Why the cloud is good for treasury

Bob Stark
Vice President, Strategy
May 4, 2017
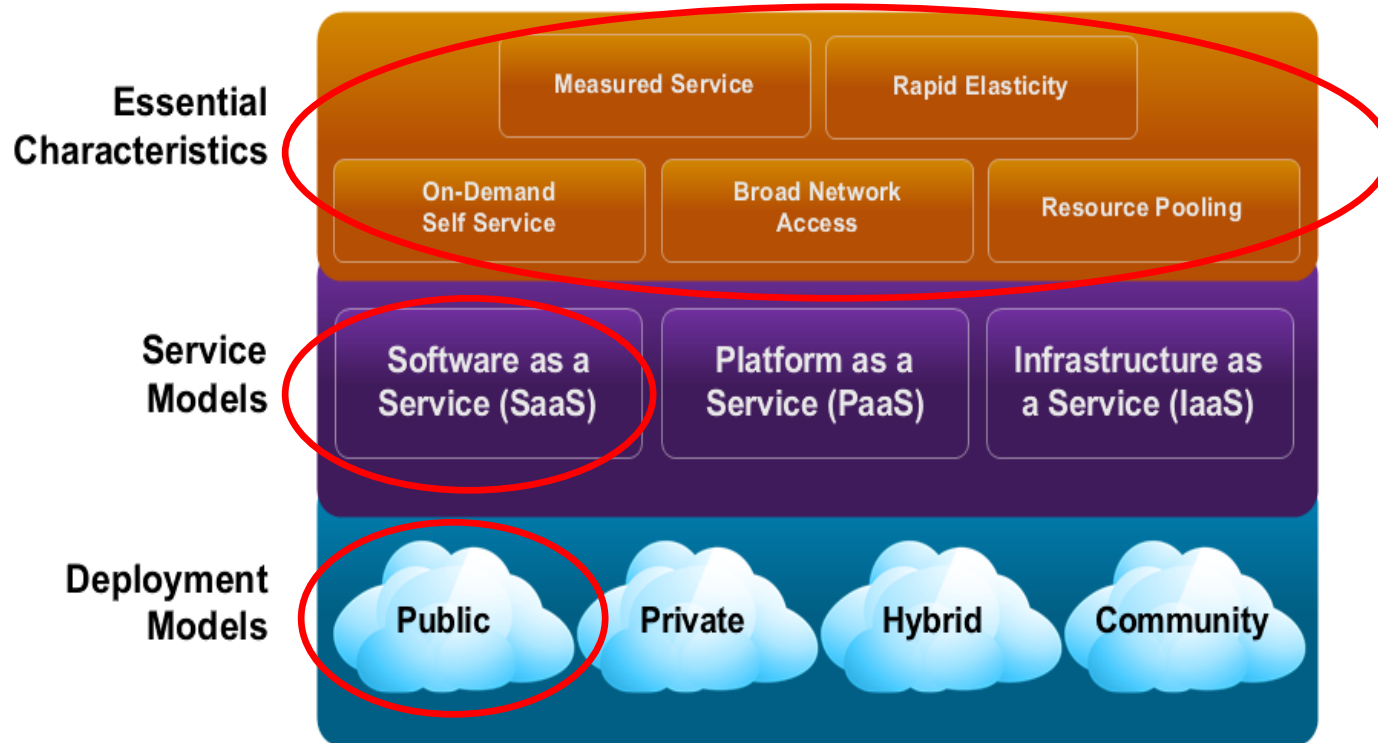
kyriba™
Proactive | Treasury | Management

Today's discussion

- ## What is the cloud (for treasury)?

- ## Operational Risk Reduction
  - IT's reduced role
  - Security of the cloud
  - Business continuity

- ## Functionality for Treasury
  - Software updates
  - (Lack of) customization
  - Global process standardization
  - System integration

kyriba

Key Questions

- How does a cloud treasury system keep my data safe?

- Doesn't the cloud present more risk?

- Is data encrypted within the cloud?

- How does a vendor like Kyriba ensure there are no insider threats?

- What if my IT says "no"?
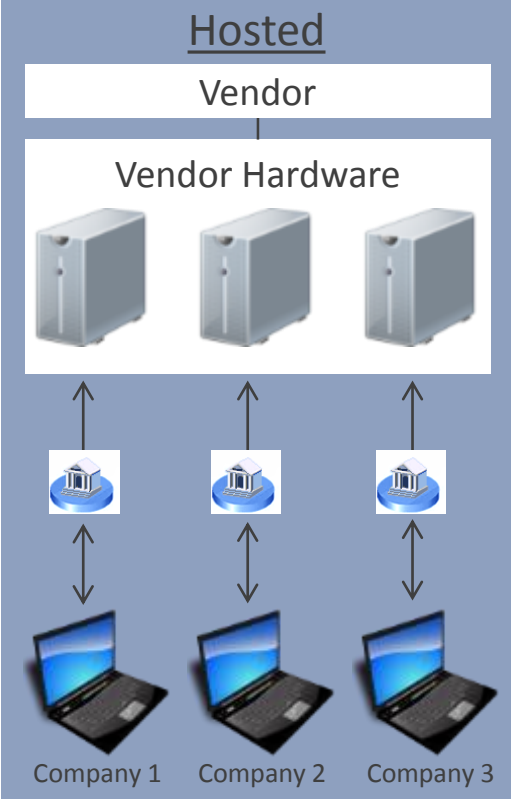
What is the Cloud

Defining the Cloud

Essential Characteristics
- Measured Service
- Rapid Elasticity
- On-Demand Self Service
- Broad Network Access
- Resource Pooling

Service Models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models
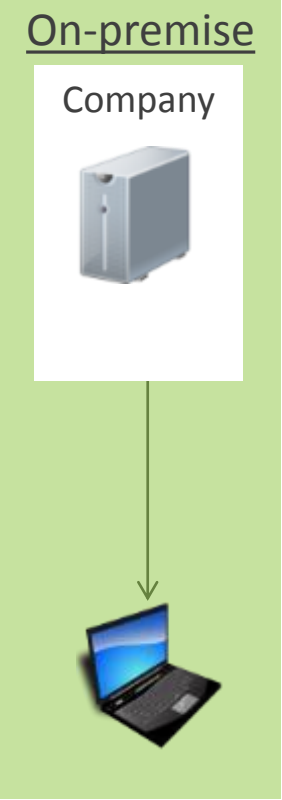- Public
- Private
- Hybrid
- Community

Key Terms:
- Fully virtualized
- Multi-tenant (vs. single tenant)
- No plug-ins or software to download

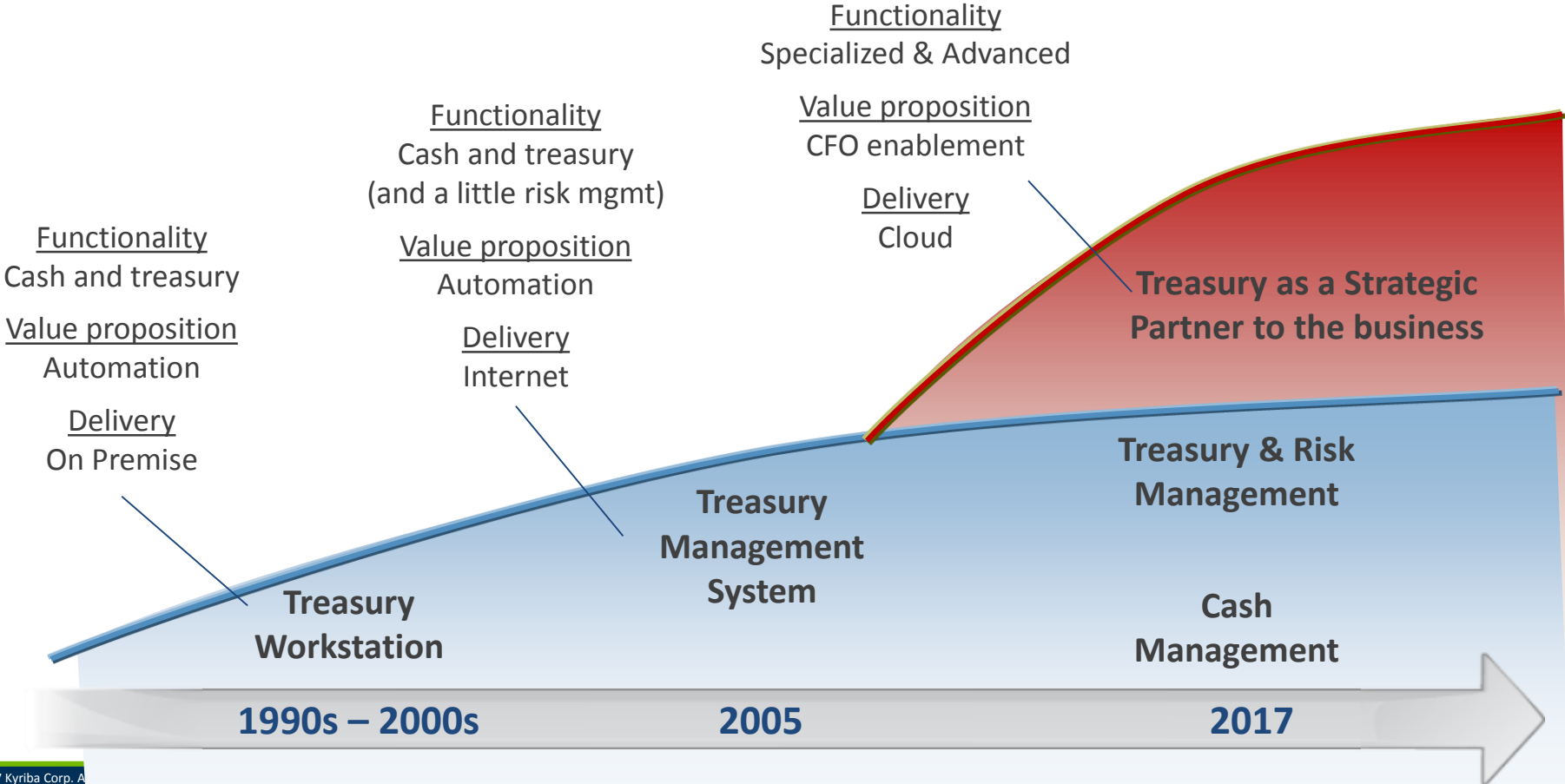Source: National Institute of Standards and Technology (NIST)

kyriba

Cloud vs. Hosted Software
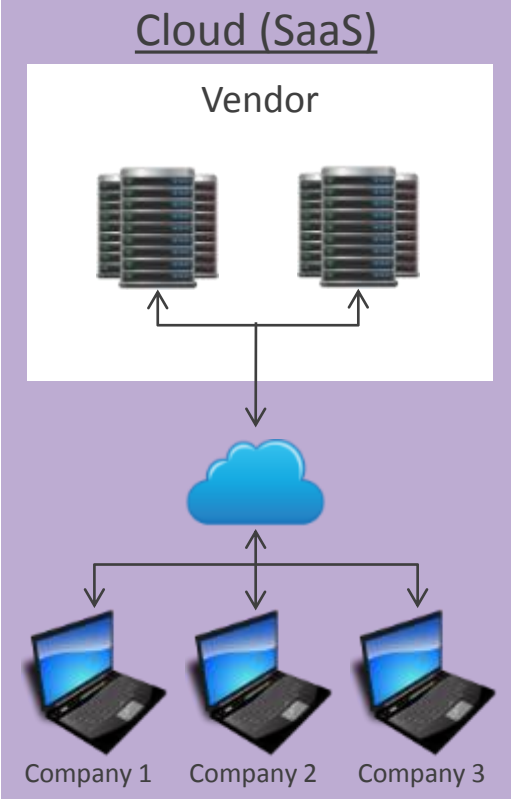
What does the cloud mean for treasury?

Treasury Requirement	Most any system can do	Unique to the cloud
Managed upgrades by vendor	X	
Access over internet	X	
Platform wide monitoring		X
Deployment of resources across all customers		X
Complete business continuity		X
Low variable cost per customer		X
Personalization by company and by user		X
Behind the scenes web integration using APIs and web services		X

kyriba™

PROPRIETARY & CONFIDENTIAL.

What does the cloud mean for treasury?

Functionality
Cash and treasury

Value proposition
Automation

Delivery
On Premise

Treasury Workstation

Functionality
Cash and treasury
(and a little risk mgmt)

Value proposition
Automation

Delivery
Internet

Treasury Management System

Functionality
Specialized & Advanced

Value proposition
CFO enablement

Delivery
Cloud

Treasury as a Strategic Partner to the business

Treasury & Risk Management

Cash Management

1990s – 2000s   **2005**   **2017**

8

Operational Risk Reduction

Operational Risk

Cloud offers transfer of risk and responsibility

- Protects company from its own employees and 'on premise' safeguards

- Shifts risk to new set of variables beyond company's immediate control

- Changes IT's responsibility from hosting to evaluating

- New set of C-level executive offices (CIO, CTO, CISO) exist to ensure that cloud offers greater safety

kyriba

Operational Risk

What are the CIO/CTO/CISO looking for?

- **Data centers**: access points, redundancy, rented vs. leased hardware
- **Software**: login, encryption, penetration testing, consistency of security in DR/BCP
- **Vendor**: viability of company, internal security procedures, investment in security infrastructure

Alignment with company's information security policies

kyriba™

## Treasury system providers plan to avoid service disruptions

- Datacenter locations are in low risk areas
- One datacenter will backup another, with full replication
  - "Full replication" = data, bank connections, ERP interfaces, login protocols, etc.
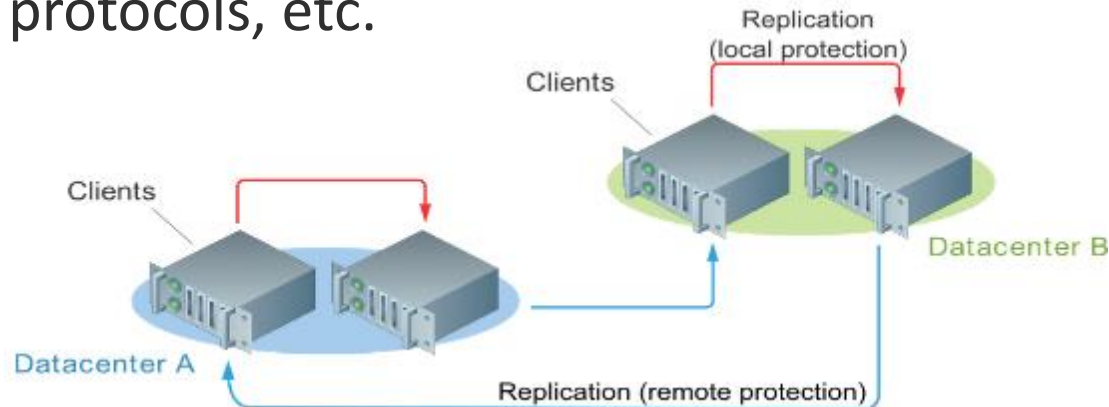
Two key metrics in disaster recovery

- Recovery Time Objective (RTO): how much time is lost

- Recovery Point Objective (RPO): how much data is lost
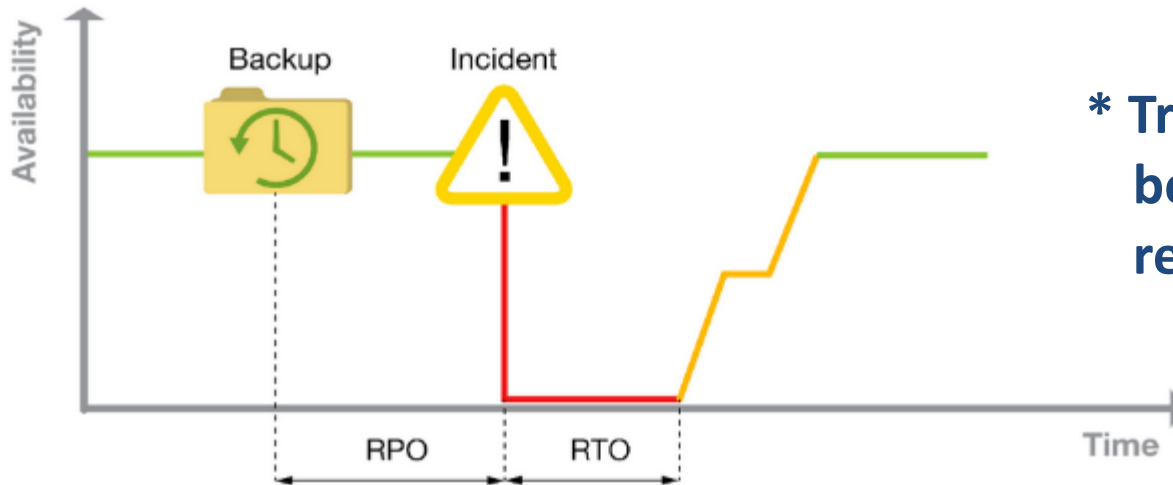
* Treasury's RTO/RPO will be <u>very different</u> than rest of organization

Evaluating Cloud Technology

UserID + Password is <u>not</u> good enough

<u>Need more layers</u>

- Virtual keyboard
- Multi-factor authentication
- IP Filtering
- Single Sign-On
- Encrypted VPN

Define password policy

Rules	Communication	Dual factor authentication	

Activation of the Dual Factor authentication

Second factor: Token

Second factor backup: SMS

Dual authentication options

The second factor must be entered before (minutes): 1

Authentication remains valid during (minutes): 10

☐ Allow a specific dual authentication at the user level

☑ Do not apply to the Admin users

☑ Do not apply dual authentication when using a trusted IP source

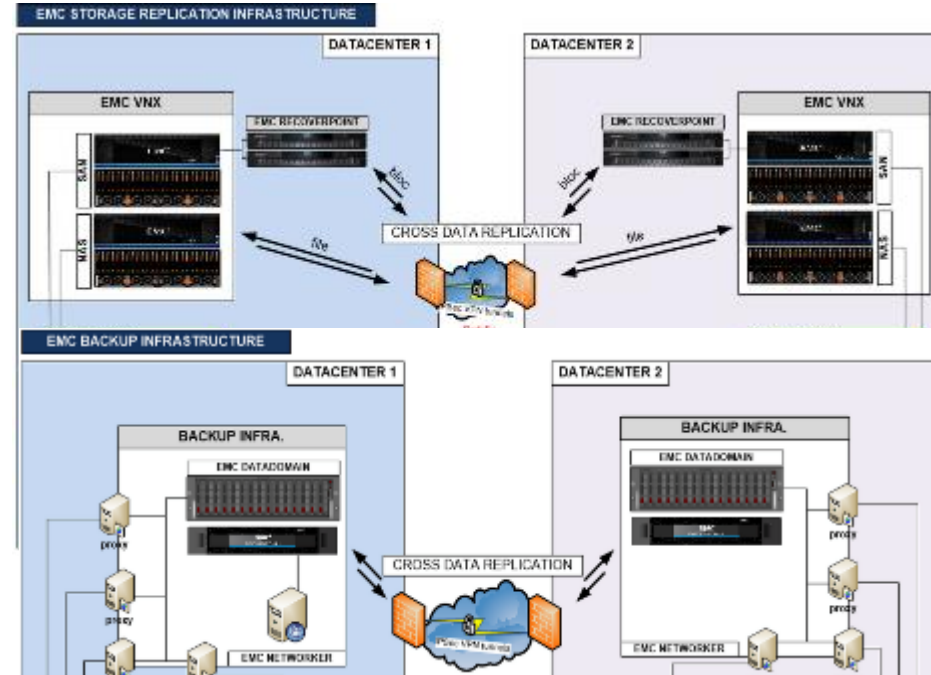|	
Trusted IP source 1:	69.89.31.226
Trusted IP source 2:	69.89.31.227
Trusted IP source 3:	69.89.31.228
Trusted IP source 4:	69.89.31.229
Trusted IP source 5:	69.89.31.230
Trusted IP source 6:	69.89.31.231
Trusted IP source 7:	69.89.31.232
Trusted IP source 8:	69.89.31.233
Trusted IP source 9:	
Trusted IP source 10:	

kyriba™

Evaluating Cloud Technology

How is the data kept secure?

IT will review data security for protection against data loss and corruption:

- Primary storage (SAN)

- Backup & archiving

- Cross site replication

- Data encryption
  - At rest and in transit
  - In database & in application
  - For SAN, backups, and archives

Pictures that confuse us in treasury

Assessing Data Security - Audit Reporting

- Much confusion around SOC1 vs. SOC2
- Must evaluate details of audit; there is no pass/fail

Report	
SOC1	**Only an assessment that controls exist**
SOC2	AICPA's recommended report for cloud service providers: • **Assesses the security behind the controls**
Penetration Testing	Most vendors hire security firms (McAfee, Qualys, etc.) to test external vulnerability

Evaluating Cloud Technology

Cost

- Treasury technology often comes from treasury's budget

- IT can evaluate cost compared to other options (e.g. hosting in cloud themselves)

- <u>Sometimes</u> some/all costs can go to IT's budget
  - Worth investigating opportunity for cost sharing entire application or only "extra security" features

kyriba

Business Continuity

Business Continuity

Loss Condition	Scenario
1) Loss of personnel	Treasury team wins the lottery and tenders resignation from a beach
2) Loss of facilities	Company offices unusable
3) Loss of services	Company offices lose key services such as power or internet
4) Loss of access	Unable to reach company offices if there is a snowstorm

kyriba™

Business Continuity

Loss Conditions	
Scenarios	Company offices are disabled (cyberhack) Company offices can't be accessed (snowstorm) Company offices lose key services (power or internet)
Goal	Perform treasury from other alternate locations (other offices, home, Starbucks…)

kyriba

Business Continuity

Loss Conditions	
Goal	Perform treasury from other alternate locations
What does the cloud offer?	The Cloud • Datacenters for Cloud TMS reside in different locations than company offices • Same workflows can be run anywhere in the world by authorized users • Treasury system can be accessed via mobile device and/or low speed web connection • Additional security can be implemented for access outside of company office

Treasury functionality

Key benefits of a cloud treasury system

Can more easily combine multiple connectivity channels

Standardised workflows across all regions

Global access from single system
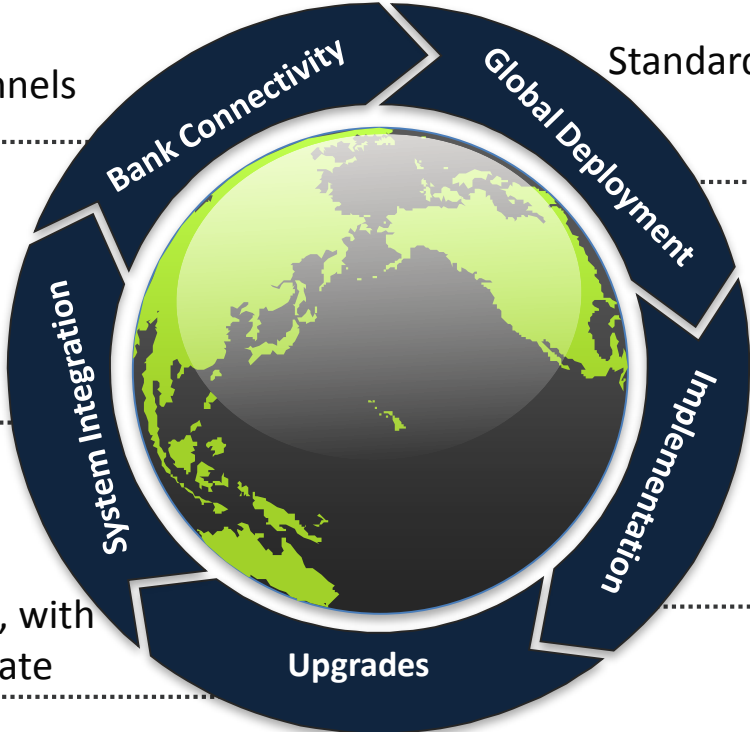
Able to link multiple best-of-breed 'treasury apps'

Cloud deployment enables quicker implementation, eliminates customisation

More new features, more often, with no treasury involvement to update

Bank Connectivity

Global Deployment

System Integration

Implementation

Upgrades

kyriba

The Cloud is good for treasury because...

- Reduced Costs to acquire and implement software-as-a-service

- Ease of access to software (including mobile)

- Vendors invest more in features

- Improved Business Continuity

- Aligns with information security policies & cloud strategy

kyriba

Questions?

Bob Stark
bob@kyriba.com
@treasurybob