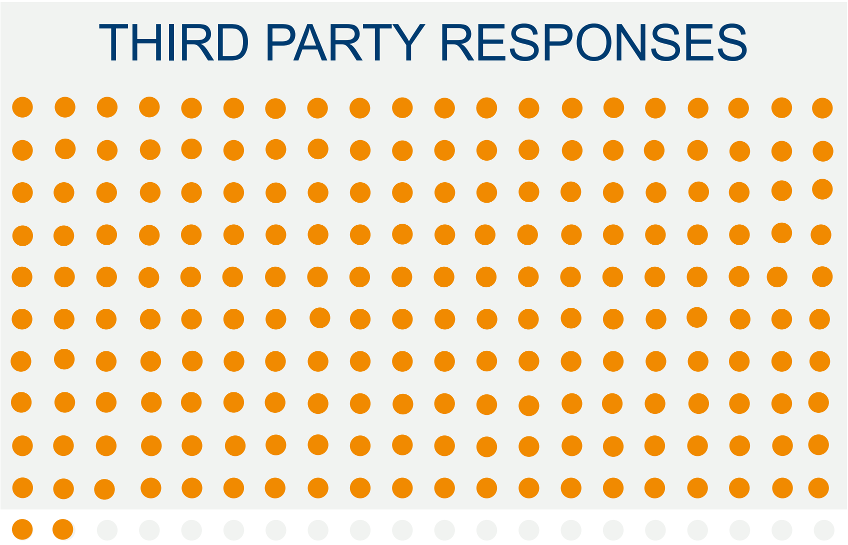
130

Total Enterprise Controls

Responding To Questions – Scope Relevant Controls

Third-Party Risk Drives Scope

876	Total Questions
442	Required Responses
58	Relevant Controls


THIRD PARTY RESPONSES

50%

Of responses are applicable to the third-party based on conditionality scoping

55%

Of enterprise controls are out of scope for the third party based on the required responses

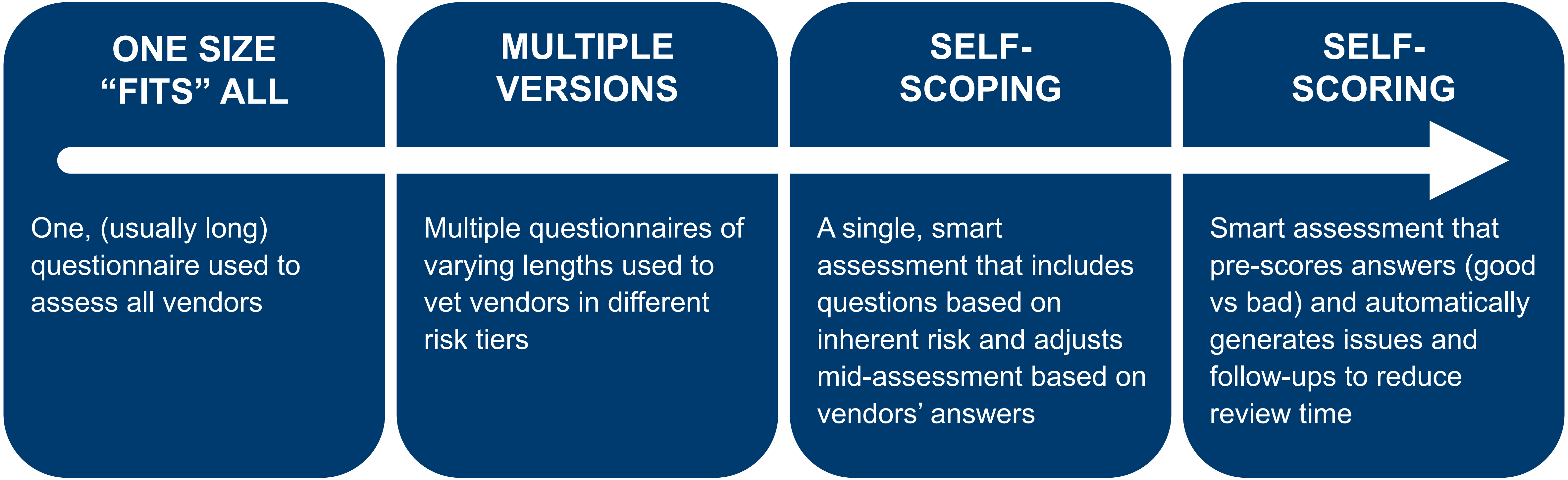
876

Total Questions in Library

130

Total Enterprise Controls

Due Diligence Questionnaire Maturity



ONE SIZE "FITS" ALL

One, (usually long) questionnaire used to assess all vendors

MULTIPLE VERSIONS

Multiple questionnaires of varying lengths used to vet vendors in different risk tiers

SELF-SCOPING

A single, smart assessment that includes questions based on inherent risk and adjusts mid-assessment based on vendors' answers

SELF-SCORING

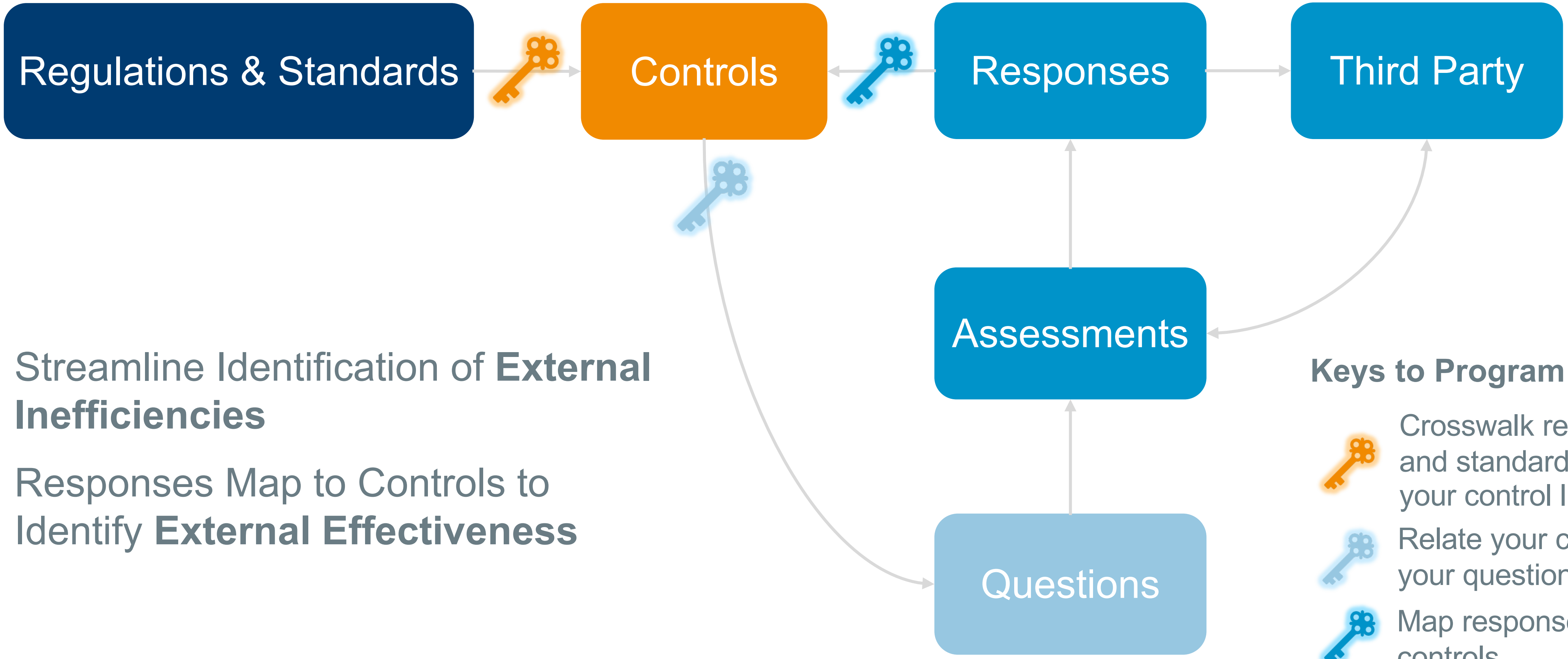
Smart assessment that pre-scores answers (good vs bad) and automatically generates issues and follow-ups to reduce review time

Step 3: Relate Third-Party Responses to Your Controls

ProcessUnity

Step 3: Mapping Third Parties to Your Controls

Establishing Relationships is the Key to Success



- Streamline Identification of **External Inefficiencies**
- Responses Map to Controls to Identify **External Effectiveness**

Keys to Program Success

- 🔑 Crosswalk regulations and standards to build your control library
- 🔑 Relate your controls to your questions
- 🔑 Map responses to controls

Step 3: Relate Third-Party Responses to Your Controls

- GOV-01 – Security & Privacy Governance Program

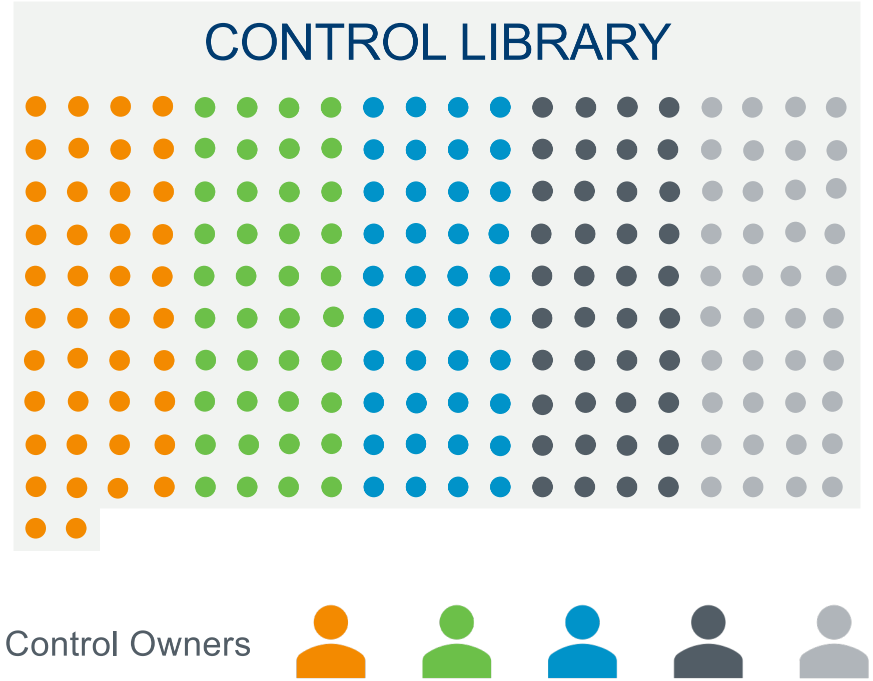
  Does the organization staff a function to centrally-govern cybersecurity and privacy controls?

5 – Continuously Improving
4 – Quantitatively Controlled
3 – Well-Defined
2 – Planned & Tracked
1 – No

VENDOR	SCORE
ACME Services	5
Rogers Appraisals	5
Golden Products	4
Weatherly Services Inc.	2
Systems Deluxe	1

Step 4: Evaluate Control Effectiveness

Step 4: Evaluate Holistic Control Effectiveness

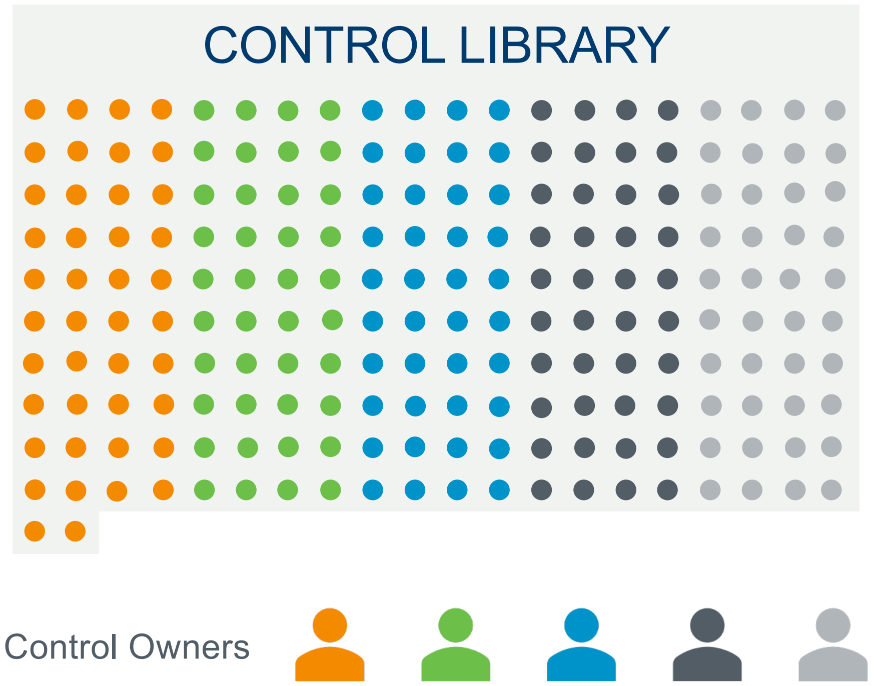


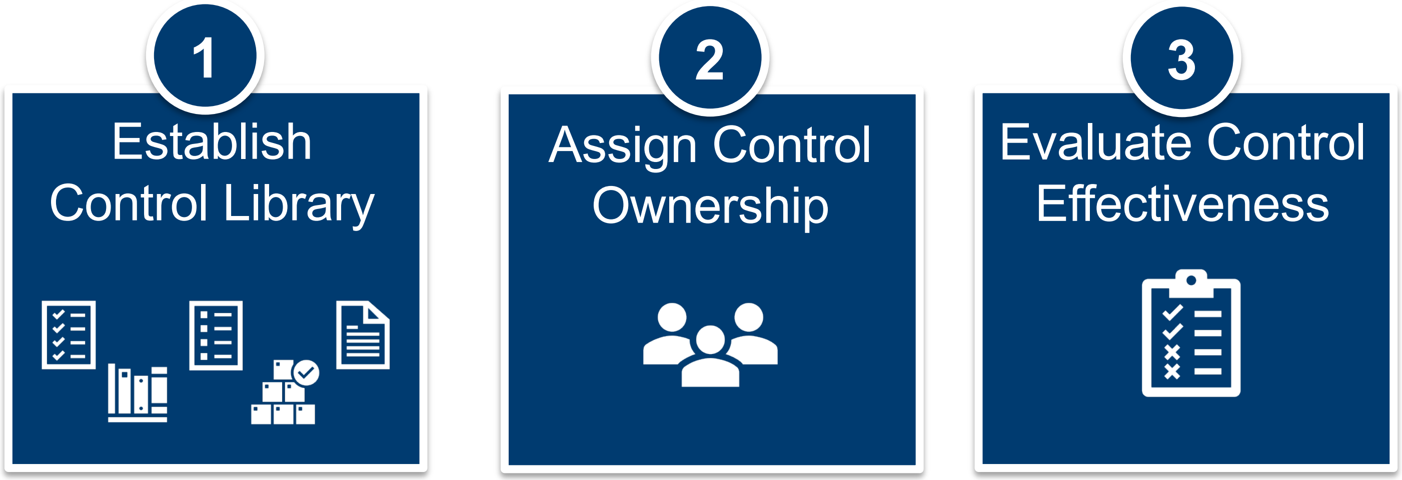
1 Establish Control Library

202 Identified Controls

2 Assign Control Ownership

Step 4: Evaluate Holistic Control Effectiveness



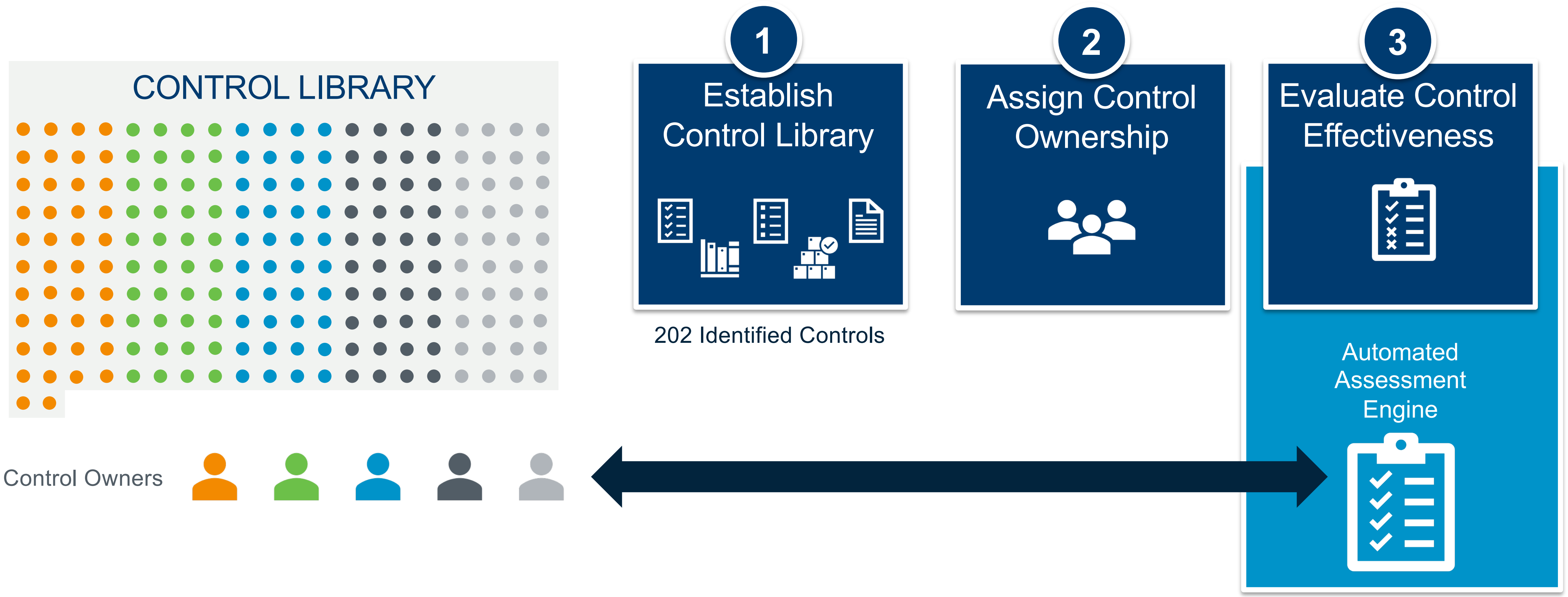

1 Establish Control Library

2 Assign Control Ownership

3 Evaluate Control Effectiveness

202 Identified Controls

Step 4: Evaluate Holistic Control Effectiveness



CONTROL LIBRARY

1 Establish Control Library

202 Identified Controls

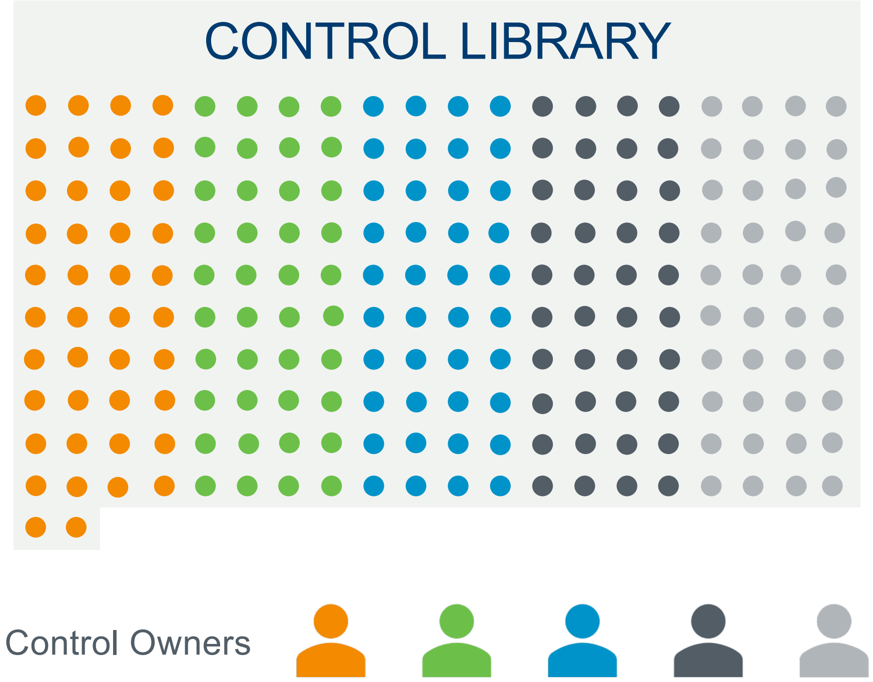
2 Assign Control Ownership

3 Evaluate Control Effectiveness

Automated Assessment Engine

Control Owners

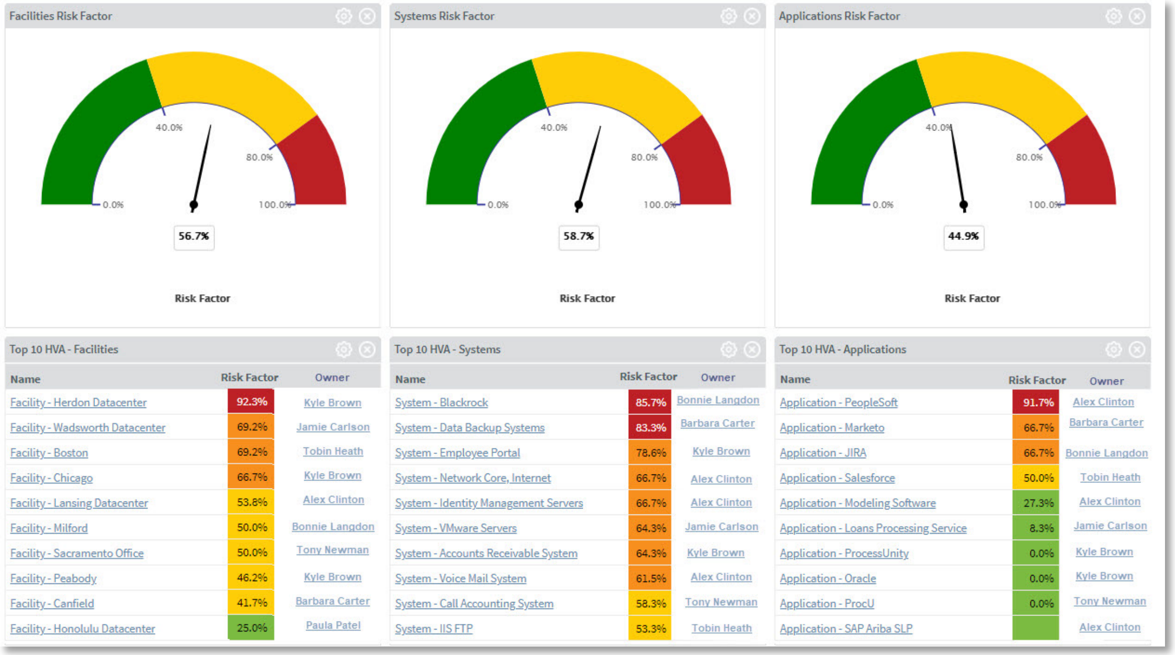
Step 4: Evaluate Holistic Control Effectiveness



CONTROL LIBRARY

Control Owners

Control Effectiveness Reporting



Top 10 HVA - Facilities

Name	Risk Factor	Owner
Facility - Herdon Datacenter	92.3%	Kyle Brown
Facility - Wadsworth Datacenter	69.2%	Jamie Carlson
Facility - Boston	69.2%	Tobin Heath
Facility - Chicago	66.7%	Kyle Brown
Facility - Lansing Datacenter	53.8%	Alex Clinton
Facility - Milford	50.0%	Bonnie Langdon
Facility - Sacramento Office	50.0%	Tony Newman
Facility - Peabody	46.2%	Kyle Brown
Facility - Canfield	41.7%	Barbara Carter
Facility - Honolulu Datacenter	25.0%	Paula Patel

Top 10 HVA - Systems

Name	Risk Factor	Owner
System - Blackrock	85.7%	Bonnie Langdon
System - Data Backup Systems	83.3%	Barbara Carter
System - Employee Portal	78.6%	Kyle Brown
System - Network Core, Internet	66.7%	Alex Clinton
System - Identity Management Servers	66.7%	Alex Clinton
System - VMware Servers	64.3%	Jamie Carlson
System - Accounts Receivable System	64.3%	Kyle Brown
System - Voice Mail System	61.5%	Alex Clinton
System - Call Accounting System	58.3%	Tony Newman
System - IIS FTP	53.3%	Tobin Heath

Top 10 HVA - Applications

Name	Risk Factor	Owner
Application - PeopleSoft	91.7%	Alex Clinton
Application - Marketo	66.7%	Barbara Carter
Application - JIRA	66.7%	Bonnie Langdon
Application - Salesforce	50.0%	Tobin Heath
Application - Modeling Software	27.3%	Alex Clinton
Application - Loans Processing Service	8.3%	Jamie Carlson
Application - ProcessUnity	0.0%	Kyle Brown
Application - Oracle	0.0%	Kyle Brown
Application - ProcU	0.0%	Tony Newman
Application - SAP Ariba SLP		Alex Clinton

Identify External Influence on Your Controls

Leverage third-party due-diligence response to more effectively evaluate YOUR controls

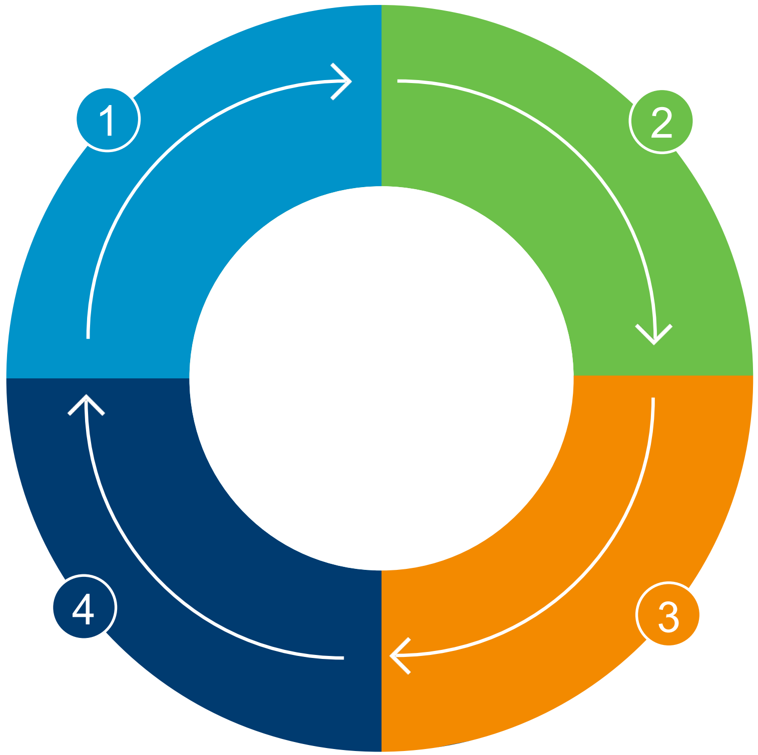
- GOV-01 – Security & Privacy Governance Program
  Does the organization staff a function to centrally-govern cybersecurity and privacy controls?

5 – Continuously Improving
4 – Quantitatively Controlled
3 – Well-Defined
2 – Planned & Tracked
1 – Performed Informally
0 – Not Performed

THIRD PARTY	RATING
ACME Services	4
~~Rogers Appraisals~~	
Golden Products	2
Weatherly Services Inc.	3
Systems Deluxe	0
External Control Effectiveness	**2.25**

Remediate Security Gaps / Patch Control Structure

IDENTIFY CONTROL GAPS & IMPROVE DOMAIN EFFICIENCIES IN YOUR PROGRAM



Assess

Assess all controls in program

Analyze

Analyze trends and patterns in domain level effectiveness

Plan

Plan projects to improve domain controls

Remediate

Prioritize, budget and execute project

Effectiveness Rating Analysis

DOMAIN	C	T	P
Control 1	2	3	3
Control 2	1	3	3
Control 3	3	3	4
AVG	**2.00**	**3.00**	**3.33**

C – Current | T – Target | P – Planned

The ProcessUnity Platform to Defend Against Internal and External Risk

Cyber Benefit

- Easily identify and remediate security gaps
- Prioritize security investments
- Continuously improve controls
- Deliver at-a-glance security summaries

Business Benefit

- Reduce the time and cost of risk reduction
- Increase customer, partner and stakeholder confidence
- Reduce reactionary spend
- Scale with business growth

Procurement Benefit

- Reduce onboarding and assessment cycle times
- Get secure products and services to the business faster
- Assess vendors against internal cybersecurity standards

For More Information

Automate Your Third-Party Risk Management Program:

www.processunity.com/automate

Forrester Report Evaluates Top TPRM Tools:

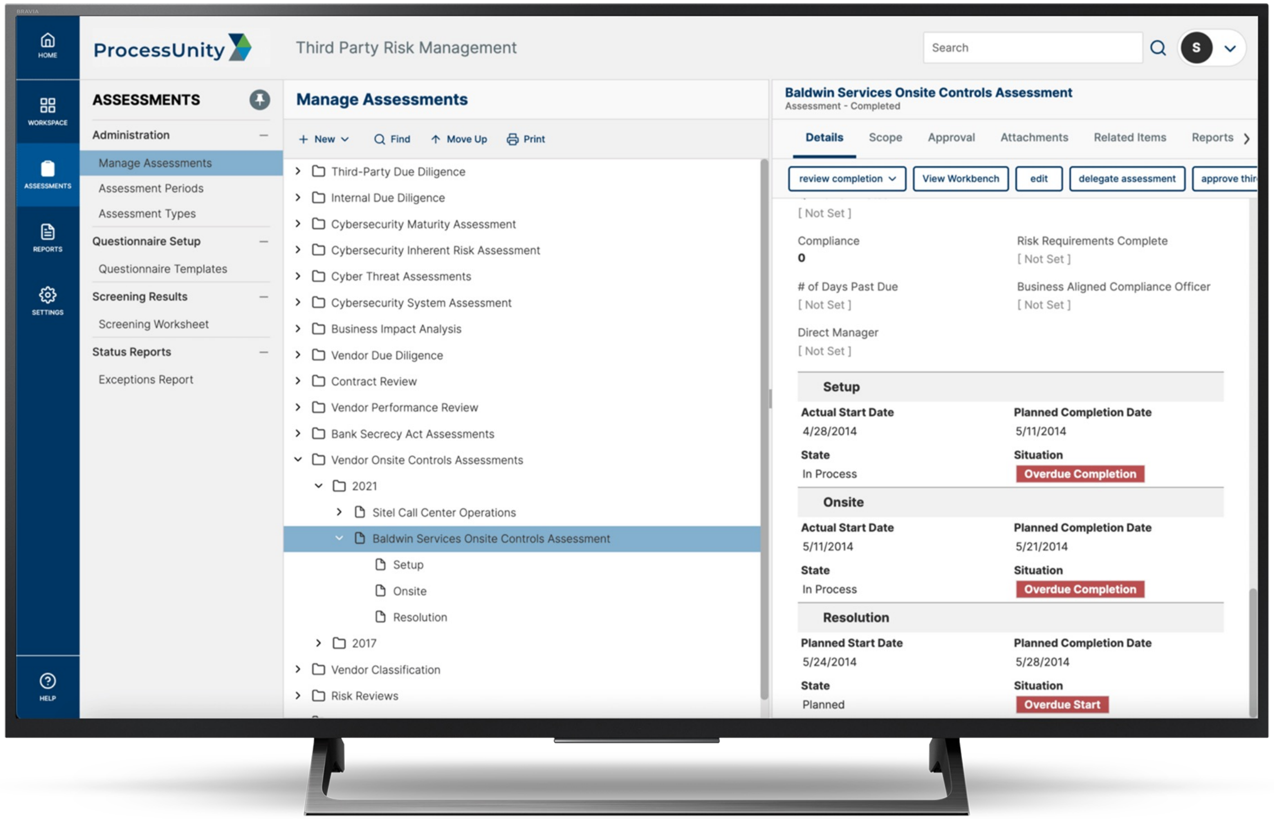
www.processunity.com/forrester

Contact ProcessUnity:

www.processunity.com/contact

Contact Brad:

brad.mcadams@processunity.com



Third Party Risk Management

ASSESSMENTS

- **Administration**
  - Manage Assessments
  - Assessment Periods
  - Assessment Types
- **Questionnaire Setup**
  - Questionnaire Templates
- **Screening Results**
  - Screening Worksheet
- **Status Reports**
  - Exceptions Report

Manage Assessments

- Third-Party Due Diligence
- Internal Due Diligence
- Cybersecurity Maturity Assessment
- Cybersecurity Inherent Risk Assessment
- Cyber Threat Assessments
- Cybersecurity System Assessment
- Business Impact Analysis
- Vendor Due Diligence
- Contract Review
- Vendor Performance Review
- Bank Secrecy Act Assessments
- Vendor Onsite Controls Assessments
  - 2021
    - Sitel Call Center Operations
    - Baldwin Services Onsite Controls Assessment
      - Setup
      - Onsite
      - Resolution
  - 2017
- Vendor Classification
- Risk Reviews

Baldwin Services Onsite Controls Assessment
Assessment - Completed

[Not Set]

Compliance 0	Risk Requirements Complete [Not Set]
# of Days Past Due [Not Set]	Business Aligned Compliance Officer [Not Set]
Direct Manager [Not Set]	

Setup

Actual Start Date 4/28/2014	**Planned Completion Date** 5/11/2014
State In Process	**Situation** Overdue Completion

Onsite

Actual Start Date 5/11/2014	**Planned Completion Date** 5/21/2014
State In Process	**Situation** Overdue Completion

Resolution

Planned Start Date 5/24/2014	**Planned Completion Date** 5/28/2014
State Planned	**Situation** Overdue Start