

The background of the entire image is a photograph of the Tower Bridge in London at night. The bridge's two massive stone towers are illuminated with warm yellow lights, and the suspension cables are visible against the dark sky. The bridge deck is lit up, and the surrounding area is dimly lit, with some city lights visible in the distance.

GRC

SUMMIT 2022

LONDON, NOV 8-9

Hosted by **MetricStream**

Experience the Power of Connection

GRC

SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

AI for GRC



Raghu Srinivas, Ph.D.

SVP, Head of Product Management
& Innovations

M metricstream



Tom Rutkowski, Ph.D., MBA
MD, Head of Artificial Intelligence

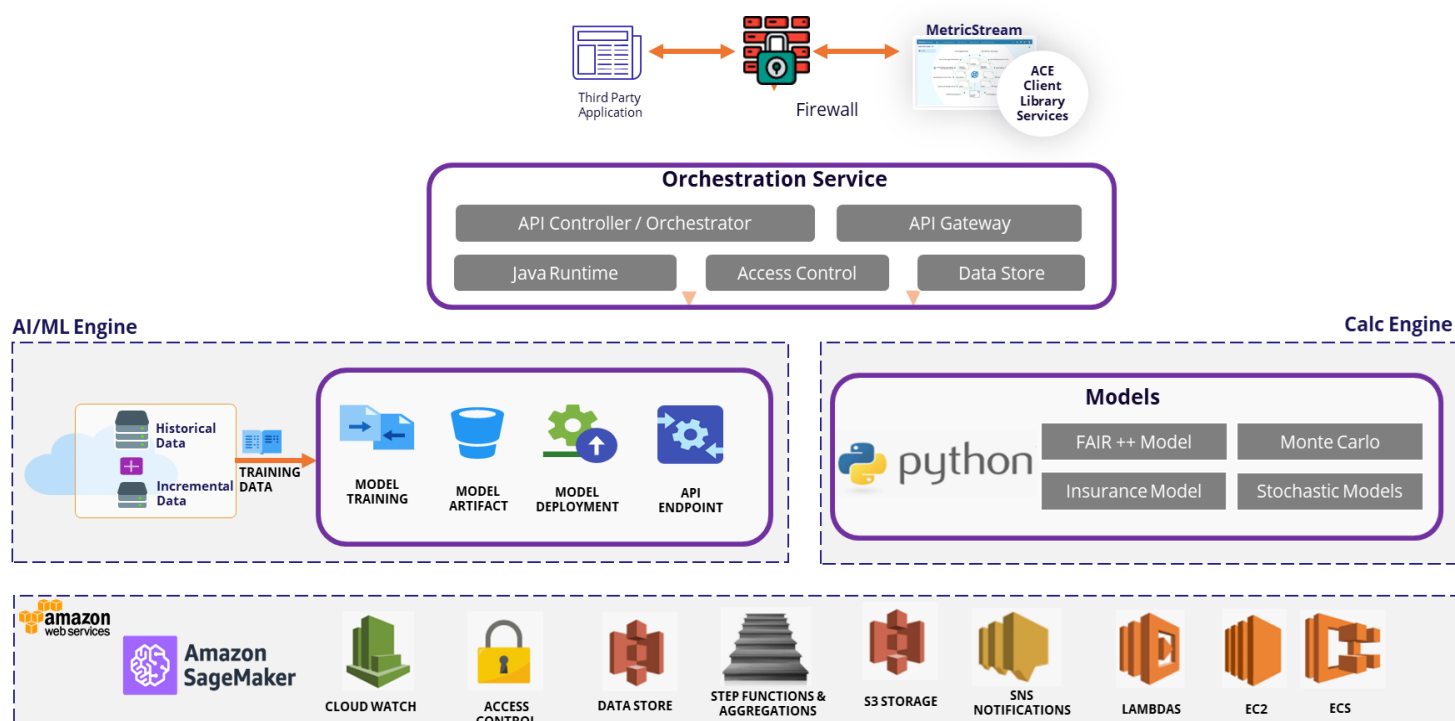
KINETIX



Kinetix delivers explainable Artificial Intelligence products for Banking and Capital Markets. At Kinetix we use a unique approach to identifying Artificial Intelligence use cases called Impactful AI. Based on an outcome from workshops, we customize and configure Kinetix Vi – a data and AI platform - to improve business processes spanning from identifying investment opportunities to streamlining trade management to improving regulatory reporting.



MetricStream Intelligence

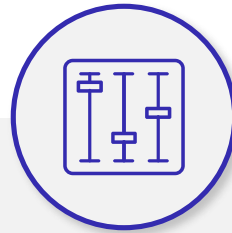


- AI / ML models specifically designed for compliance and risk use cases
- Supports multiple models - both internal and external models
- Calculation engine that provides services for multiple models, stateless and scalable
- Advanced Simulation engine

MetricStream Intelligence: **AI-Centric Workflows** for Better **GRC** Experiences



**Risk Identification &
Assessment**



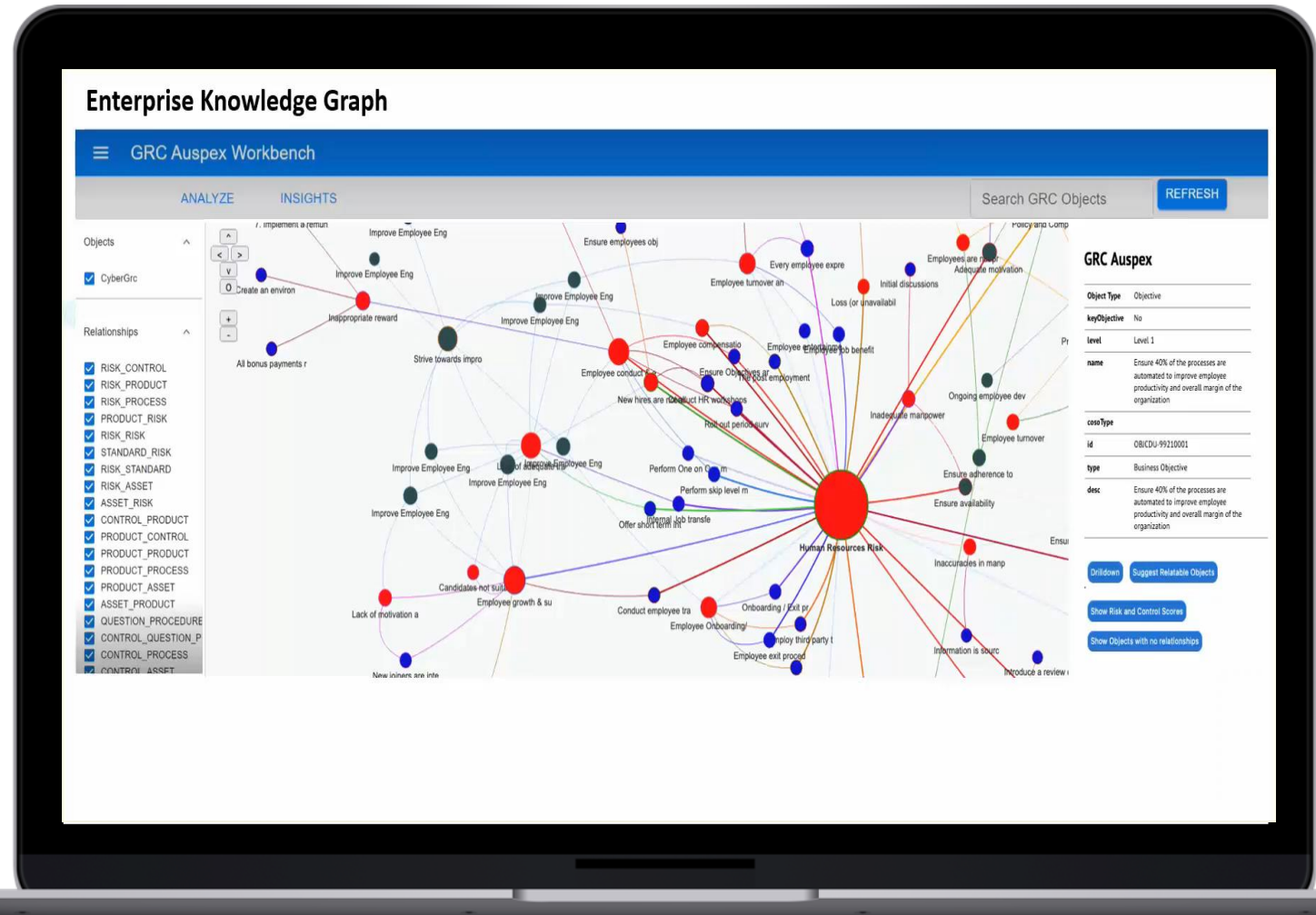
**Risk Mitigation &
Treatment**



**Risk Monitoring &
Reporting**

Risk Identification & Assessment

- Achieved via GRC Ontology based Knowledge Graph
- Manages relationships between processes, risks & controls
- Identifies critical gaps in risk & control coverage
- Intelligently triggers risk assessments & control tests



Risk Mitigation & Treatment

- Identifies patterns and themes across issues & observations
- Automatically performs root cause analysis
- Recommends treatment & action plans

The screenshot displays the 'Issue Creation' interface within the 'metricstream' application. The interface is divided into a left sidebar with navigation links (General, Issue Details, Classification, Source, Ownership and Security, Relationships, Root Cause, Action Plan, Additional Details) and a main content area. The main area is titled 'Issue Creation' and contains a form for creating a new issue. The form includes fields for Title, Status, Business Remediation Completed, Description, Date First Identified, Issue Due Date, Review Group Due Date, Classification, Plan for a Plan, Stream, Issue Classification, Subsidary Issue Classification, SOX Classification Rating, Exception Type, Priority, Issue Locations, Legal Entity Impacted, RCM Theme(s), Types, Related Issues, and Source. The 'Title' field is populated with 'Personal USD Term Deposits - AML Gaps'. The 'Status' field is set to 'New'. The 'Description' field contains a detailed text about AML information not being captured consistently. The 'Date First Identified' field is set to 'Date First Identified'. The 'Issue Due Date' field is set to 'Issue Due Date'. The 'Review Group Due Date' field is set to 'Review Group Due Date'. The 'Classification' section includes a 'Confidential Issue' checkbox and a 'Plan for a Plan' dropdown. The 'Stream' field is set to 'Stream'. The 'Issue Classification' field is set to 'Issue Classification'. The 'Subsidary Issue Classification' field is set to 'Subsidary Issue Classification'. The 'SOX Classification Rating' field is set to 'SOX Classification Rating'. The 'Exception Type' field is set to 'Exception Type'. The 'Priority' field is set to 'Priority'. The 'Issue Locations' field is set to 'Issue Locations'. The 'Legal Entity Impacted' field is set to 'Legal Entity Impacted'. The 'RCM Theme(s)' field is set to 'RCM Theme(s)'. The 'Types' field is set to 'Deficiency'. The 'Related Issues' field is set to 'Personal USD Term Deposits - AML Gaps' and 'Personal Lending AML Third Party Beneficiary Information'. The 'Source' field is set to 'Source Type'. A progress indicator at the bottom left shows 18% completion.

Monitoring & Reporting on Regulatory Change

Regulation

AI extraction of parts of the regulation
relevant to your organisation



Monitoring & Reporting on Regulatory Change

Regulation

AI extraction of parts of the regulation relevant to your organisation



Obligations

AI generated summary of extracted content with impact score

- § 201.108 (a)** **Must Do**
to authorize advances thereunder to member banks "secured by such obligations as are eligible for purchase under section 14(b) of this Act...
 - § 201.108 (c)** **Should Do**
Nothing less than a full guarantee of principal and interest by a Federal agency will make an obligation eligible...
 - § 201.108 (b)** **Must Do**
 - § 201.108 (d)** **No longer required**
 - ...** **Should Do**
- ...

Monitoring & Reporting on Regulatory Change

Regulation

AI extraction of parts of the regulation relevant to your organisation



Obligations

AI generated summary of extracted content with impact score

§ 201.108 (a) **Must Do**
to authorize advances thereunder to member banks "secured by such obligations as are eligible for purchase under section 14(b) of this Act...

§ 201.108 (c) **Should Do**
Nothing less than a full guarantee of principal and interest by a Federal agency will make an obligation eligible...

§ 201.108 (b) **Must Do**

§ 201.108 (d) No longer required







... **Should Do**

Actions

Next best action for each impact piece.
Tasks are distributed across your employees and systems.

- ☐ **Update ISMS Policy**  
- ☐ **Update AML Policy**  
- ☐ **Update Conflict of Interest (COI) Policy**  

...

- ☐ **Perform Risk Assessment**  
- ☐ **Perform Control Tests**  
- ☐ ...  

...

☒ **Already compliant. No actions required**

☒ **Policy review**

☒ **Already compliant. No actions required**

Monitoring & Reporting on Regulatory Change

Regulation

AI extraction of parts of the regulation relevant to your organisation



Obligations

AI generated summary of extracted content with impact score

§ 201.108 (a) **Must Do**
to authorize advances thereunder to member banks "secured by such obligations as are eligible for purchase under section 14(b) of this Act...

§ 201.108 (c) **Should Do**
Nothing less than a full guarantee of principal and interest by a Federal agency will make an obligation eligible...

§ 201.108 (b) **Must Do**

§ 201.108 (d) No longer required







... **Should Do**



Actions

Next best action for each impact piece.
Tasks are distributed across your employees and systems.

- ☐ **Update ISMS Policy**  
- ☐ **Update AML Policy**  
- ☐ **Update Conflict of Interest (COI) Policy**  

- ☐ **Perform Risk Assessment**  
- ☐ **Perform Control Tests**  
- ☐ ...  

☒ **Already compliant. No actions required**

☒ **Policy review**

☒ **Already compliant. No actions required**

GRC for AI 2023-2024

//

High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately.

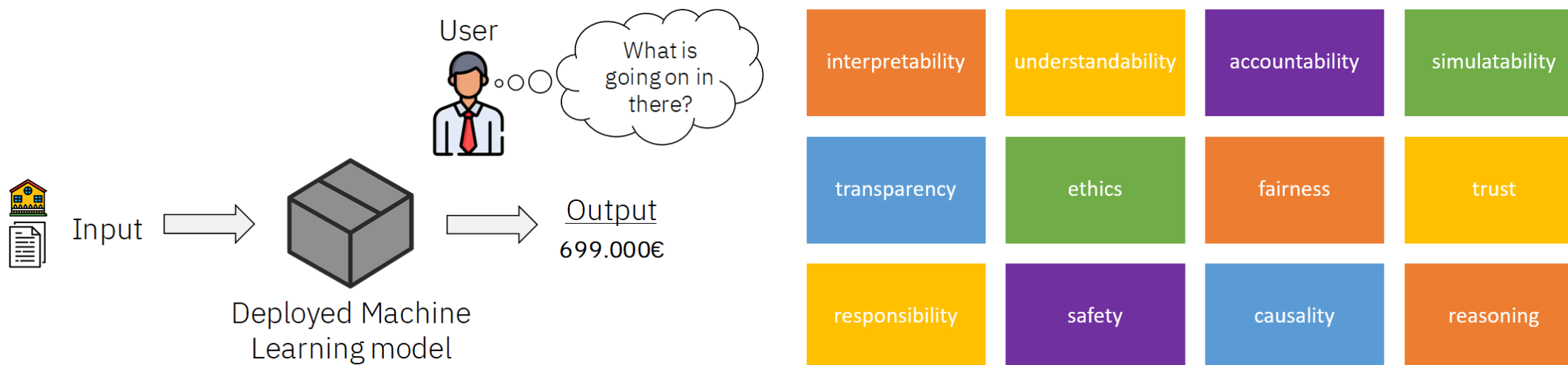
Article 13, EU AI ACT

//

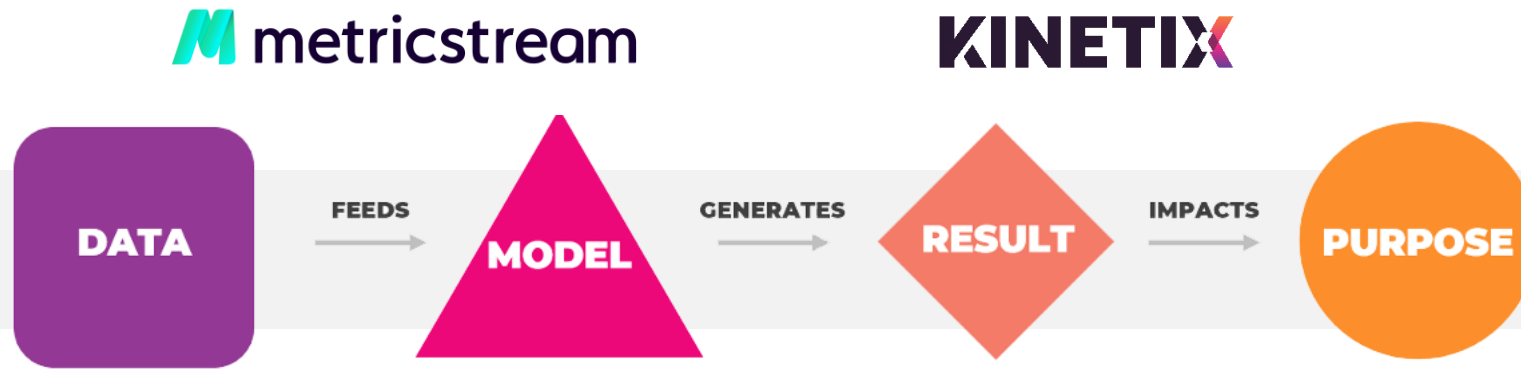


Explainable & Responsible AI

An **Explainable AI (XAI)** is an artificial intelligence (AI) whose actions can be easily understood by humans and therefore can be trusted



AI & Risk Management use cases



Purpose: _____

- Regulatory obligation determination
- Redlining and context analysis using Natural Language Processing (NLP)
- Explainable AI (XAI) decision transparency
- AI assurance and regulatory reporting validation
- Mapping obligations to controls and policies

A night-time photograph of the Tower Bridge in London, illuminated with warm lights against a dark blue sky. The bridge's two towers and suspension cables are clearly visible. In the foreground, a dark metal railing is partially visible.

GRC

SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

Thank You

 **metricstream**
thrive on risk™

Appendix

Third Party Management

Automated Survey Attachment Processing



TPM – Third Party Automated Survey Response processing

Available in Brazos

Problem:

- In the third-party Survey app, user send out surveys and receive survey responses with attached documents. Reviews and audits are required for information embedded within these survey attachments which can be a time-consuming task.

Solution:

- Processing of these survey can be automated such as SOC2/SOC3/ISO. Also provide drill down report based on the scope users will look at.

Benefits:

- Efficiency - Reduce time and effort for risk managers to review each third-party documents one by one.
- Transparency – Increased risk coverage by automatically extracting important information that could be potentially missed by the human eye.



Third Parties Upload

IT Vendors upload
SOC2, SOC3 & ISO Reports

IAM-11	An automatic alert is triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance group. Appropriateness of access is reviewed and approved.	CC6.1 CC6.2 CC6.3	Inquired of the control owner and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR for any role change between the following groups: Engineering, Customer Support and Success ("CSS"), or Finance group. Further ascertained that appropriateness of access was reviewed and approved.	No deviation noted.
			Inspected the approval for a sample of role changes between the Engineering, Customer Support and Success ("CSS"), or Finance group and ascertained that an automatic alert was triggered to the Risk and Compliance Manager and HR, and appropriateness of access was reviewed and approved.	Deviation Noted.



MetricStream Intelligence

Identify deviations/exceptions
needing attention

THIRD PARTY SOC2 REPORT DETAILS			
Choose a Saved Layout *			
Third Party	Document	Product/Service	Document Type
Microsoft Inc.	Document\Vendor Azure & Azure Governance SOC...	Microsoft Azure and Dynamics 365 Services customers	SOC2
Reflexive, INC.	Document\Vendor Reflexive, Inc. SOC 2 Type 2 201...	Description of the Employee Performance Managem...	SOC2
Intermap	Document\Vendor SOC 2 Report Jan 2014.pdf	Intermap Network Services	SOC2
Atlassian PTY Ltd.	Document\Vendor Atlassian SOC2 Type 2, 31 Oct 2...	Atlassian	SOC2

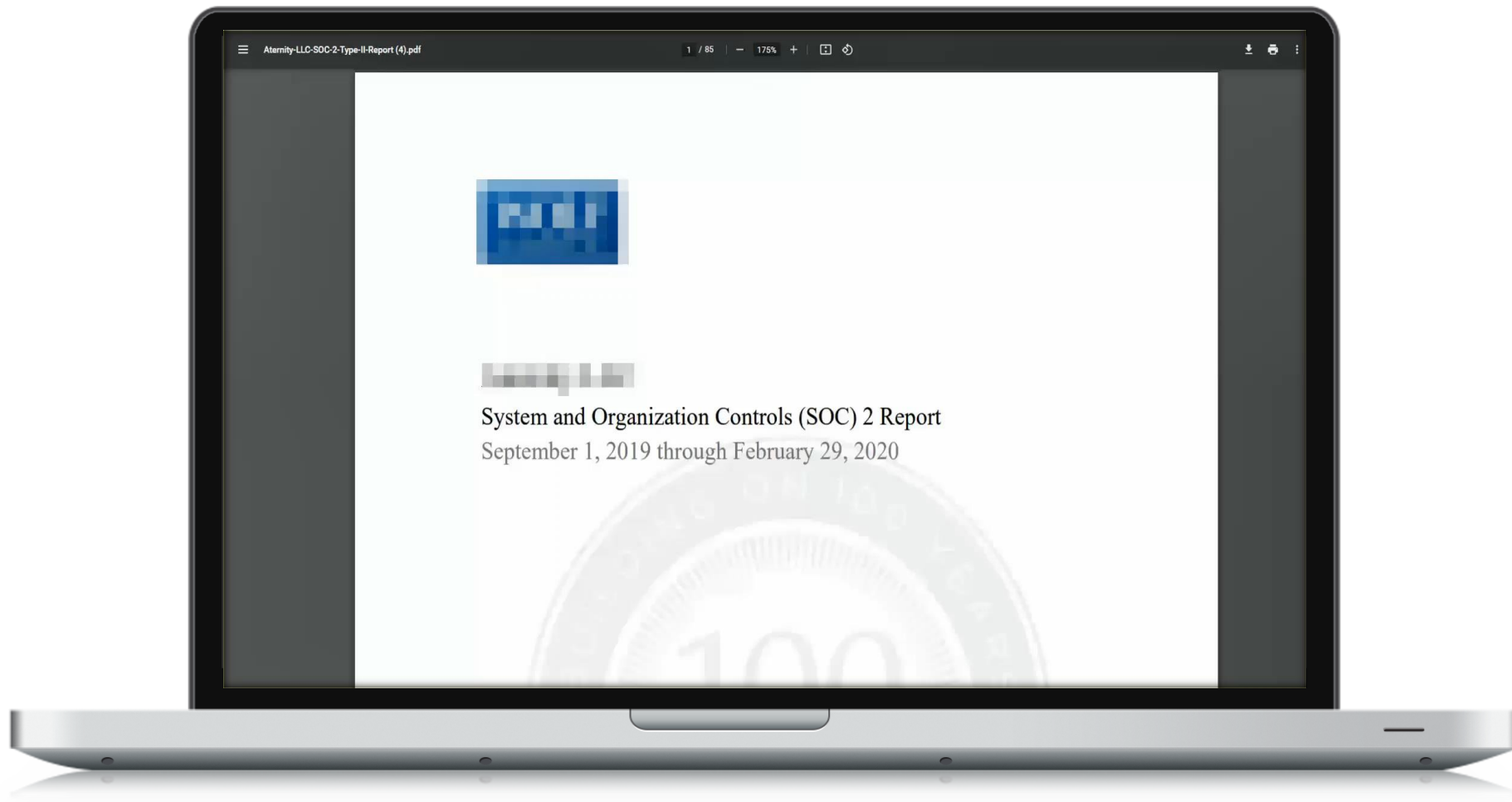


Risk Report

Consolidated risk report with
actionable insights

SOC2 EXCEPTION DETAILS		
Choose a Saved Layout *		
Page No	Keyword	Extracted Text
68	Deviation Noted	Deviation noted. One (1) of the five (5) role changes sampled for testing was not reviewed and approved timely.
72	Deviation Noted	Deviation noted. One (1) of three (3) sampled quarterly disaster recovery testing was not performed.
76	Deviation Noted	Deviation noted. One (1) of three (3) sampled quarterly capacity audit was not performed.

TPM – Third Party Artifacts Anomalies



Collaborative Learning

A night-time photograph of the Tower Bridge in London, illuminated with warm lights against a dark blue sky. The bridge's two towers and suspension cables are visible. In the foreground, a dark metal railing with a diamond-patterned mesh runs across the frame. The overall scene is dimly lit, with the bridge's lights providing the primary illumination.

Regulatory Change Management (Collaborative Learning)

Overview :

RCM, enabled via MetricStream Intelligence allows for:

- Identify regulatory changes that will impact your organization.
- Identify GRC Library Objects that are impacted from these regulatory changes.
- Anonymize & Identify patterns to build your knowledge graph.
- Recommend actions performed by domain experts at similar entities via collaborative learning.

