#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PRV-W02**

Adaptive Assurance: Implementing an Automated Control Testing Program

David Carter

Manager, Cyber Risk Management
Delta Dental of California

Christie Gross

Manager, Cyber Risk Management
Delta Dental of California

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSA Conference2022

Value Proposition for Automated Control Testing

what problem are we solving

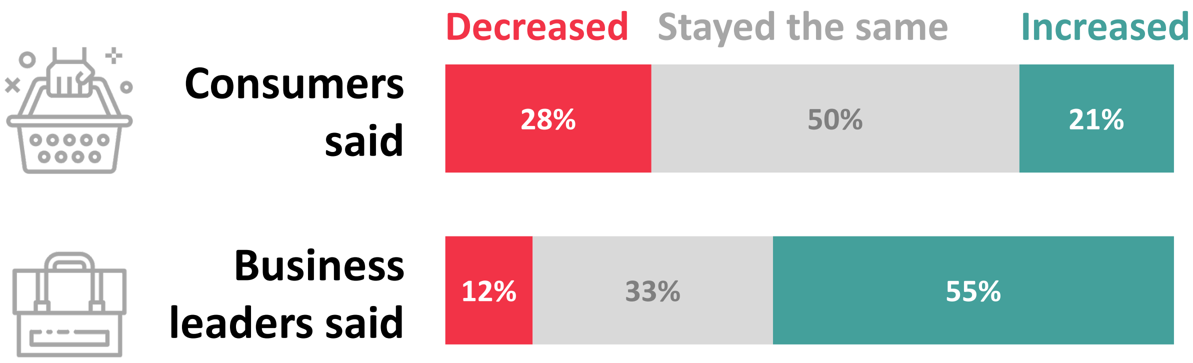
The Importance of Trust

Consumers want to do business with companies that are trustworthy custodians of their sensitive data; however, trust in companies' ability to protect data is declining and many business leaders are underestimating the gap.

85%

of global consumers "wish there were more companies I could trust with my data."

How has consumer trust in companies' ability to protect data over the past 2 years changed?



Pressure from customers, partners, regulators, and standards bodies is increasing the frequency and sophistication of technology assurance activities.

Source: PwC Consumer Intelligence Series: Trusted Tech Survey 2020

Effort as Proxy for Value

- Organizations operate hundreds of cyber risk controls across thousands of assets and spend significant time and money performing periodic manual tests to assure appropriate control performance.
- As the modern technology environment becomes more dynamic, manual testing is increasingly cost-ineffective and leaves windows between tests where controls may deviate from our risk tolerance.

Organizations across several industries are spending

more than 15,000 hours

completing cybersecurity assessments each year.

Despite that…

54%

of requestors say the data they get from assessments is **only somewhat valuable in decision making.**

55%

of organizations feel assessments are **not accurate reflections of their security posture.**

Source: Ponemon Cost of Third-Party Risk Management 2019

Effort ≠ Effectiveness

Inconsistent Measurement

Traditional testing methodologies rely on point-in-time observation, inquiry, or sampling, which fail to ensure sustained control effectiveness.

Doesn’t Scale Up

The adoption of new technology capabilities and increasing demand on resources to provide assurance of cyber risk management effectiveness requires progressively greater effort.

Poor Time to Detect

Manual assessment frequency leaves a window for potential concerns to go unnoticed.

Automated Control Testing

the solution

Creating an Automated Control Testing Program

An Automated Control Testing Program provides **timely detection of control failures, higher quality assurance of cyber controls, and improved resource utilization within assurance and control testing groups**.

Prioritize

Prioritizes regulatory and compliance requirements for automation

Define

Defines controls, control tests, and control effectiveness metrics for each requirement

Validate

Associates and ***validates*** organizational data sources and technologies

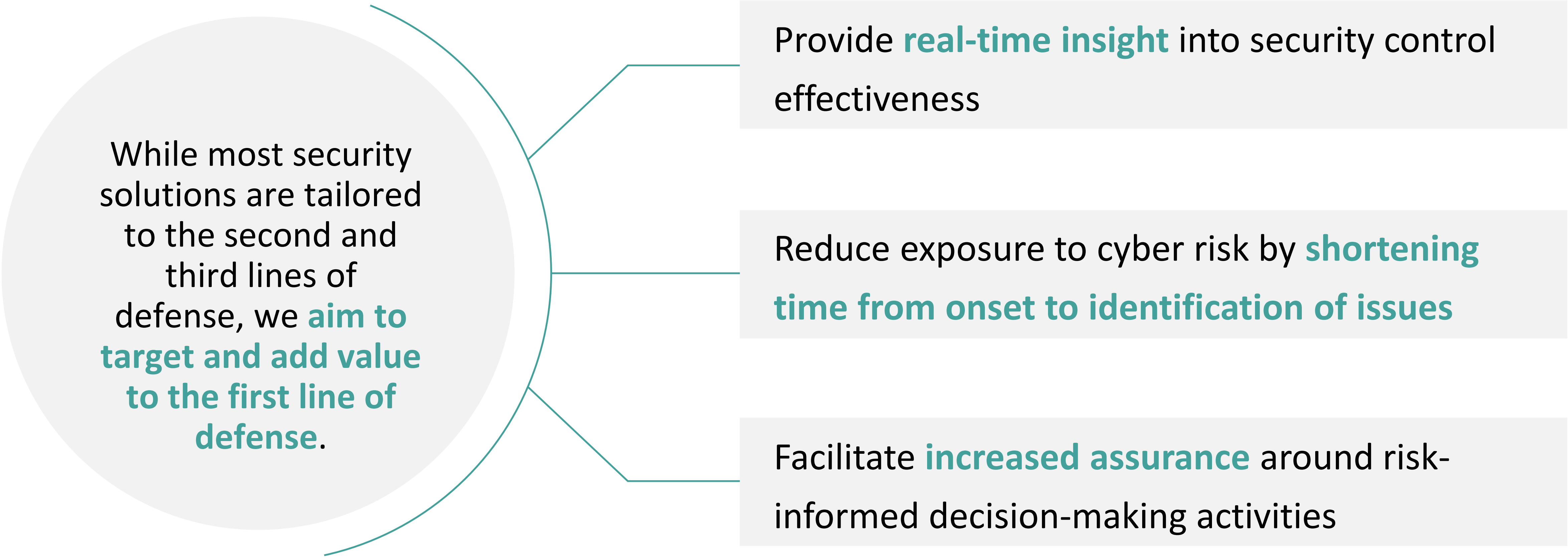
Implement

Implements automated tests to assess control effectiveness

Report

Reports at a consistent and higher frequency to increase cyber capability monitoring

Improving Effectiveness



While most security solutions are tailored to the second and third lines of defense, we **aim to target and add value to the first line of defense**.

Provide **real-time insight** into security control effectiveness

Reduce exposure to cyber risk by **shortening time from onset to identification of issues**

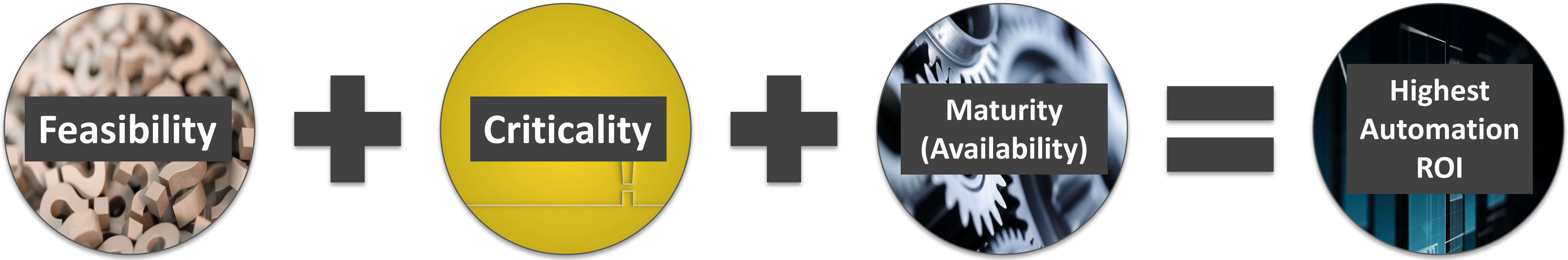
Facilitate **increased assurance** around risk-informed decision-making activities

RSAConference2022

Automated Control Testing Approach

an implementation case study

Prioritize – Identify Requirements



Feasibility + Criticality + Maturity (Availability) = Highest Automation ROI

Is it possible to automate some or all of the controls per requirement?
(Y/N and %)

Baseline Criticality Based on Requirement Found in Major Industry Standards
(VH=4, H=3, M=2, L=1)

Automation Complexity (Based on control maturity, internal assessment information)
(Low, Moderate, High)

Prioritize ● Define ○ Validate ○ Implement ○ Report ○

Prioritize – Decompose Requirements

ID	Requirement Name	Requirement Abstraction	Requirement Details
SI-03	Malicious Code Protection	The organization implements malicious code protections for systems, assets, and data	The organization: 1. Must define and document a policy and procedures addressing malicious code protection 2. Must implement malicious code protection mechanisms on all systems commonly affected by malicious software 3. Must implement malicious code protection mechanisms at key system entry and exit points 4. Must document any assets or system entry and exit points without malicious code protection and a threat-based rationale if any such assets exist 5. Implemented malicious code protection mechanisms must detect and eradicate malicious code 6. Must update malicious code protection mechanisms whenever new releases are available 7. Must configure malicious code protection mechanisms to: - Perform periodic scans of assets and key system entry and exit points - Real-time scans of files from external sources at key endpoint or network entry/exit points as files are downloaded, opened, or executed - Block or quarantine malicious code when it is detected - Be unable to be disabled by non-malicious code protection personnel excepting for short term exceptions 8. Must log and/or alert malicious code protection personnel in response to malicious code detection 9. Must address the receipt of false positives during malicious code detection and eradication and resulting potential impact on the availability of key systems

Prioritize ● — **Define** ○ — **Validate** ○ — **Implement** ○ — **Report** ○

Define - Controls & Effectiveness Metrics

The control and data source is **the organization's anti-malware solution** (e.g., Symantec) installed for in-scope systems and operating effectively.

Metric Type	Metric Description	Requirement Mapping
Coverage	Is the control installed (present on disk) on at least 90% of the in-scope population?	SI-03 – 2, 3, 4
Availability	Is the control operating (running in memory) on at least 90% of the in-scope population?	SI-03 – 5
Recency	Are 90% of assets of the in-scope population updating normally (are agents running updated software/definitions/heuristics)?	SI-03 – 6
Effectiveness	Are control configurations compliant with the expected standard? Are 90% of quarantine/blocking alert volumes within the tolerance zone?	SI-03 – 7
Exceptions	How many assets are exempt from coverage?	

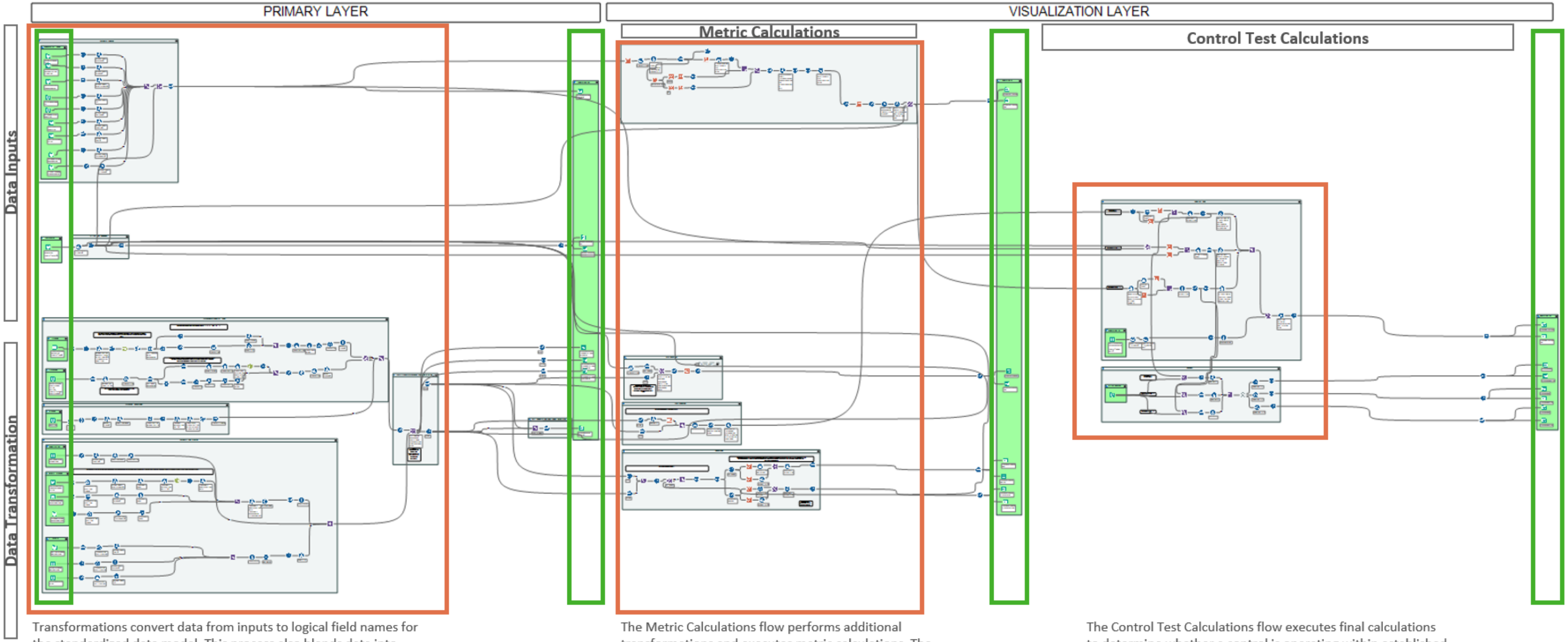
Validate – Inspect Data & Fill Gaps

Items in the green boundary are input data files from technology solutions. During the automation process, these will migrate from data extracts to API pulls.

Items in the green boundary are outputs from the Primary Layer. These Primary Layer outputs are currently exported to a shared drive as flat files.

Items in the green boundary are outputs from the Metric Calculations flow in the Visualization Layer. These outputs are currently exported to a shared drive as flat files and feed into dashboards.

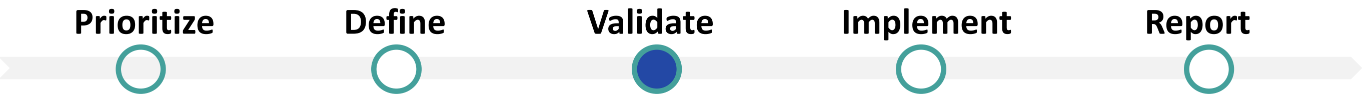
Items in the green boundary are outputs from the Control Test Calculations flow in the Visualization Layer. These outputs are currently exported to a shared drive as flat files and feed into dashboards.



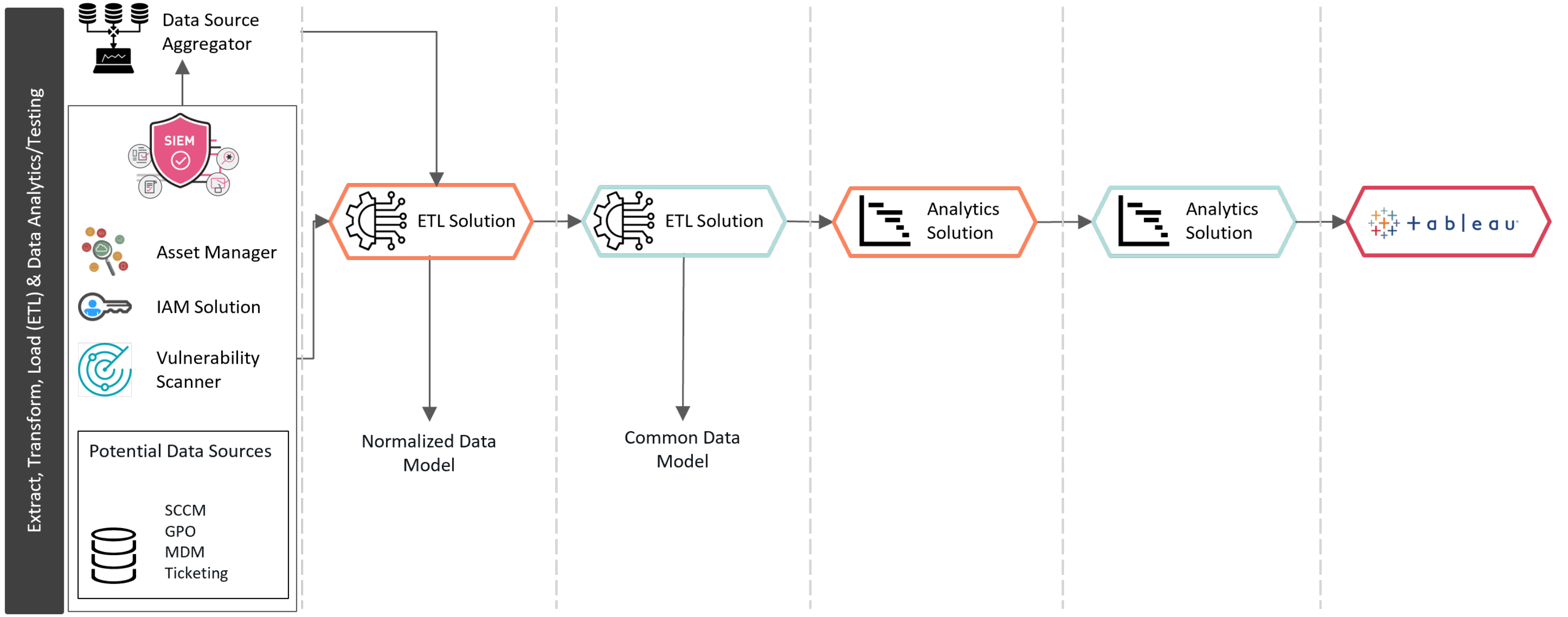
Transformations convert data from inputs to logical field names for the standardized data model. This process also blends data into data sets required to execute metric calculations.

The Metric Calculations flow performs additional transformations and executes metric calculations. The workflow also ties calculations to corresponding metrics.

The Control Test Calculations flow executes final calculations to determine whether a control is operating within established effectiveness boundaries (meets or does not meet).



Implement – Construct Solution Stack



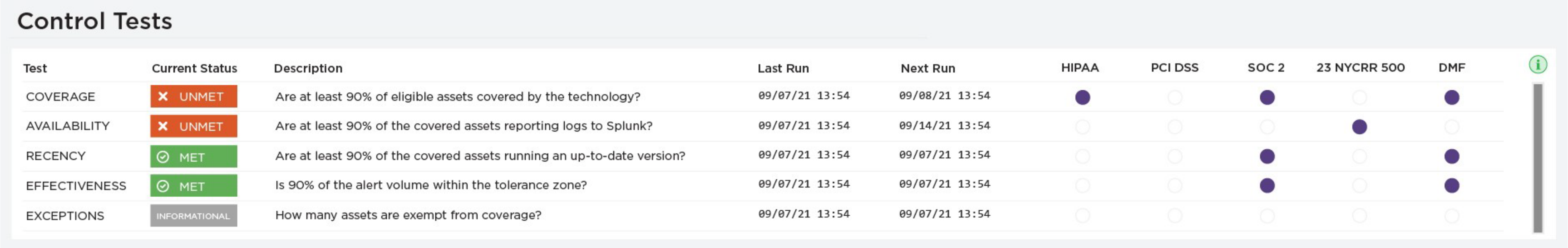
	Data Sources	Extract & Transform – Primary Layer	Load – Primary Layer	Analytics – Visualization Layer	Load – Visualization Layer	Dashboards
Notes	Direct tool connections to Data Source Aggregator or ETL solutions (API, Adapters, etc.) Input files to ETL solutions	Extract and transform data (and reference tables) into ETL solutions to create master tables	Load master datasets into primary layer (ETL solutions)	Perform data analysis and execute control testing (transform data to support metrics for visual outputs)	Load datasets into visualization layer (ETL solutions)	Load datasets from visualization layer into dashboard solution

Prerequisite Tasks

- ❑ Set up primary and visualization layers using ETL solutions
- ❑ Get read access to initial primary data sources & APIs
- ❑ Install stack technologies
- ❑ Set up stack infrastructure
- ❑ Configure adapter connections to data sources
- ❑ Set up data pipelines using ETL solutions
- ❑ Connect dashboard solution to data pipelines and export methods
- ❑ Test and troubleshoot

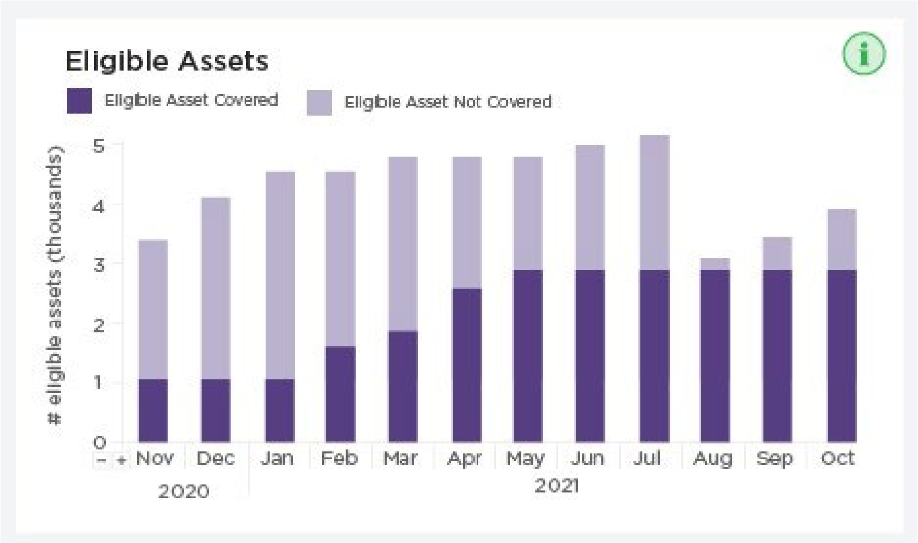
Prioritize ○ Define ○ Validate ○ Implement ● Report ○

Report – Drive Action

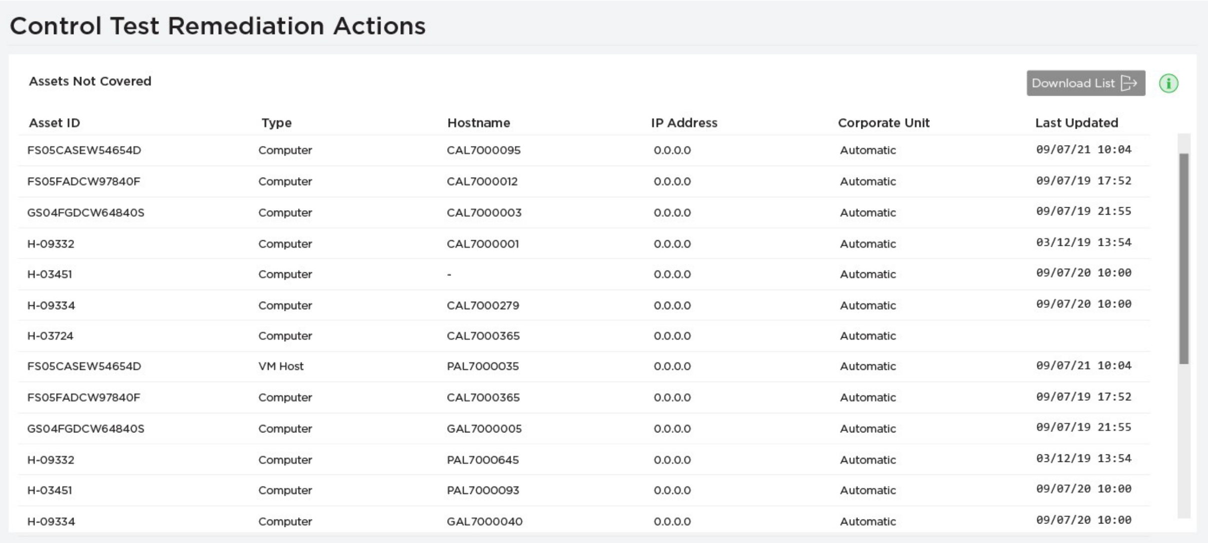


Control Tests

Test	Current Status	Description	Last Run	Next Run	HIPAA	PCI DSS	SOC 2	23 NYCRR 500	DMF
COVERAGE	✕ UNMET	Are at least 90% of eligible assets covered by the technology?	09/07/21 13:54	09/08/21 13:54	●	○	●	○	●
AVAILABILITY	✕ UNMET	Are at least 90% of the covered assets reporting logs to Splunk?	09/07/21 13:54	09/14/21 13:54	○	○	○	●	○
RECENCY	✓ MET	Are at least 90% of the covered assets running an up-to-date version?	09/07/21 13:54	09/07/21 13:54	○	○	●	○	●
EFFECTIVENESS	✓ MET	Is 90% of the alert volume within the tolerance zone?	09/07/21 13:54	09/07/21 13:54	○	○	●	○	●
EXCEPTIONS	INFORMATIONAL	How many assets are exempt from coverage?	09/07/21 13:54	09/07/21 13:54	○	○	○	○	○



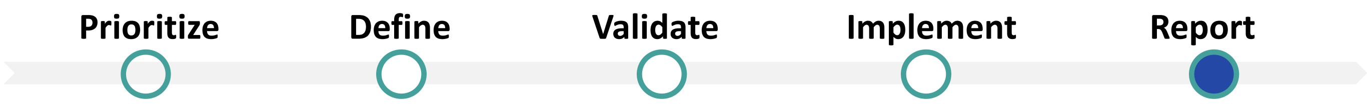
Eligible Assets



Control Test Remediation Actions

Assets Not Covered

Asset ID	Type	Hostname	IP Address	Corporate Unit	Last Updated
FS05CASEW54654D	Computer	CAL7000095	0.0.0.0	Automatic	09/07/21 10:04
FS05FADCW97840F	Computer	CAL7000012	0.0.0.0	Automatic	09/07/19 17:52
GS04FGDCW64840S	Computer	CAL7000003	0.0.0.0	Automatic	09/07/19 21:55
H-09332	Computer	CAL7000001	0.0.0.0	Automatic	03/12/19 13:54
H-03451	Computer	-	0.0.0.0	Automatic	09/07/20 10:00
H-09334	Computer	CAL7000279	0.0.0.0	Automatic	09/07/20 10:00
H-03724	Computer	CAL7000365	0.0.0.0	Automatic	
FS05CASEW54654D	VM Host	PAL7000035	0.0.0.0	Automatic	09/07/21 10:04
FS05FADCW97840F	Computer	CAL7000365	0.0.0.0	Automatic	09/07/19 17:52
GS04FGDCW64840S	Computer	GAL7000005	0.0.0.0	Automatic	09/07/19 21:55
H-09332	Computer	PAL7000645	0.0.0.0	Automatic	03/12/19 13:54
H-03451	Computer	PAL7000093	0.0.0.0	Automatic	09/07/20 10:00
H-09334	Computer	GAL7000040	0.0.0.0	Automatic	09/07/20 10:00



Prioritize ○ Define ○ Validate ○ Implement ○ Report ●

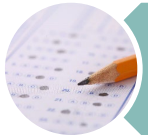
Quick Start Guide to Automated Control Testing

Take initial steps to foster buy-in with applicable use-cases and proof-of-concepts

Prioritize high value requirements among regulatory & compliance frameworks

Define effectiveness metrics, controls, and control tests

Validate data sources, establish populations, and fill data gaps



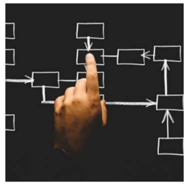
Establish solution stack and run control tests

Create reports at multiple tiers to identify effectiveness

Apply What You Have Learned Today

Next Week

- Identify partners to foster buy-in
- Begin drafting approach to applicable use-cases and proof-of-concepts



First 3 Months

- Examine organizational compliance & regulatory frameworks
- Develop requirement prioritization approach
- Prioritize high value requirements

Within 6 Months

- Select the highest value requirement
- Define effectiveness metrics
- Identify controls
- Define control tests

RSAConference2022

Questions