metricstream

GRC SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

Business Advantages Connecting Your GRC Platform on a Secure Cloud

Marco Icardi & Neeraj Patel

Agenda

- MetricStream Cloud for a Connected GRC Platform
- European Regulations
- The MetricStream Cloud Offering
- Migration to Cloud
- Q&A

MetricStream GRC Cloud

- Dedicated Instance, No co-mingling of data
- Multi Layered Security and Controls
- Industry Standard Monitoring Tools
- 3rd party Vulnerability/ Penetration Testing
- IDS/ High Availability
- Compliant with HIPAA, ISO, SOC2, GDPR, EBA
- Defined SLAs - 99.90% uptime and higher
- Encryption of data-in-transit, data-at-rest, & *database-at-rest

*Optional offering

Connected GRC

BUSINESS GRC

- Enterprise & Operational Risk
- Regulatory Compliance
- Internal Audit
- Third-party Risk
- Risk Quantification
- AI & Mobile

CYBER GRC

- IT & Cyber Policy
- IT & Cyber Compliance
- IT & Cyber Risk
- IT Vendor Risk
- Cyber Risk Quantification
- AI & Mobile

ESG GRC

- Disclosure Frameworks
- Metrics
- Supplier Assessments
- Policy
- Board Reporting

metricstream platform

GRC SUMMIT 2022

LONDON, NOV 8-9

Hosted by MetricStream

European Regulations

MetricStream

Schrems II

- On July 16, 2020, the Court of Justice of the European Union (CJEU) published its judgment in the Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) (the Schrems II case).
- In its judgment, the CJEU declared the EU-US Privacy Shield – one of the primary data transfer mechanisms for the safe and free flow of data between EU and US organizations - invalid.
- On June 18, 2021, the European Data Protection Board (EDPB) adopted its final recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

MetricStream

Data Privacy in Europe

- Schrems II basically invalidated the EU-US Privacy Shield which was related to transferring personal data between EU & US.
- MetricStream already hosts EU customers' instances in EU region which complies with Schrems II.
- WE are prepared and ready to move forward with getting European customers to migrate to MetricStream managed Cloud

MetricStream

Trans-Atlantic Data Privacy Framework

The European Commission and the United States reached an agreement in principle for a **Trans-Atlantic Data Privacy Framework.**

Key principles

- Based on the new framework, **data will be able to flow freely and safely** between the EU and participating U.S. companies
- A new set of rules and **binding safeguards to limit access to data** by U.S. intelligence authorities to what is **necessary and proportionate** to protect national security; U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
- **A new two-tier redress system** to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a **Data Protection Review Court**
- **Strong obligations for companies** processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce
- **Specific monitoring and review mechanisms**

MetricStream

Data Privacy in Switzerland

- Switzerland is in the final stage of releasing the revised data protection legislation. Therefore, it is time to review your GDPR implementation and adapt it to meet the Swiss-specific provisions, where necessary.

MetricStream

Data Privacy in Switzerland

Global Privacy Regulations

Privacy regulations all over the world are being changed, enhancing the privacy rights of individuals and the protection of their personal data. The tightening regulatory frameworks require substantial changes by organizations. Knowing which regulations must be complied with and then implementing the required changes is crucial.

GDPR

The EU GDPR has been in force since 25 May 2018 and must be complied with by organizations in the EU and in some cases also outside of it. The EU GDPR with its large scope has fundamentally changed the privacy landscape and continues to be the biggest game changer introducing new controls, processes, responsibilities, reporting standards and fines up to 4% of the global turnover of a firm.

Swiss Federal Data Protection Regulation

The revised Swiss data protection legislation will soon be released by the Swiss parliament and come into immediate effect. However, there will be a transition period to adapt to the new regulation. The legislation will introduce GDPR-like standards also in Switzerland.

MetricStream Cloud

MetricStream GRC Cloud is Modern & Secure

Traditional Cloud

- Multi-tenant
- Security Concerns
- Performance Concerns
- Rigid Configuration
- Not easy/difficult to configure to meet customer specific needs as multiple customers use the same instance

Modern & Secure GRC Cloud

- Single-tenant Architecture
- Dedicated Instance and Containers
- Secure – No co-mingling of data
- High Performance - Not affected by other customers
- Highly Configurable
- Easy to update and upgrade

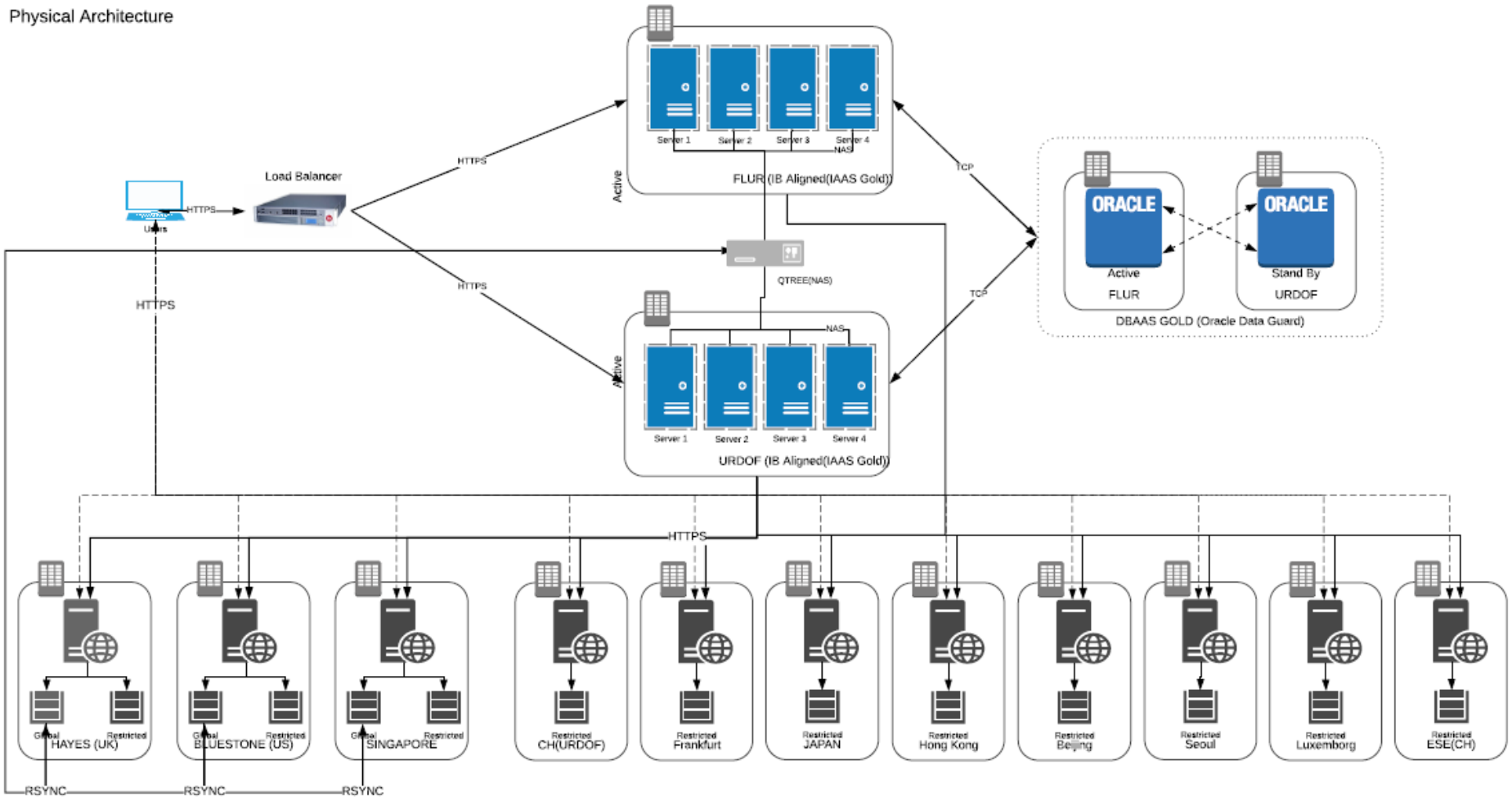
Secure by Design

Multi-layered Security for Superior Data Protection

- **Network and Infrastructure Security -** Designed to detect and protect from malicious or unauthorized traffic
- **Host and Endpoint Security -** Detect and protect against malware and other threats
- **Data Protection and Encryption -** Protect data via encryption, user behavior analysis, and identification of content
- **Logging, Monitoring, Threat Detection, and Analytics -** Centralized logging, reporting, and analysis of logs to provide visibility and security insights
- **Privacy and Regulatory Compliance -** GDPR, ISO, HIPAA, and audited for SOC to further strengthen standards of privacy and regulatory compliance
- **Intrusion Detection Systems -** Monitor the network for malicious activity and policy violations
- **Identity and Access Control -** define and manage user identity, access policies and entitlements
- **Periodic Vulnerability Assessments -** Penetration testing helps identify risks and implement appropriate mitigation measures
- **Application Security -** Assesses code, logic, and application inputs to detect software vulnerabilities and threats
- **Security Audits -** Regular Internal and Third-party audits to ensure no security vulnerabilities

Prod Infrastructure Architecture

- Example on-premises



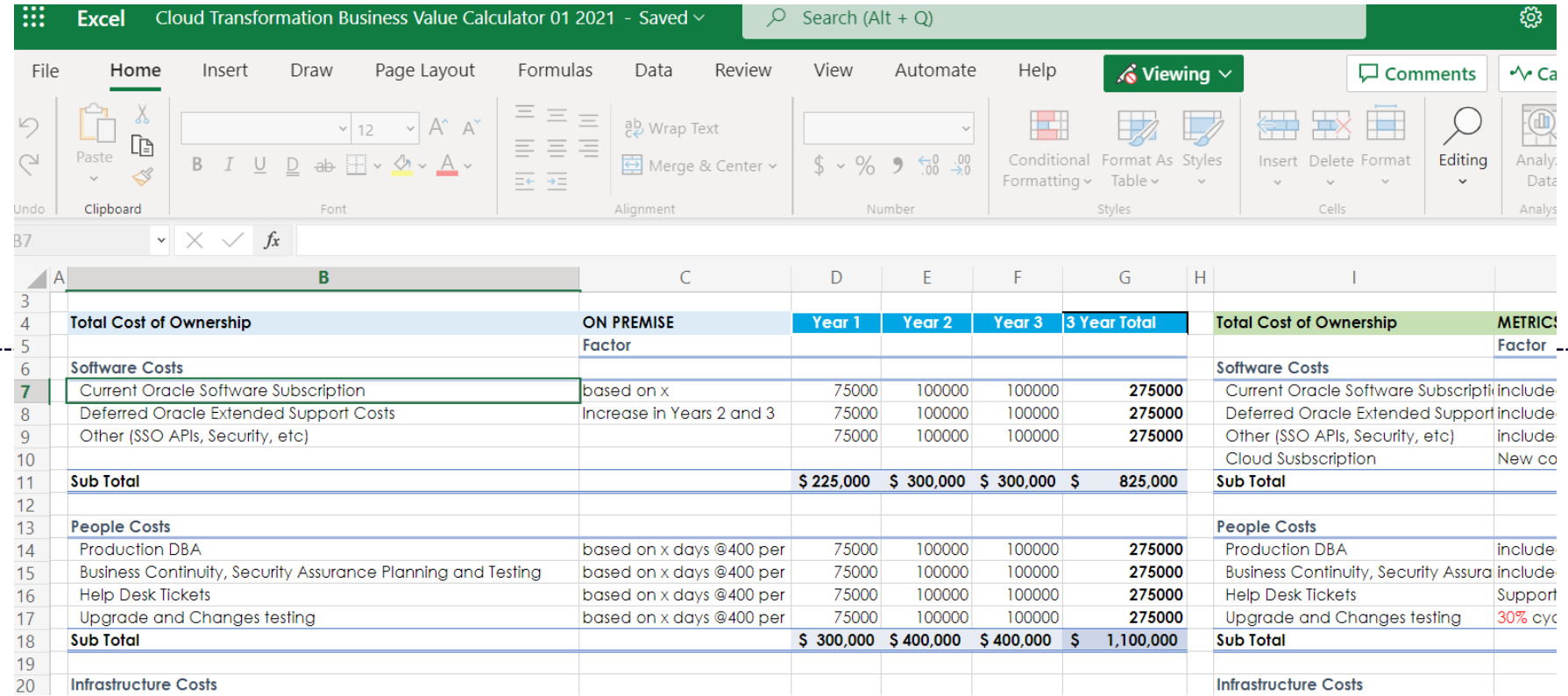
MetricStream Cloud Offerings

Business/technical considerations	MetricStream Cloud
Service Level Availability	99.90%
Production Environment (and Disaster Recovery environment)	Included
UAT Environment (and QA environment)	Included
Development Environment	Included
Disaster Recovery – Recovery Time Objective (RTO)	1 Business Day
Disaster Recovery – Recovery Point Objective (RPO)	4 Hours
Disaster Recovery Capacity Objective (RCapO)	70%
Storage Capacity	Unlimited
Encryption (In Transit, At Rest)	✓

Business/technical considerations	MetricStream Cloud
Encrypted Backups	15 Days
Access Management Integration (SSO, LDAP, AD)	✓
Standard AWS Key Management	✓
Customer-managed or MetricStream-managed Key	✓
IP Filtering	✓
Enterprise Server Security (HIPS, Anti-Virus, Malware)	✓
Compliance (SOC2, ISO, HIPAA)	SOC2, ISO, HIPAA
Data Location and Sovereignty*	✓

MetricStream

Cloud Transformation Workshop



	B	C	D	E	F	G	H	I	
3									
4	**Total Cost of Ownership**	**ON PREMISE**	**Year 1**	**Year 2**	**Year 3**	**3 Year Total**		**Total Cost of Ownership**	**METRICS**
5		**Factor**							**Factor**
6	**Software Costs**							**Software Costs**	
7	Current Oracle Software Subscription	based on x	75000	100000	100000	**275000**		Current Oracle Software Subscripti	include
8	Deferred Oracle Extended Support Costs	Increase in Years 2 and 3	75000	100000	100000	**275000**		Deferred Oracle Extended Support	include
9	Other (SSO APIs, Security, etc)		75000	100000	100000	**275000**		Other (SSO APIs, Security, etc)	include
10								Cloud Susbscription	New co
11	**Sub Total**		**$ 225,000**	**$ 300,000**	**$ 300,000**	**$ 825,000**		**Sub Total**	
12									
13	**People Costs**							**People Costs**	
14	Production DBA	based on x days @400 per	75000	100000	100000	**275000**		Production DBA	include
15	Business Continuity, Security Assurance Planning and Testing	based on x days @400 per	75000	100000	100000	**275000**		Business Continuity, Security Assura	include
16	Help Desk Tickets	based on x days @400 per	75000	100000	100000	**275000**		Help Desk Tickets	Support
17	Upgrade and Changes testing	based on x days @400 per	75000	100000	100000	**275000**		Upgrade and Changes testing	30% cyc
18	**Sub Total**		**$ 300,000**	**$ 400,000**	**$ 400,000**	**$ 1,100,000**		**Sub Total**	
19									
20	**Infrastructure Costs**							**Infrastructure Costs**	

Business Value Calculator: Cloud

Path to Success

Key Benefits of MetricStream GRC Cloud

Business Centric

- Immediate access to new releases and features
- Respond to business quickly with faster deployments and upgrades
- Improve application availability, scalability to handle increasing data volume and performance requirements

3x

More new features delivered per year

Lower TCO

- Reduce costs including for hardware, software, chargebacks, and IT personnel required to manage and maintain environments
- Better Support with a predictable patch schedule, on a standard technology stack - with greater security and resilience

50%

Reduction in Cost

Key Benefits of MetricStream GRC Cloud

Flexibility

- Easy, migration of data from on-premise to cloud and vice versa
- Ability to move more easily to latest version with seamlessly delivered future enhancements in a SaaS environment
- Manage business and security expectations on architectural flexibility, scalability

99.9%
Uptime

Advanced Security & Privacy

- Adhere to Regional and Regulatory Security Standards such as HIPAA, SOC2, Privacy requirements
- Application, Network and Physical tier security is managed in a transparent and auditable manner
- Granular App & Instance level security as per regulatory standards

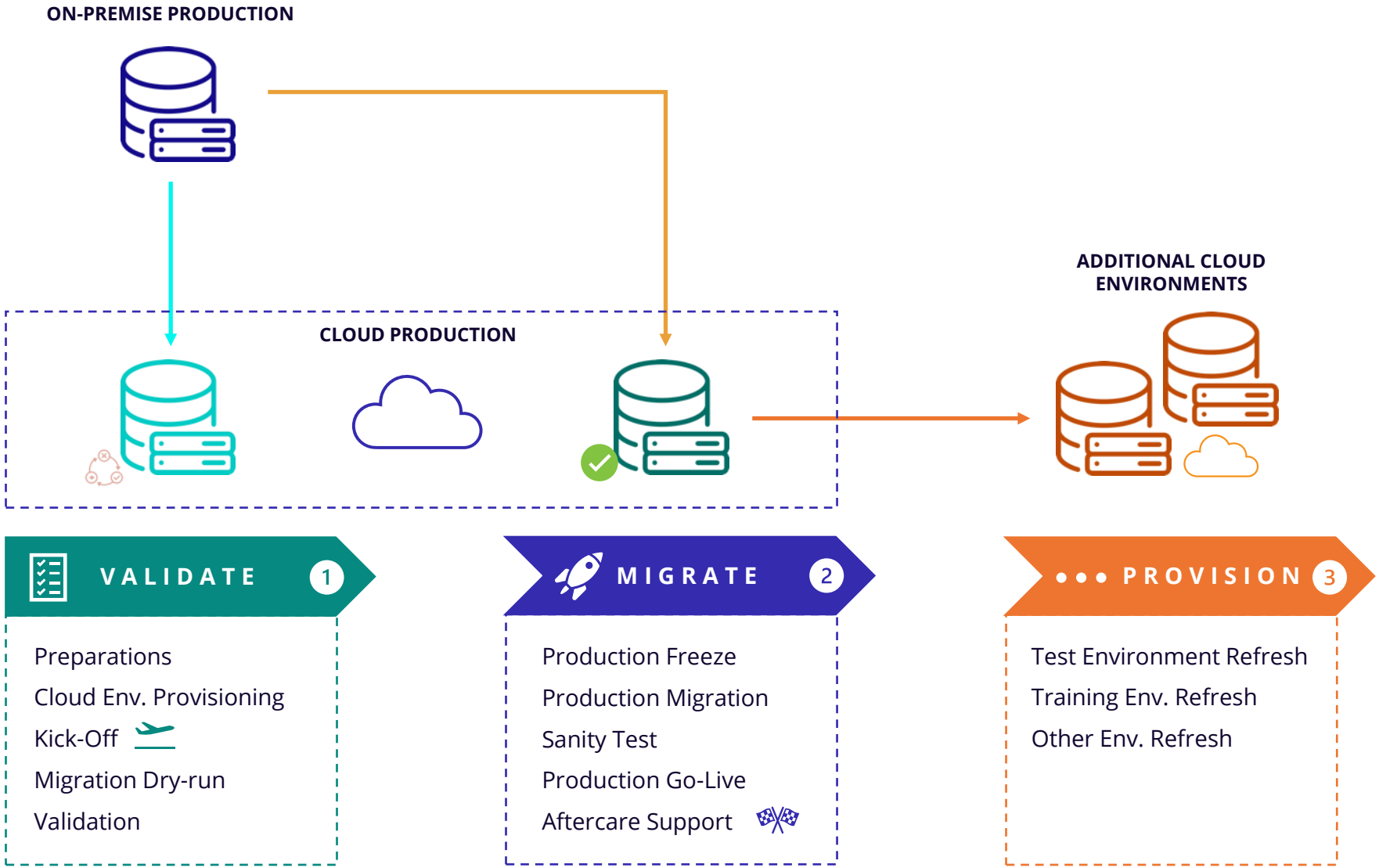
0
Critical Incidents in the last 3 years

GRC SUMMIT 2022

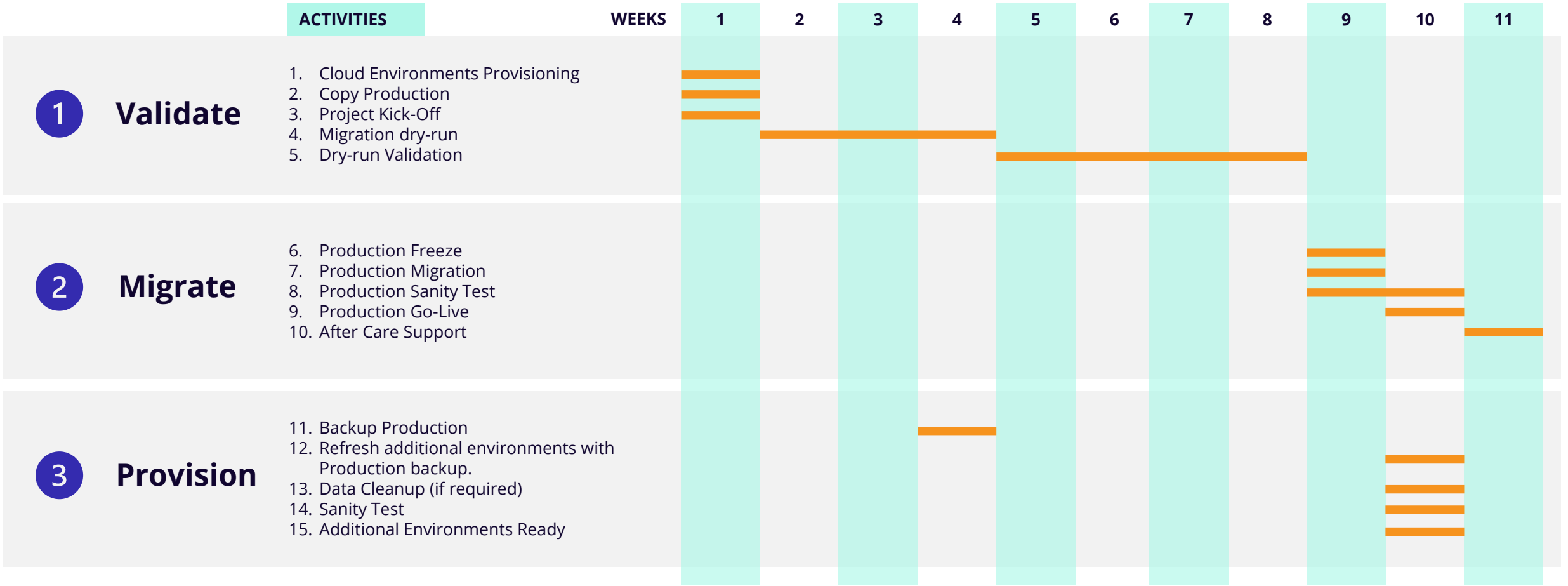
LONDON, NOV 8-9

Hosted by MetricStream

On-prem to Cloud Migration


ON-PREMISE PRODUCTION
CLOUD PRODUCTION
ADDITIONAL CLOUD ENVIRONMENTS
VALIDATE 1
Preparations
Cloud Env. Provisioning
Kick-Off
Migration Dry-run
Validation
MIGRATE 2
Production Freeze
Production Migration
Sanity Test
Production Go-Live
Aftercare Support
PROVISION 3
Test Environment Refresh
Training Env. Refresh
Other Env. Refresh

Preliminary Timelines



Commercial Overview

- Cloud Environments Provisioning
- Production Environment Export
- Attachment Decryption/Encryption
- Cloud Security Setup
- Identity Management Integration (AD/SSO)
- Project Preparation, Planning and Alignment
- Kick-Off
- Migration Dry-run
- Dry-run Validation
- Production Migration
- Production Verification
- Production Sanity Test
- Go-Live and Aftercare Support
- Test *and/or Additional* Environments Setup
- CRs, Upgrades or New Functionality Setup


Q&A
TELEPHONE

Thank You!

micardi@metricstream.com

Mobile: +39 3346088735