

The background of the image is a night-time photograph of the Tower Bridge in London. The bridge's two towers are illuminated with warm yellow lights, and the suspension cables are visible against the dark blue and purple twilight sky. The overall mood is professional and sophisticated.

# GRC

SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

# Experience the Power of Connection

---

The background of the slide is a photograph of the Tower Bridge in London at night. The bridge's two towers are illuminated with warm yellow lights, and the suspension cables are visible against the dark blue twilight sky. The overall scene is dimly lit, with the bridge's lights providing the primary illumination.

**GRC**

SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

# Safeguard your Digital Business

## With CyberGRC - Continuous Control Monitoring (CCM)



# CONNECTEDGRC

## BUSINESSGRC

- Enterprise / Operational Risk
- Operational Resilience
- Internal Audit
- SOX Compliance
- Business Continuity
- Third-party Risk
- Regulatory Compliance
- Policy Management
- Regulatory Change
- Regulatory Engagement
- Case & Incident

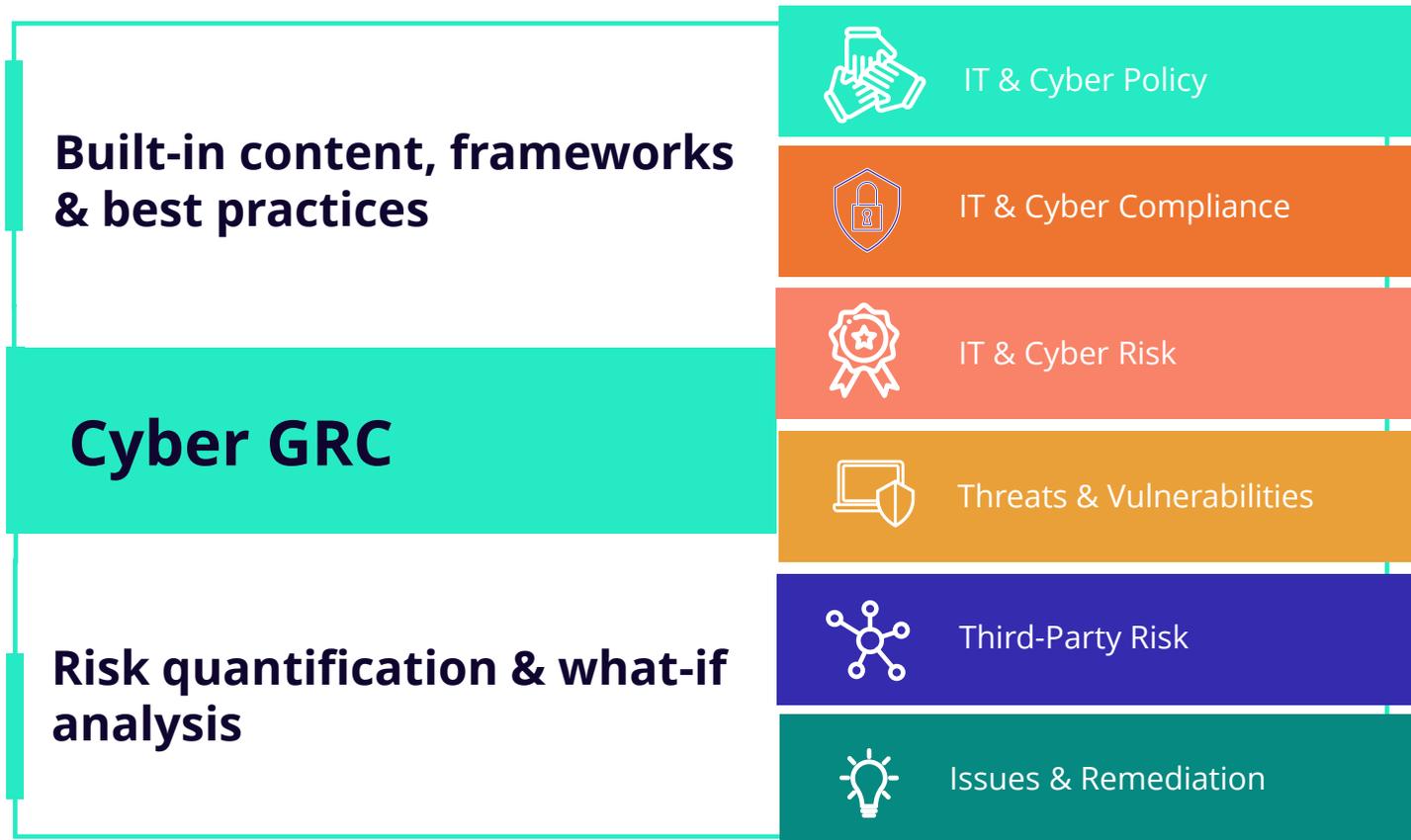
## CYBERGRC

- IT & Cyber Policy
- IT & Cyber Compliance
- IT & Cyber Risk
- IT Vendor Risk

## ESGRC

- Disclosure Reporting
- Metrics Management
- Assessments & Certifications

# MetricStream CyberGRC provides an end-to-end, connected solution



- Protect your organization from cyber risks and incidents
- Model and communicate real-time quantified IT & cyber risk exposure in monetary terms
- Prioritize risk mitigation efforts, investments and reduce residual risk
- Ensure compliance with multiple industry standards and requirements
- Reduce cost and improve efficiencies in your cyber security team

# Continuous Control Monitoring (CCM)

**Continuous controls monitoring** (CCM) is a set of technologies to reduce business losses through continuous monitoring and reducing the cost of audits through continuous auditing of the controls in financial and other transactional applications.



**Control Monitoring**



**Evidence Gathering**



**Assess Risk On Entire Population**



**End-to-End Control Testing**

# How CCM Benefits Your Business



# How CCM Works?



## Plug-in

The “**Plug-in Target Application**” will collect the Details needed to Get access to the Destination. It’s the server from where the application will fetch the Rules and Results of every asset.



## Relationships

The Rules/Controls that are automatically created can be related to other internal controls and/or requirements of other standards.



## Analytics

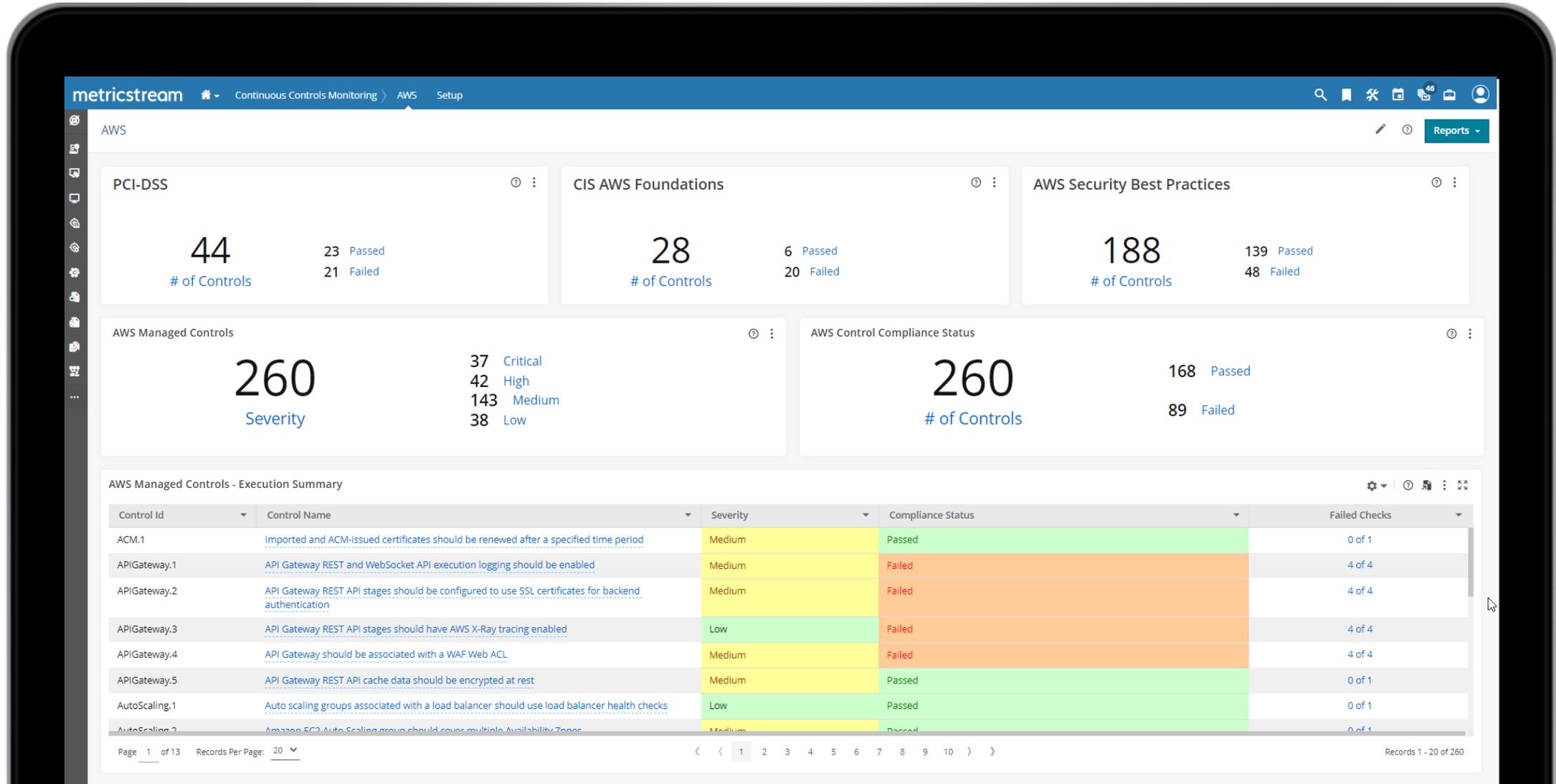
The “**Reports**” will reflect the results of the External Controls Compliance results. Also, with the relationships that are built out with internal libraries, the results can be reviewed against those relationships.





Demo

# Overview



# Execution Summary

The screenshot displays the AWS Managed Controls - Execution Summary dashboard. The interface includes a navigation bar with a back arrow, the title 'AWS MANAGED CONTROLS - EXECUTION SUMMARY', and a 'Saved Layout' dropdown. On the right, it shows 'Last updated a few seconds ago' and several utility icons (refresh, help, grid, print, etc.). Below the navigation bar, there are 'Show Filters' and 'Severity: Critical' filter options, along with 'Reset Filters' and 'Options' buttons. The main content is a table with the following columns: Control Id, Control Name, Severity, Compliance Status, and Failed Checks. The table lists 20 controls, with their respective severity levels, compliance statuses (Passed or Failed), and the number of failed checks out of the total number of checks for each control. The bottom of the dashboard shows 'Page 1 of 2', 'Records Per Page: 20', and navigation arrows for the table.

Control Id	Control Name	Severity	Compliance Status	Failed Checks
CIS.1.12	<a href="#">Ensure no root user access key exists</a>	Critical	Passed	0 of 1
CIS.1.13	<a href="#">Ensure MFA is enabled for the root user</a>	Critical	Passed	0 of 1
CIS.1.14	<a href="#">Ensure hardware MFA is enabled for the root user</a>	Critical	Failed	1 of 1
CIS.2.3	<a href="#">Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible</a>	Critical	Passed	0 of 1
CloudFront.1	<a href="#">CloudFront distributions should have a default root object configured</a>	Critical	Passed	0 of 1
CodeBuild.1	<a href="#">CodeBuild GitHub or Bitbucket source repository URLs should use OAuth</a>	Critical	Passed	0 of 1
CodeBuild.2	<a href="#">CodeBuild project environment variables should not contain clear text credentials</a>	Critical	Passed	0 of 1
DMS.1	<a href="#">Database Migration Service replication instances should not be public</a>	Critical	Passed	0 of 1
EC2.1	<a href="#">EBS snapshots should not be publicly restorable</a>	Critical	Passed	0 of 1
EC2.19	<a href="#">Security groups should not allow unrestricted access to ports with high risk</a>	Critical	Failed	3 of 6
ES.2	<a href="#">Elasticsearch domains should be in a VPC</a>	Critical	Passed	0 of 1
IAM.4	<a href="#">IAM root user access key should not exist</a>	Critical	Passed	0 of 1
IAM.6	<a href="#">Hardware MFA should be enabled for the root user</a>	Critical	Failed	1 of 1
KMS.3	<a href="#">AWS KMS keys should not be deleted unintentionally</a>	Critical	Passed	0 of 1
Lambda.1	<a href="#">Lambda function policies should prohibit public access</a>	Critical	Failed	1 of 54
Opensearch.2	<a href="#">OpenSearch domains should be in a VPC</a>	Critical	Passed	0 of 1
Opensearch.7	<a href="#">OpenSearch domains should have fine-grained access control enabled</a>	Critical	Passed	0 of 1
PCI.CodeBuild.1	<a href="#">CodeBuild GitHub or Bitbucket source repository URLs should use OAuth</a>	Critical	Passed	0 of 1

A night-time photograph of the Tower Bridge in London, illuminated with warm lights. The bridge's two towers and the suspension cables are visible against a dark blue sky. The bridge is reflected in the water below.

# GRC

SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

# Thank You

 **metricstream**  
thrive on risk™