

The background of the poster is a vibrant sunset over a beachfront in Miami. Palm trees are silhouetted against the colorful sky, and buildings are illuminated with warm lights. A large, stylized teal graphic element, resembling a network or data flow, is overlaid on the scene. The main text is contained within a white box with a teal border.

GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by **MetricStream**

EXPERIENCE

the Power of Connection

The logo for the GRC Summit 2023 is centered in the upper half of the image. It consists of the letters 'GRC' in a large, bold, teal font. Below this, the words 'SUMMIT 2023' are written in a smaller, black, sans-serif font. Underneath that, the location and dates 'MIAMI, JUNE 14 & 15' are listed in the same black font. At the bottom of the logo, it says 'Hosted by MetricStream' in a smaller black font. The entire logo is enclosed in a white square with a thin black border, which is itself set within a larger, slightly offset teal square border.

GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by **MetricStream**

The background of the slide is a photograph of a beach at sunset. The sky is filled with vibrant colors of orange, pink, and purple. In the foreground, there are several palm trees silhouetted against the bright sky. In the middle ground, there are buildings with colorful neon lights in shades of blue, pink, and orange. The overall atmosphere is tropical and lively.


Cyber Risk and Compliance

Presented by MetricStream Product Management

Agenda

- Introduction
- CyberGRC – 5 Mins
- Automated control testing – 5 mins
- Dynamic Risk Assessment – 5 mins
- New UI UX – 5 Mins
- Q & A – 5 Mins



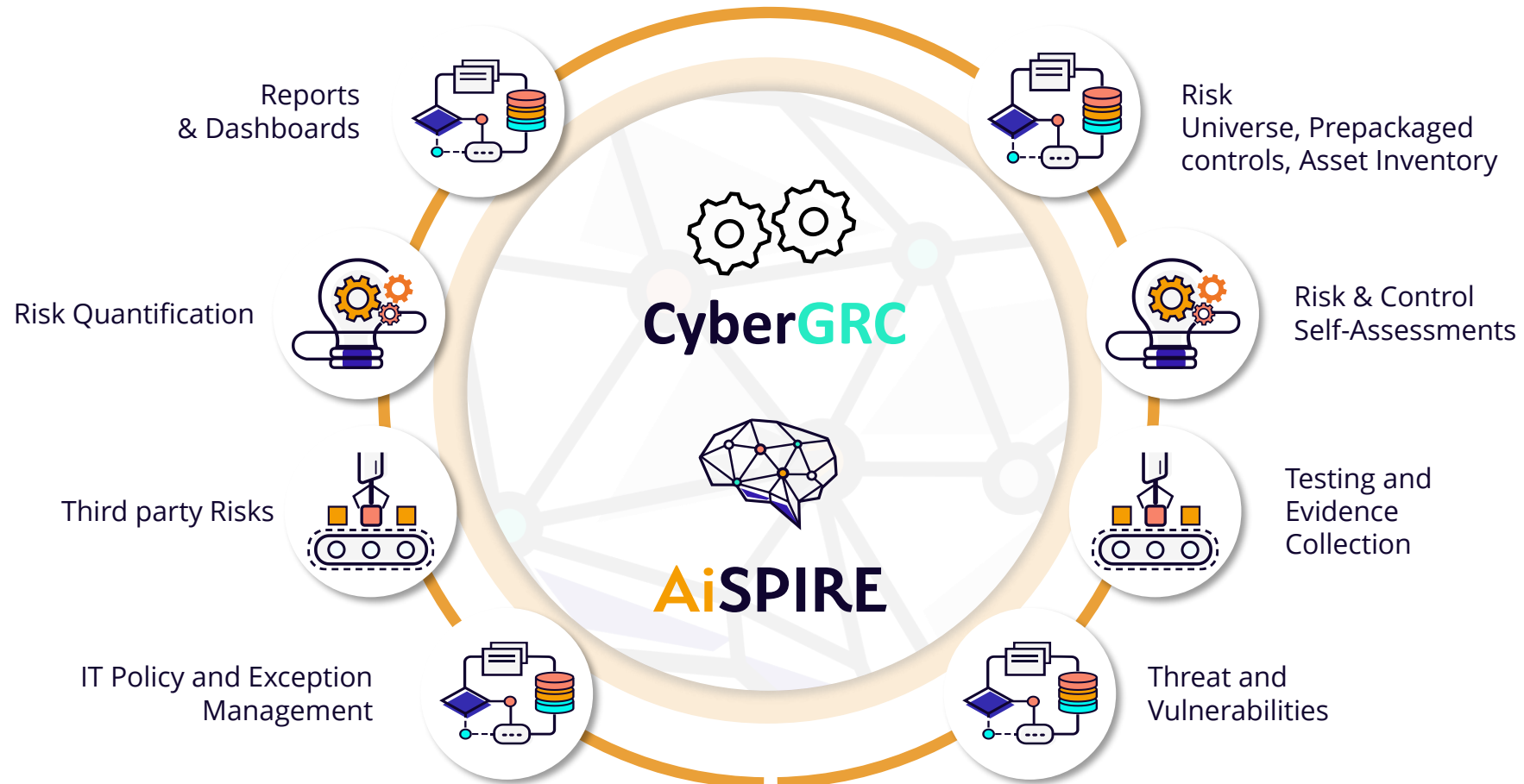
An aerial view of a city skyline at dusk, with a teal quote box overlaid on the image. The quote box contains the text: "Everyone passes audits, inspections, assessments & reviews – but the frequency and severity of security issues continue at record pace. Are we measuring risk effectively?". The quote is enclosed in a teal border with double teal quotation marks at the top left and bottom right corners. The background shows a dense urban landscape with many skyscrapers, some with lights on, and a few clouds in the sky.

“
Everyone passes audits, inspections,
assessments & reviews – but the
frequency and severity of security issues
continue at record pace. Are we
measuring risk effectively?
”

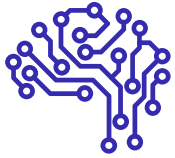
**Joe Martinez, CISO,
AON**

MetricStream CyberGRC

AI Powered Risk and compliance management



Future of GRC is **CONNECTED**



COGNITIVE

From Data to Decision Making

- *Understanding, Reasoning & Learning*
- *AI Infused Workflows & Decision Making*
- *Risk Quantification*



CONTINUOUS

From Workflows to Hyper Automation

- *Continuous Control Monitoring*
- *Continuous Audits & Assessments*
- *Content Integrations*



CLOUD

Next level of Simplicity

- *On-Demand, Self-Service and Secure*
- *Rapid Elasticity and Scalability*
- *Low-Code / No-Code SaaS Platform*

The logo for the GRC Summit 2023, featuring the letters 'GRC' in a large, bold, teal font. The background of the slide is a photograph of a modern building at dusk, with palm trees in the foreground and colorful neon lights (blue, red, purple) illuminating the scene. A decorative teal wave graphic with thin white lines runs across the top of the image.

GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

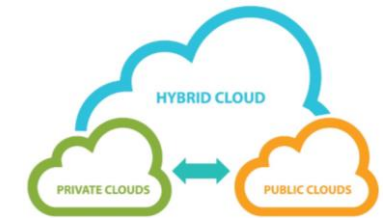
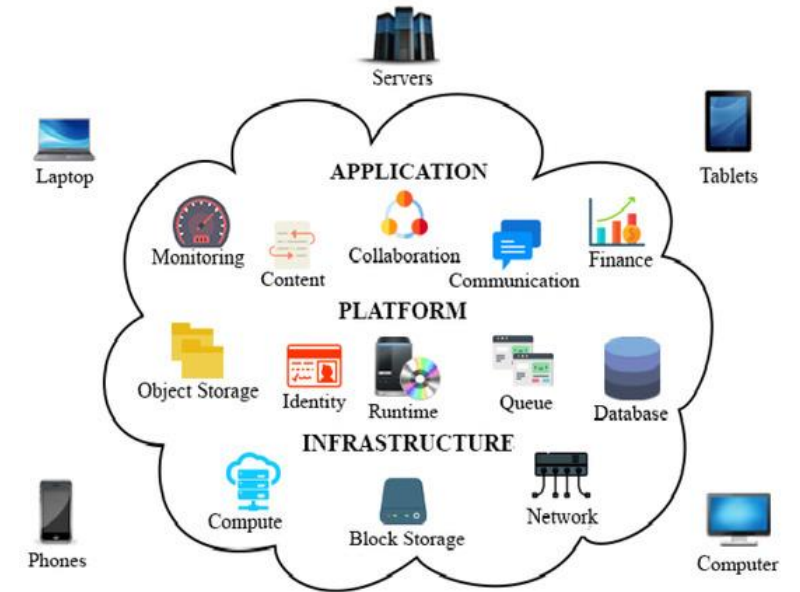
Hosted by MetricStream

EXPERIENCE
the Power of Connection

Automated control Testing

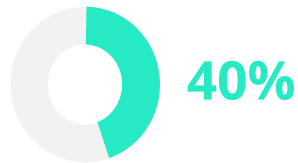
Complex Control Environment

- High number of process and applications handling sensitive data
- Multitude of cloud deployments and infrastructure elements
- Varied third-party providers
- Significant compliance requirements



Broad classification of controls

Area of applicability



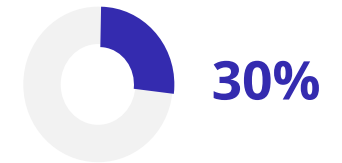
Infrastructure

- They help to protect the organizations infrastructure from a variety of threats, including unauthorized access, data breaches, and malware attacks.



Applications

- They are designed to protect specific applications from a variety of threats, including unauthorized access, data breaches, and malware attacks.



Policies and Procedures

- Policy and procedural controls are an important part of an organization's overall information security program.

Consolidated View of Control testing

➤ Integrated test results for GRC controls from Manual and Automated testing

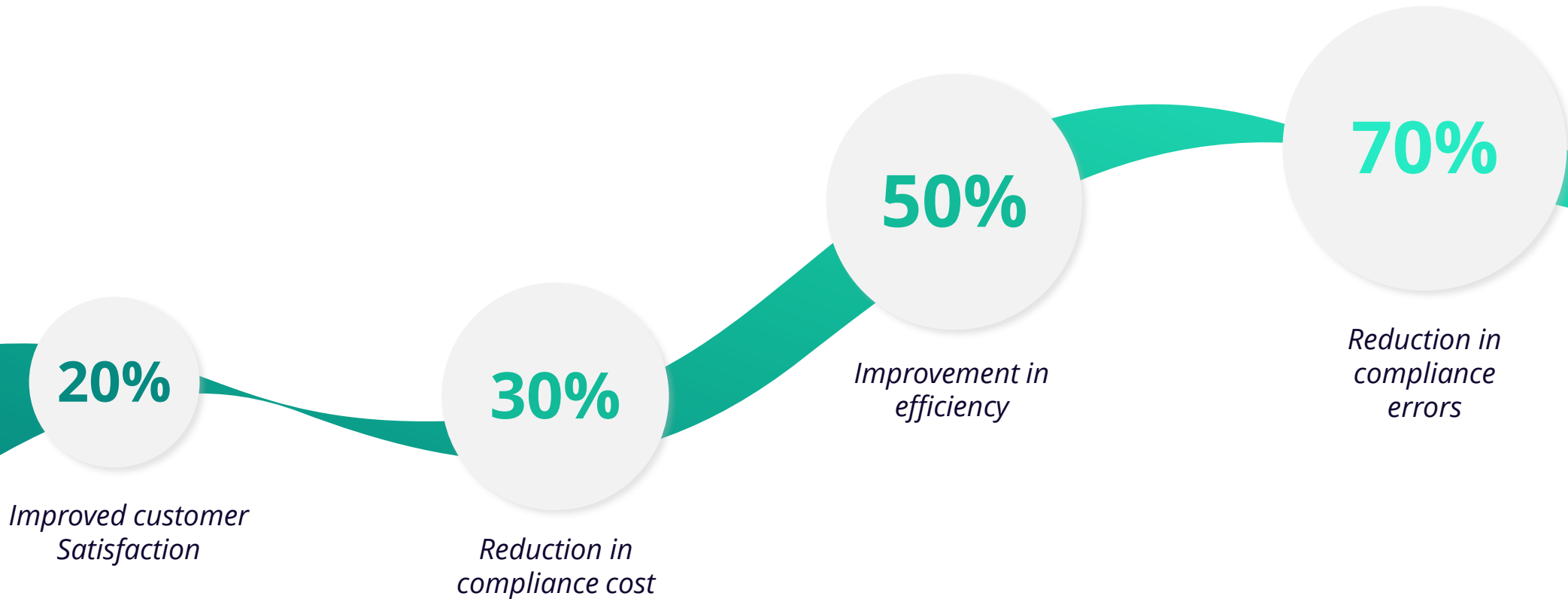
➤ Easy Access to evidences gathered across control testing

The screenshot displays a web application interface for 'IT COMPLIANCE CONTROL TESTING'. The interface includes a header with 'Saved Layout' and 'Last updated a few seconds ago'. Below the header is a 'Show Filters' section and an 'Options' menu. The main content is a table with columns: Control Name, Design Effectiveness, Operating Effectiveness, CCM Rating, # Rules, and Start Task. The table is divided into two sections: 'HIPAA Security Rule (10)' and 'PCI DSS v3.2.1 (14)'. Each row represents a control, with its status in the Design and Operating Effectiveness columns and its CCM Rating in the CCM Rating column. The # Rules column shows the number of rules associated with each control. The Start Task column contains a right-pointing arrow icon.

Control Name	Design Effectiveness	Operating Effectiveness	CCM Rating	# Rules	Start Task
AREA OF COMPLIANCE : HIPAA Security Rule (10)					
PM-15 Contacts With Security Groups And Associations	Designed Effectively	Operating Effectively	N/A		▶
PM-09 Risk Management Strategy	Designed Effectively	Operating Effectively	N/A	1	▶
RA-02 Security Categorization	Designed Effectively	Operating Effectively	N/A		▶
PM-02 Senior Information Security Officer			Passed		▶
PM-03 Information Security Resources			Failed		▶
PM-04 Plan Of Action And Milestones Process			Failed	1	▶
PM-05 Information System Inventory			Passed	1	▶
PM-06 Information Security Measures Of Performance	Designed Effectively	Operating Effectively	Failed	1	▶
PM-07 Enterprise Architecture	Not Designed Effectively	Not Operating Effectively	Failed	1	▶
PM-08 Critical Infrastructure Plan	Designed Effectively	Operating Effectively	N/A	1	▶
AREA OF COMPLIANCE : PCI DSS v3.2.1 (14)					
AC-10 Concurrent Session Control	Designed Effectively	Operating Effectively	N/A	2	▶
AC-25 Reference Monitor	Designed Effectively	Operating Effectively	N/A		▶
AC-24 Access Control Decisions			Failed	1	▶
AC-21 Information Sharing			Passed		▶
AC-03 Access Enforcement					▶

Page 1 of 9 Records Per Page: 20

Capturing automated compliance ROI





“ Compliance \neq Security ”

Compliance is necessary, but not sufficient to mitigate Cyber Risk

The logo for the GRC Summit 2023, featuring the letters 'GRC' in a bold, teal, sans-serif font. The background of the slide is a photograph of a modern building at dusk, with palm trees in the foreground and colorful neon lights (blue, red, and purple) illuminating the scene. A series of teal, wavy lines are overlaid on the image, connecting the various text elements.

GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

EXPERIENCE
the Power of Connection

Dynamic Risk Assessments

Asset Risk Score

What is dynamic risk assessment

Numerical representation (quantification) of risk to the asset

Continuous process to evaluate/assess the risk associated with an asset.

Constantly considers changing threat landscape and the assets environment.

Process steps

Steps



Identify Assets and source for Risk factors

- Identify IT Assets (sources could be vulnerability scanners, CMDB etc)
- Identify all the sources where risk information is available example Vulnerability scanners, Threat intelligence, Patch management systems



Define KRIs (Risk factors)

Define KPIs to use to determine the Asset Risk score.
Examples: No of exploited Vulnerabilities, Patching Status



Automate capturing Metrics using APIs

Tap into sources via API to collect metrics for KRIs



Algorithm Framework

Buildout simple Algorithm and equation to assign weightage for each source and calculate the asset risk score



Dynamic Dashboard to display asset risk score

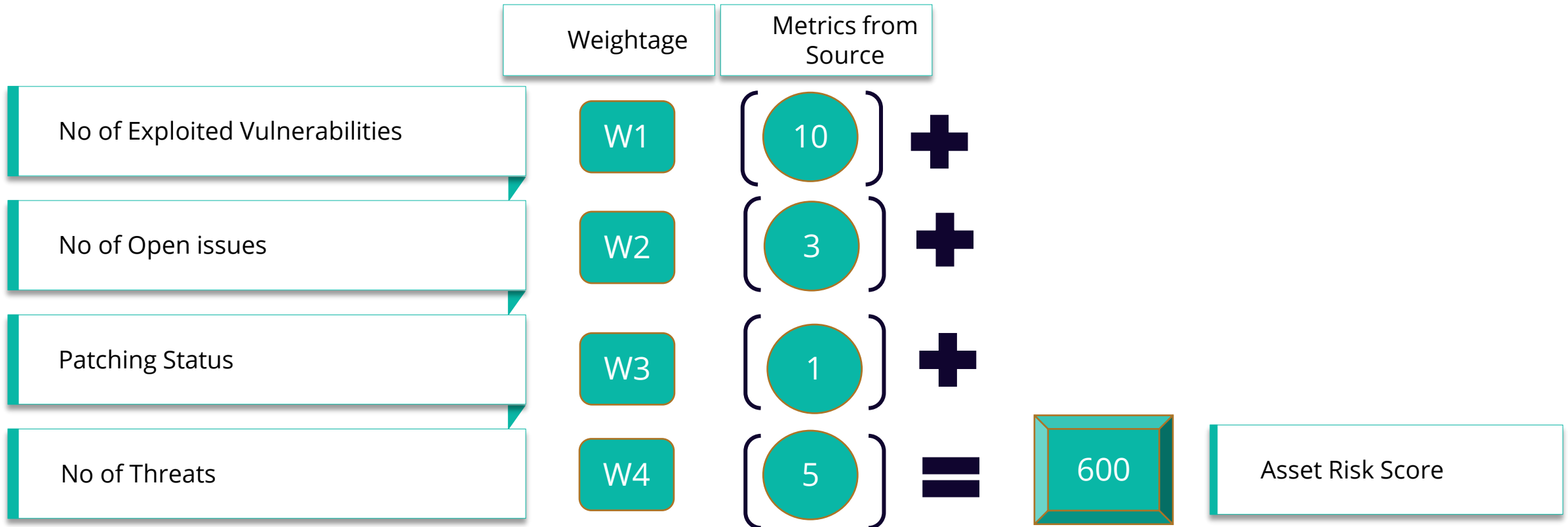
View the assets ordered by highest risk score to prioritize mitigation efforts.

Equation Example

Asset : Payroll Data Base

Business Criticality : High

Asset Value : \$\$\$\$



Asset Risk Score Dashboard

Dynamically updating Dashboard

Ordered by Asset Risk Score

Helps prioritize remediation actions

	Asset ID	Asset Name	Asset Owner	Type	Asset Class	Risk Score	Trend	Business Criticality
<input type="checkbox"/>	A-001	Apache Web Server	John. Doe	IP	Server	610	↑	Critical
<input type="checkbox"/>	A-002	Cisco Firewall	Mike Milton	IP	Firewall	540	↑	High
<input type="checkbox"/>	A-003	SQL Server 2019	Raymond James	IP	Server	510	↑	Medium
<input type="checkbox"/>	A-004	Office 365	John. Doe	IP	Office	480	↓	Critical
<input type="checkbox"/>	A-005	Laptop Dell X - M3149	Jane Smith	IP	Laptop	420	↓	Critical
<input type="checkbox"/>	A-006	Laptop Dell X - M3150	Jon Doe	IP	Laptop	380	↑	High
<input type="checkbox"/>	A-007	Laptop Dell X - M3152	Cindy Chan	IP	Laptop	360	↓	High
<input type="checkbox"/>	A-008	Laptop Dell X - M3154	Mike Morton	IP	Laptop	340	↓	High
<input type="checkbox"/>	A-009	Laptop Dell X - M3151	Sandra Sellers	IP	Laptop	320	↑	High
<input type="checkbox"/>	A-010	Laptop Dell X - M3155	John Doe1	IP	Laptop	310	↓	High
<input type="checkbox"/>	A-011	Laptop Dell X - M3157	Cindy Chan	IP	Laptop	180	↓	High
<input type="checkbox"/>	A-015	Laptop Dell X - M3156	Jane Smith	IP	Laptop	140	↑	Medium
<input type="checkbox"/>	A-014	Laptop Dell X - M3144	Mike Morton	IP	Laptop	140	↓	Medium

The background of the entire image is a vibrant sunset over a Miami skyline, featuring numerous palm trees and buildings illuminated with colorful lights (blue, red, purple). A series of glowing green lines arch across the top of the scene, connecting the event information on the left to the theme on the right.

GRC

SUMMIT 2023

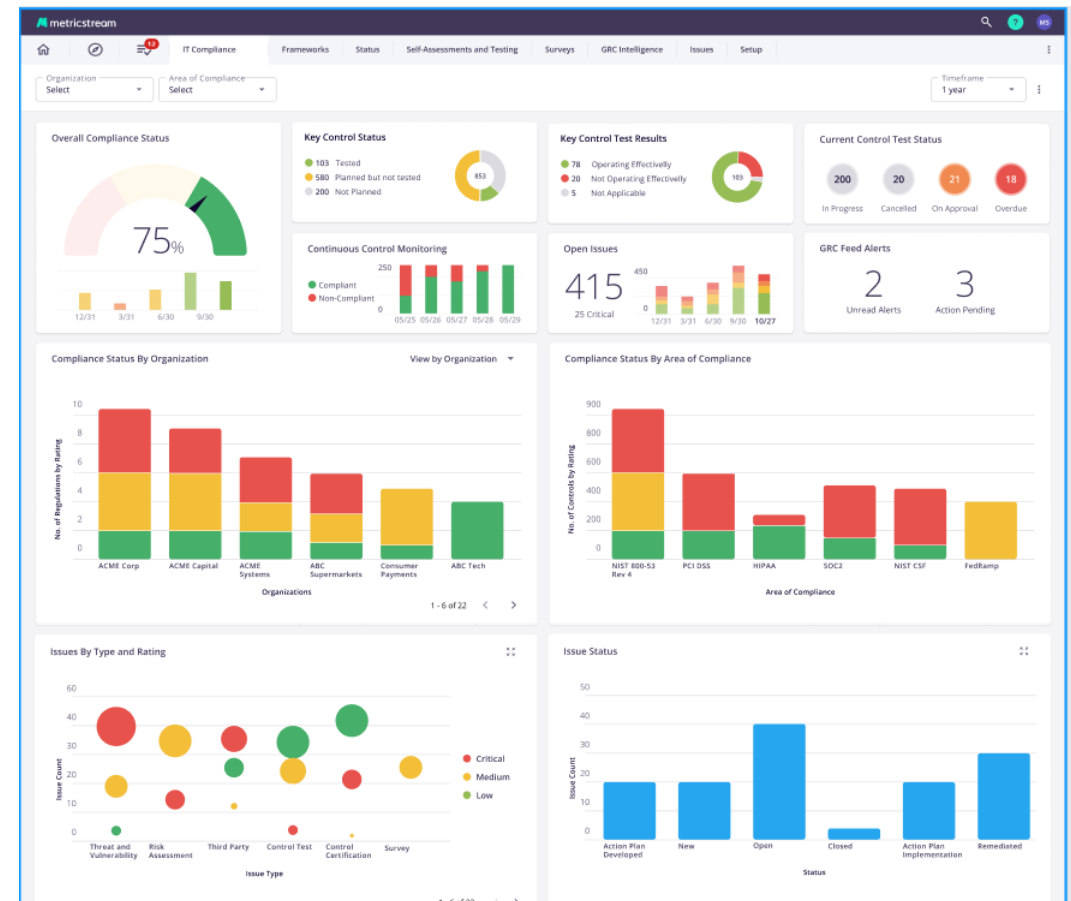
MIAMI, JUNE 14 & 15

Hosted by MetricStream

EXPERIENCE
the Power of Connection

UI UX

Improved Reports and Dashboards



Brand New Assessment Experience

Improved collaboration

New form layout seamlessly combines Tab convenience with section organization

Pinned contextual info where the left page offers contextual information

UX

The screenshot displays the MetricStream assessment interface. The top navigation bar includes the MetricStream logo, a search icon, and user profile icons. The main header shows the assessment title 'Custody of Fiduciary Assets -12 CFR 9.13' and buttons for 'SAVE' and 'SUBMIT'. The interface is divided into several sections:

- Stage 1 of 6:** A progress indicator showing the current stage.
- Owner:** Trevor McDonnell
- Key Control:** Yes
- Description:** A national bank shall place assets of fiduciary accounts in the joint custody or control of not fewer than 2 of the fiduciary officers or employees designated for that purpose by the Board of Directors. Assets of the fiduciary account shall be kept separate from the assets of the bank. Each fiduciary account shall be kept separate from all other accounts.
- Test Plan:** TP-0001
- Related Risks:** Credit Risk, Business Disruption and System Failures, Structured transactions risk, Frequent transactions in high risk loc...
- Checklist:** A section for tracking test progress.
- Design Effectiveness:** Not Rated
- Operational Effectiveness:** Not Rated
- TEST STEPS:** A summary table showing test statistics.
- Imported:** A list of imported test samples.
- Manually Added:** A table of manually added test results.

Expected Sample Size	Tested	Passed	Failed	Error
400	550	525	23	2

ID	Description	Result	Questions / Answered
1254621	Imperdiet eu conubia adipiscing vestibulum at a leo enim vestibulum dictumst taciti lobortis facilisi suspendisse ant...	Pass	10 / 3
1254621	Imperdiet eu conubia adipiscing vestibulum at a leo enim vestibulum dictumst taciti lobortis facilisi suspendisse ant...	Pass	10 / 3
1254621	Imperdiet eu conubia adipiscing vestibulum at a leo enim vestibulum dictumst taciti lobortis facilisi suspendisse ant...	Pass	10 / 3
974310	Imperdiet eu conubia adipiscing vestibulum at a leo enim vestibulum dictumst taciti lobortis facilisi suspendisse ant...	Fail	10 / 3
1254621	Imperdiet eu conubia adipiscing vestibulum at a leo enim vestibulum dictumst taciti lobortis facilisi suspendisse ant...	Pass	10 / 3

The logo for the GRC Summit 2023, featuring the letters 'GRC' in a bold, teal, sans-serif font. The background of the entire slide is a photograph of a modern building at dusk, with palm trees in the foreground and colorful neon lights (blue, red, purple) illuminating the scene. A decorative teal wave graphic with multiple parallel lines flows across the top of the image.

GRC

SUMMIT 2023

MIAMI, JUNE 14 & 15

Hosted by MetricStream

EXPERIENCE
the Power of Connection

Q & A