DATA PROCESSING LOCATION STRATEGY
DRAFT AND FOR DISCUSSION ONLY

Table of Contents

Document Purpose

The purpose of the document is to define a comprehensive set of data processing location types of SCB along with their characteristics, specification and functionality informed by the characterised compute and storage requirements of the bank as well as identify their ideal placement (target location) considering SCB market locations (current and future), technical constrains. The document also seeks to establish a strategy to mitigate both IT and Cyber failure and attack scenarios.

Executive Summary

This document provides an analysis and recommendations for SCBs Global Processing Strategy considering the requirements expressed to the authors of the SCB Businesses, the ICS TRP Programme and IT Resilience.

The document takes a ten year forward look at the requirements of the business and bases its recommendations against agreed Non-Functional Requirements (NFR) of the Retail Bank, CCIB, Global Functions and End User Services.

IT Resilience failure scenarios are considered in the document and provide the NFRs for the Data Centre and Cloud Service Provider CSP) designs. Data Centre and CSP compute and storage NFR designs have been defined and agreed with the relevant lines of business technology teams. Regional disaster is mitigated by the provisioning of Regional 3rd Copy Sites.

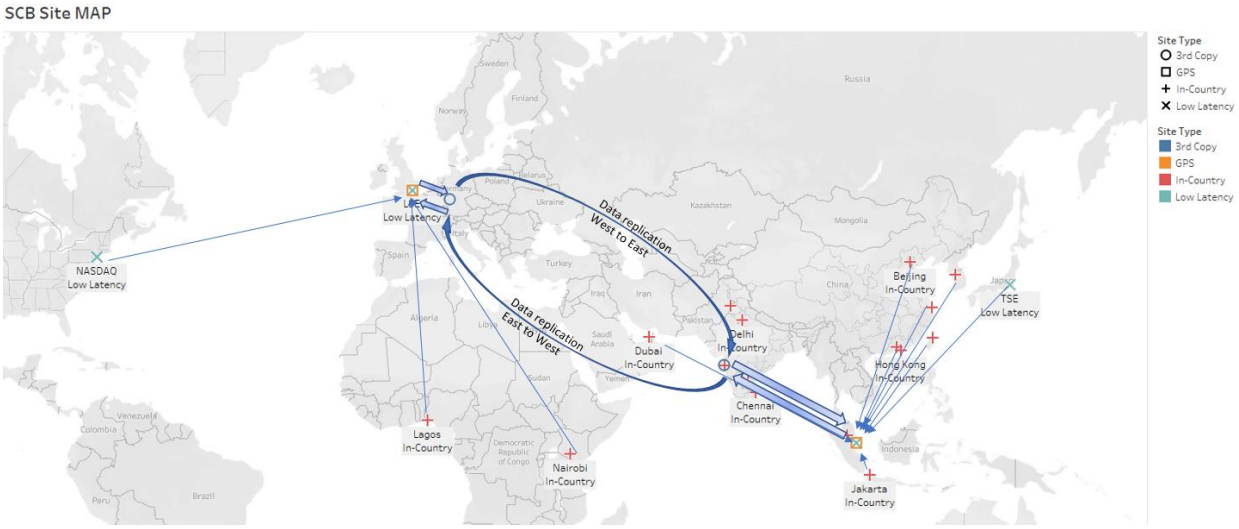
ICS TRP threat scenarios provided by the programme and their mitigations are included in the analysis and the development of the concepts of Cyber Vault.

The document evolves an 'ideal' topology that represents all of these considerations and then provides an 'optimised' topology given constraints around existing sites and the evolving risk situation in Hong Kong. The document provides a plan to mitigate the degradation of key market user experience imposed by these constraints by establishing a Global Edge Caching strategy.

Lastly the document provides a Non-Functional design and costing for both Capex and Opex for both the 3rd Party Site and for he Cyber Vault.

SCB Optimised Topology

The following figure shows the Optimised SCB Global Processing Topology



London will remain the Global Processing Site (GPS) for EMEA; Singapore become a GPS to serve APAC and ultimately replace the one currently located in HK which will become an In-Country location.

Regional Edge Caches, based in Virginia, Frankfurt, Dubai, Mumbai, Singapore and Seoul, should be employed to improve user experience of web apps within strategic markets.

3rd Copy Site & Cyber Vault

The 3rd Copy & Cyber Vault Strategy chosen in this analysis is a Regional one that gives a regionally balanced 3rd Copy proximate to the markets it serves in the recovery situation but outside the natural disaster zone of that the GPS it pairs. This strategy allows for the recovery and extended operational run from Non-Cyber disaster events, giving 'good' performance to markets they recovers.

Cyber events mitigation will be taken care of by London replicating encrypted data to AWS Frankfurt to form a short-lived 3rd Copy site, post validation and cleansing this data will be replicated across to AWS Mumbai and then eventually pulled into a purpose-built air-gapped on-prem cyber vault facility within the Singapore GPS. Data from Singapore will get pushed to AWS Mumbai, replicated across to AWS Frankfurt and pulled down to London GPS' cyber vault.

The deployment option analysed for 3rd Copy in this document is "Ready to Recover" – meaning applications will keep a copy of data and configuration but not of their infrastructure (will need to be provisioned) – and in the event of failure would need to be rebuilt either CSP resources or on prem by holding or re-purposing SCB resources. It is a concern of the authors of this document that should such an event occur that SCB will not be the only FSI affected and the market for CSP resources may become saturated by competing FSI's. Obviously holding SCB resources for this type of exercise is very cost prohibitive.

It is the strong recommendation of this document, therefore, that a Regional Ready to Go model is adopted and coupled with a global development compute strategy where the uplift of cost of the capacity held in the 3rd Sites is mitigated by using it, in its BAU state, as regional development sites and developing a rapid reprovisioning mechanism in the event of Catastrophic failure.

It is also a strong recommendation of the authors that all applications in scope of the 3rd Copy and Cyber Vault are migrated as a pre-requisite to the Vx Platform and employ Infrastructure Patterns through Polaris and multi-cloud API as their means of reconstitution.

3rd Copy and Cyber Vault Indicative Costs

The following costs are based on the inclusion of all BC4& 5 Applications and scopes data and infrastructure costs for the baseline solution only (not app infra).

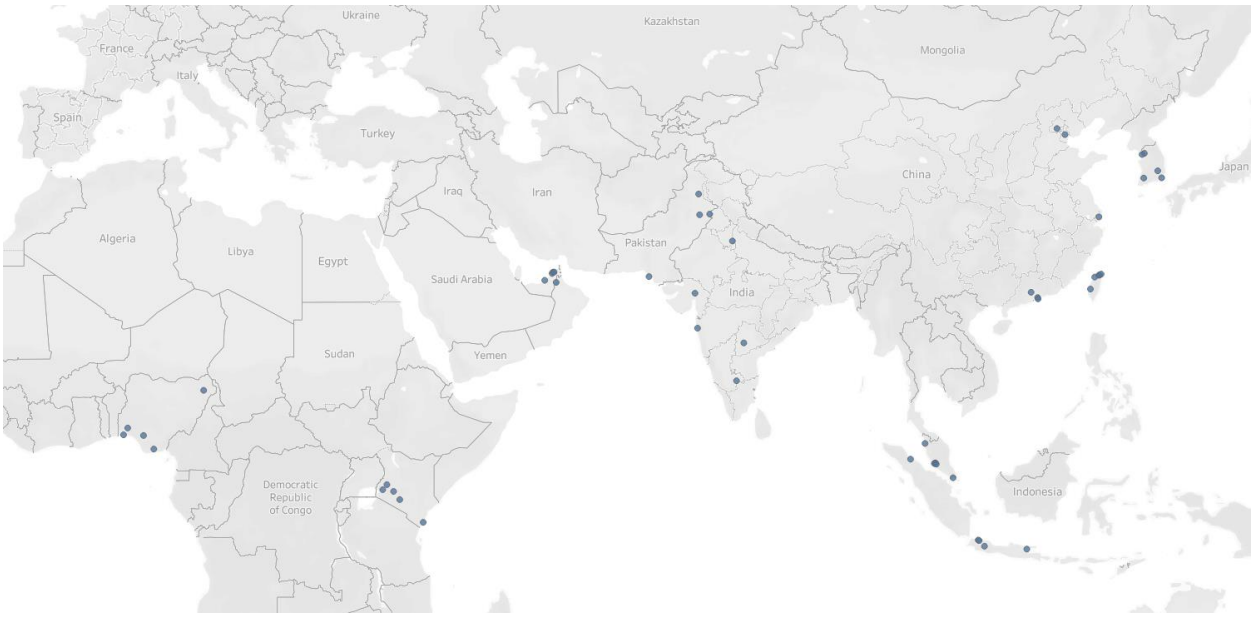
The 3rd Copy & Cyber Vault solutions are estimated to be responsible for transmitting 24+ TB of data East to West and West to East combined as well the storage of 14 days' worth of data; approximately 336TB.

While there are several unknowns that are expected to inform the overall cost of this solution, it is currently estimated to be in the ballpark of USD 1.7M to establish the necessary storage facilities on-prem as well as circa USD 400K on a monthly basis to cleanse, validate and transfer the data to the respective vaults.

SCB Markets

Retail Markets

Country	Current Outlook	10 Year Outlook	Top Five Population Centres
Hong Kong	Top 5 Market	Strategic	Hong Kong
Singapore	Top 5 Market	Strategic	Singapore
Taiwan	Top 5 Market	Strategic	Taipei, Chiayi City, Hsinchu City, Keelung City, New Taipei City
China	Top 5 Market	Strategic	Shanghai, Beijing, Tianjin, Shenzhen, Guangzhou
India	Top 5 Market	Strategic	Mumbai, Delhi, Bangalore, Hyderabad, Ahmedabad,
South Korea		Strategic	Seoul, Busan, Incheon, Daegu, Gwangju
Malaysia		Strategic	Kuala Lumpur, Seberang Perai, Kajang, Klang, Suban Jaya
Indonesia		Strategic	Jakarta, Surabaya, Medan, Bekasi, Bandung
United Arab Emirates		Strategic	Dubai City, Abu Dhabi City, Sharjah City, Al Ain, Ajman City
Nigeria		Strategic	Lagos, Kano, Ibadan, Benin City, Port Harcourt
Kenya		Strategic	Nairobi, Mombasa, Kisumu, Nakuru, Eldoret
Pakistan		Strategic	Karachi, Lahore, Faisalabad, Hyderabad, Rawalpindi



Retail User Journeys and Metrics

Perform Online Banking Transaction – Great Experience (BAU)

Step	Sub-step	Max Step Time (ms)	Average Size MB*
Load Page	1. Load static data 2. Load animated data	• 5,000 (L)	• 4
Login	1. Enter login credentials 2. Initial Authentication 3. Receive 2FA 4. Input 2FA 5. Authenticate 2FA	• 5,000 (L) • 5,000 (M)	• 4 • 0.128
Receive Entitlements	1. Query entitlement server 2. Receive entitlement 3. Set app context to entitlement	• 100 (P)	• None
Load transaction page	1. Request transaction page 2. Load transaction page	• User • 5,000 (L)	• 4
Perform transaction	1. Input transaction value(s) 2. Perform transaction 3. Write transaction to primary database 4. Write transaction to secondary database 5. Pass transaction to application	• User • 100 (P)	• None
Receive transaction confirmation	1. Receive Transaction confirmation	• 100 (P) • 5,000 (M)	• 0.128
Receive supplementary information	1. Receive supplementary information	• 100 (P) • 5,000 (M)	• 0.128
Logout	1. Logout 2. Receive logout information	• 300 (P) • 2,000 (M)	• 0.128

Perform Online Banking Transaction – Degraded Experience (DR)

Step	Sub-step	Max Step Time (ms)	Average User transfer Size MB*
Load Page	3. Load static data 4. Load animated data	• 10,000 (L)	• 4
Login	6. Enter login credentials 7. Initial Authentication 8. Receive 2FA 9. Input 2FA 10. Authenticate 2FA	• 10,000 (L) • 10,000 (M)	• 4 • 0.128
Receive Entitlements	4. Query entitlement server 5. Receive entitlement 6. Set app context to entitlement	• 300 (P)	• None
Load transaction page	• Request transaction page • Load transaction page	• User • 10,000 (L)	• 4
Perform transaction	• Input transaction value(s) • Perform transaction • Write transaction to primary database • Write transaction to secondary database • Pass transaction to application	• User • 300 (P)	• None
Receive transaction confirmation	• Receive Transaction confirmation	• 300 (P) • 10,000 (M)	• 0.128
Receive supplementary information	• Receive supplementary information	• 300 (P) • 10,000 (M)	• 0.128
Logout	• Logout • Receive logout information	• 300 (P) • 4,000 (M)	• 0.128

*https://www.seoptimer.com/blog/webpage-size/
*https://speedcurve.com/blog/web-performance-page-bloat/

Retail Technical Considerations

User satisfaction

User satisfaction is strongly correlated to performance. https://www.nngroup.com/articles/satisfaction-vs-performance-metrics/
This section defines what good experience looks like and explores the quantifiable impact of distance on performance to help inform the site location strategy.

User experience

Google RAIL, the industry standard user-centric performance model, describes the performance metrics related to user experience. Since human perception is relatively constant, these goals are unlikely to change any time soon.

User Perception of Performance Delays	
0 to 16ms	Users are exceptionally good at tracking motion, and they dislike it when animations aren't smooth. They perceive animations as smooth so long as 60 new frames are rendered every second. That's 16ms per frame, including the time it takes for the browser to paint the new frame to the screen, leaving an app about 10ms to produce a frame.
0 to 100ms	Respond to user actions within this time window and users feel like the result is immediate. Any longer, and the connection between action and reaction is broken.
100 to 300ms	Users experience a slight perceptible delay.
300 to 1000ms	Within this window, things feel part of a natural and continuous progression of tasks. For most users on the web, loading pages or changing views represents a task.
1000ms or more	Beyond 1000 milliseconds (1 second), users lose focus on the task they are performing.
10000ms or more	Beyond 10000 milliseconds (10 seconds), users are frustrated and are likely to abandon tasks. They may or may not come back later.

Load Time

https://developers.google.com/web/fundamentals/performance/rail#load
Great User Experience (BAU Experience)
Definition: Optimize for fast loading performance relative to the device and network capabilities that your users use to access your site. **Currently, a good target for first loads is to load the page and be interactive in 5 seconds or less on mid-range mobile devices with slow 3G connections.**
Degraded User Experience (Recovery Experience)
Definition: Optimize for fast loading performance relative to the device and network capabilities that your users use to access your site. **Currently, a good target for first loads is to load the page and be interactive in 10 seconds or less on mid-range mobile devices with slow 3G connections**

Response Time

https://developers.google.com/web/fundamentals/performance/rail#response
Great User Experience (BAU Experience)
Definition: Complete a transition initiated by user input within ***100ms.*** Users spend the majority of their time waiting for sites to respond to their input, not waiting for the sites to load.

Rule: Process user input events within 50ms to ensure a visible response within 100ms
Degraded User Experience (Recovery Experience)
Definition: Complete a transaction initiated by a user input within 100 to 300ms
Rule: Process user input events within 150ms to ensure a visible response within 300ms

CCIB

FM and CIB Markets

FM and CIB Venues

The SCB FM and CIB business have four current and strategic venues that this analysis considers, this was confirmed by the heads of Architecture of both groups, these venues are detailed in the table below.

Country	Current Outlook	10 Year Outlook	Venue
USA	Strategic	Strategic	NYSE, New York
USA	Strategic	Strategic	NASDAQ, New York
Japan	Strategic	Strategic	TSE, Tokyo
UK	Strategic	Strategic	LSE, London
Singapore	Strategic	Strategic	SGX, Singapore

We will consider these venues as “anchor points” of the data processing location strategy and in considering our latency calculations these areas will proxy the areas of high population in the Retail analysis – that is to say we will consider these sites the sites that we calculate acceptable compute paths from. To do this we need to understand a different set of processing requirements that service the FM and CIB businesses.

As NYSE and NASDAQ are very closely located to each other, for the purposes of this document they will be treated as a single location.

SCB Financial Markets Businesses (FM)

The SCB FM business is comprised of the following business units and trade flows:

- FX trading
- Rates trading
- Commodities Trading
- Derivatives Trading
- Bespoke Credit Solutions

Within these solutions we need to understand the flow of the businesses and how that is manifested in application and technologies. If we consider the flow of any order it can we can generalise thus

- Trade Capture & Execution – typically (but not limited to) trade capture, order execution, some order management systems.
- Pricing – typically (but not limited to), price capture, price matching, price publishing
- Post Trade Processing – typically (but not limited to) some order management systems, reconciliations, brokerage, general ledger.

There is a further two axioms that we need to consider when we look at these types of workloads:

- Frequency – high frequency vs low frequency trade capture and order management. High frequency means a very high throughput of messages that needs to reach their destinations in as short a time as possible. In low frequency messages still need to be processed as quickly as possible but they are far less numerous.
- Price sensitivity – the tolerance of the trade to the published value or movement of the value of an asset, in securities trading this is often called the tick, in FX it is the arbitrage of buy sell prices of currencies.

We can generalise a ruleset of technology requirements from these definitions:

Business Type	Workload Type		Frequency	Price Sensitivity (Highly Sensitive to Price change)
FX Trading	Trade Capture & Execution		High	High
FX Trading	Trade Capture & execution		Medium	Medium
FX Trading	Pricing		High	High
FX Trading	Post Trade Processing		High	Low
Rates Trading	Trade Capture and Execution		Medium	Medium
Rates Trading	Pricing		Medium	Medium
Rates Trading	Post Trade Processing		Low	Low
Commodities Trading	Trade Capture & Execution		Medium	Medium
Commodities Trading	Pricing		Medium	Medium
Commodities Trading	Post Trade Processing		Low	Low
Derivatives Trading	Trade Capture & Execution		Medium	Medium
Derivatives Trading	Pricing		Medium	Medium
Derivatives Trading	Post Trade Processing		Low	Low
Bespoke Credit Solution	Trade Capture & Execution		NA	NA
Bespoke Credit Solution	Pricing		Medium	Medium
Bespoke Credit Solution	Post Trade Processing		Low	Low

Taking these as a proxy for a set of requirements and if we remove the business type we are left with the following requirements “buckets”

Workload Type	Frequency	Price Sensitivity (Highly Sensitive to Price change)	Workload Category
Trade Capture & Execution	High	High	TCEHH
Trade Capture & execution	Medium	Medium	TCEMM
Pricing	High	High	PHH
Post Trade Processing	High	Low	PTPHL
Pricing	Medium	Medium	PMM
Post Trade Processing	Low	Low	PTPLL

And we can now assign characteristics to these types of processing, such as

TCEMM	5ms	Store and forward network permissible Multicast permitted Millisecond local hop latency No oversubscription	Virtual permitted No oversubscription 10Gbps
PHH	<1ms (as close as is network possible)	Cut-through networks Multicast permitted Nanosecond local hop latency	Physical compute only. No virtual machines No Oversubscription Highest chipset speed Offload cards (GPU, FPGA)
PTPHL	50ms	Store and forward network permissible Millisecond local hop latency No oversubscription	Virtual permitted No oversubscription 10Gbps
PMM	5ms	Store and forward network permissible Multicast permitted Millisecond local hop latency No oversubscription	Virtual permitted No oversubscription 10Gbps
PTPLL	50ms	Store and forward network permissible Millisecond local hop latency No oversubscription	Virtual permitted Oversubscription permitted 10Gbps

Categorisations in the context of SCB Business

FM Business

Application / Service	Categorisation	Anchor Points
S2BX	TCEHH	LDN,

SCB Transaction Banking (TB)

Requirements match FM & CIB specific content - confirmed by domain specialist architect.

Channels – API – low latency & high frequency (e.g. HK jockey club – 200 / sec transactions)
web, mobile – similar to retail conclusion

Cash Business

Management
Payments – institutional payroll management
Collections – e.g. direct debit

Trade Financing

- open account finance – e.g. back outstanding invoices SUM by providing short term / bridging loans
- documentary finance - letter of credit (old barter system) (physical documents, image scanning, uploading, etc)

Securities

SWIFT type transactions - not low latency, but hard cut-off times apply (3rd party imposed)

SCB Global Banking (GB)

Requirements match FM & CIB specific content - confirmed by domain specialist architect.

CRM
CLDM
CRO
CLM

Global Functions

Global Functions holds several key areas for the bank, these are:

- Human Resources
- Finance and Treasury
- Compliance (Group)
- Legal
- Property
- Audit

Global functions inherit some of the persona bundles outlined in the EUS section, the differences are outlined in this section.

Job Family to Persona Rollup

All the functions within Global Functions can be categorised as Group Business Operations, however we cannot generalise too much here. The Group Business Operations persona will inherit the lowest latency and the highest bandwidth requirement from the job families

Persona	Job Family
Group Business Operations	Human Recourses
Group Business Operations	Compliance
Group Business Operations	Finance & Treasury
Group Business Operations	Legal
Group Business Operations	Property
Group Business Operations	Audit

Characteristics of Workloads per job family

Job Family	Sub	Latency	Bandwidth
Human Resources	-	Medium	Low
Compliance	-	Low	Low
Compliance	Trades	Low	Medium
Compliance	Financial Crime	Low	Medium
Legal	-	Medium	Low
Property	-	Medium	Low
Property	Access Barriers	Low	Low
Property	Access Cards	Low	Low
Property	Security	Low	Low
Property	Cameras	Low	High
Audit	-	Low	Low

A proxy table for a set of requirements without the activity detail we are left with the following requirements “buckets"

	Latency	Bandwidth	Category
Human Resources	Medium	Low	GBOHRML
Compliance	Medium	Low	GBOCLL
Compliance Trades	Low	Medium	GBOCTLM
Compliance Financial Crime	Low	Medium	GBOCFC
Legal	Medium	Low	GBOLML

Property	Medium	Low	GBOPML
Property Access Barriers	Low	Low	GBOPABLL
Property Access Cards	Low	Low	GBOPACLL
Property Security	Low	Low	GBOPSLL
Property Cameras	Low	High	GBOPCLH
Audit	Medium	Low	GBOAML

Generalised characteristics to these types of workloads

Category	Latency	Network	Compute
GBOHRML	<50ms	Cut-Though Permitted Oversubscription Allowed	Virtual Permitted Oversubscription Allowed 1Gbps
GBOCLL	<50ms	Cut-Through Permitted Oversubscription Allowed	Virtual Permitted Oversubscription Allowed 1Gbps
GBOCTLM	5ms	Store and Forward networking permissible Low Latency No over subscription	Virtual Permitted No Oversubscription 10Gbps
GBOCFC	5ms	Store and Forward networking permissible Low Latency QOS – Priority	Virtual Permitted for processing only No Oversubscription 10Gbps
GBOLML	<50ms	Cut-Though Permitted Over subscription allowed	Virtual Permitted Oversubscription Permitted 1Gbps
GBOPML	<50ms	Cut-Though permitted networking permissible No over subscription	Virtual Permitted Oversubscription permitted (low) 1Gbps
GBOPABLL	5ms	Cut-Through permitted Low Latency QOS – Priority No over subscription	Virtual Not Permitted 1Gpbs
GBOPACLL	5ms	Cut-Through permitted Low Latency QOS – Priority No over subscription	Virtual Not Permitted 1Gpbs
GBOPSLL	5ms	Cut-Through permitted Low Latency No over subscription	Virtual Not Permitted 1Gpbs
GBOPCLH	5ms	Cut-Through permitted Low Latency QOS – Priority Separate Network No over subscription	Virtual Not Permitted 10Gpbs
GBOAML	<50ms	Cut-Through permitted Oversubscription allowed	Virtual Permitted 1Gbps

			Oversubscription allowed

End User Services

End User Requirements

Our colleagues work in many different areas and disciplines. This is a consolidated view of all the business areas and roles into an abstracted view of a persona. These personas map to a user experience that directly or indirectly impact their ability to perform their roles based on latency from the data they work with.

Personas

Personas relate the many different jobs within the bank. In the sections below, we show how the persona bundles have been rolled from a job family in to a persona.

Persona Bundles

These represent a generalised view of all the roles with in the organisation which allows us to categorise them in terms of bandwidth and latency requirements.

Generalised rule set for each persona bundle

Persona Bundles	Tools	Latency Band	Data Transfer
Technical Operations Tools	Monitoring Dashboards Putty Clients Database Operations tools Network Operations tools	Low	Low
General Workspace Tools	Email Microsoft Suite Phone Tools Skype Video Conferencing Video to desktop	Low	High
Base Productivity Tools	JIRA Confluence theBridge	Low	Low
Security Operations tools	Security Scanning tools real time logs from systems security alerts	Low	Medium
Development Tools	Eclipse / IDEs SQL Servers (any flavour) Remote Dev Servers	Medium	Low

A proxy table for a set of requirements without the Activity detail we are left with the following requirements “buckets”

Persona Type	Latency Band	Bandwidth	Category
Technical Operations Tools	Low	Low	TOTLL
General Workspace Tools	Low	High	GWTLH
Base Productivity Tools	Low	Low	BPTLL
Security Operations tools	Low	Medium	SOTLM
Development Tools	Medium	Low	DTML

We can now assign characteristics to these types of workloads

Category	Latency	Network	Compute
TOTLL	5ms	Store and forward networking permissible No oversubscription	Virtual permitted Oversubscription allowed 1Gbps
GWTLH	5ms	Cut-Through permitted Low latency No oversubscription Prioritised traffic	Virtual permitted 10Gbps Over subscription allowed for lower use systems
BPTILL	5ms	Cut-Through permitted Low latency	Virtual Permitted 1Gbps Allows a little oversubscription
SOTLM	5ms	Store and forward networking permissible Low latency No oversubscription	Virtual Permitted No oversubscription 1Gbps to 10Gpbs
DTML	10ms	Cut-Through permitted Oversubscription allowed	Virtual Permitted Oversubscription allowed 1Gbps

Describes the latency band and data throughput.

Latency Band

Latency Band	Latency to Processing Site
Low	<10ms
Medium	10ms – 50ms
High	50ms – 200ms

Data Transfer

Data Transfer	Typical Data Transfer per day per Min (KB)
Low	<50
Medium	<3,000
High	<15,000

Characteristics of Workloads

Persona Bundles	**Activity**	**Tool**	**Duration in Mins**	**Characters per min**	**KB per min**
Technical Operations Tools	Debug database	Putty(like)	240	360	0.36
Technical Operations Tools	Debug network	Putty(like)	240	360	0.36
Technical Operations Tools	Debug servers	Putty(like)	240	360	0.36
				Page Size Update KB	
Technical Operations Tools	Monitoring Observations	Monitoring Dashboards	1440	300	300.00
				Technical Operations Tools Subtotal	***301.08***
General Workspace Tools	Function	Tool	***Average Size per Email (KB)***	***Email per day***	
General Workspace Tools	Send Email	Email	75	33.6	2,590.00
	Function	Tool	***Average Size Per Save (KB)***	***Saves per day***	
General Workspace Tools	Microsoft Suite (Save)	Multiple	10000	8	166.67
	Function	Tool	***Average Size per Message (KB)***	***Messages per day***	
General Workspace Tools	Send Receive Instant Message	Skype	35	330	24.06
		Tool	***Average Size per Video Call (KB)***		
General Workspace Tools	Make Video Call	Video	128KB/S (Up) + 512KB/s (down)		9,600.00
		Tool	***Average Per Video (KB)***	***Videos per day (2 per mth)***	

General Workspace Tools	Video to Desktop	Video Streaming	4000	0.066666667	266.67
				General Workspace Tools Subtotal	***12,647.40***
Base Productivity Tools			***KB per update***	***Updates per day***	
Base Productivity Tools	Tickets	JIRA	50	20	2.08
Base Productivity Tools	Documentation	Confluence	2000	4	16.67
Base Productivity Tools	Information Mgmt	Bridge	2000	2	8.33
				Base Productivity Tools Subtotal	***27.08***
Security Operations Tools	Log Correlations	Splunk (Reporting only)	1440	300	300.00
Security Operations Tools	Security Orchestration & response	Phantom	1440	300	300.00
Security Operations Tools	Behavioural Analytics	Splunk UEBA	1440	300	300.00
				Security Operations Tools Subtotal	***900.00***
			KB per update	***Updates per day***	
Development Tools	Java Dev	Eclipse/JetBrains/IDEs	10	200	0.42
Development Tools	Database Dev	SQL Management Studio	300	6000	12.50
Development Tools	Any Dev	Local Dev Servers	300	6000	12.50
				Development Tools Subtotal	***25.42***

Persona to Types of tools

This maps a persona to its tooling bundle

Personas	Persona Bundle
Technical Operations	Technical Operations Tools General Workspace Tools Base Productivity Tools
Infrastructure & Application Development	General Workspace Tools Base Productivity Tools Development Tools
Business Operations	General Workspace Tools Base Productivity Tools
Project Workers	General Workspace Tools Base Productivity Tools
Security Operations	Security Operations Tools General Workspace Tools Base Productivity Tools
Retail Business Operations	Business Operations Tools General Workspace Tools Base Productivity Tools
Risk & Controls Operations	General Workspace Tools Base Productivity Tools
Frontline Sales	General Workspace Tools Base Productivity Tools
Trade Operations	General Workspace Tools Base Productivity Tools
FM Operations	General Workspace Tools Base Productivity Tools
Finance Operations	General Workspace Tools Base Productivity Tools
HR Operations	General Workspace Tools Base Productivity Tools
Treasury Operations	General Workspace Tools Base Productivity Tools
CCIB Business Operations	General Workspace Tools Base Productivity Tools
Cash Operations	General Workspace Tools Base Productivity Tools
Legal Operations	General Workspace Tools Base Productivity Tools

Job Family to Persona Rollup

Takes Job Family, which is the name of each team within the organisation and maps it to an overarching persona.

Persona	Role Family
Business Operations	Support and Administration

Business Operations	Client Support Services
Business Operations	COO
Business Operations	IMO
Business Operations	Implementation
Business Operations	Corporate Lending
Business Operations	Information Management
Business Operations	Non Clerical Support
Business Operations	CFCC Mgmt.
Business Operations	Finance Advisory
Business Operations	Vendor Mgmt.
Business Operations	B&M and Corporate Afrs Mgmt.
Business Operations	Functional Mgmt.
Business Operations	HR Ops & Delivery
Business Operations	Ops Management
Business Operations	Financial Market Ops
Business Operations	Reporting & Analytics
Business Operations	Customer Service
Business Operations	CDD
Business Operations	Retail Banking
Business Operations	Corporate Afrs
Business Operations	Financial & Regulatory Rpting
Business Operations	Business Planning Management
Business Operations	Non-Executive Heads
Business Operations	Research
Business Operations	Product Management
Business Operations	Global Process Mgmt.
Business Operations	Product Mgmt.
Business Operations	Metrics & Performance Mgmt.
Business Operations	Surv., Mon & Investigations
Business Operations	Workplace
Business Operations	Product Advisory
Business Operations	Retail & Distribution Mgmt.
Business Operations	Private Banking Mgmt.
Business Operations	Supply Chain Management
Business Operations	Tax
Business Operations	Biz Continuity & Resilience
Business Operations	Company Secretary
Business Operations	Policy Professional
Business Operations	Reconciliation
Business Operations	Channel Management
Cash Operations	Cash Ops
CCIB Business Operations	CCIB Management
Finance Operations	Accounting Control
Finance Operations	Finance Advisory
Finance Operations	Financial Planning & Analysis
Finance Operations	Tax
FM Operations	Financial Market Ops
Frontline Sales	Origination

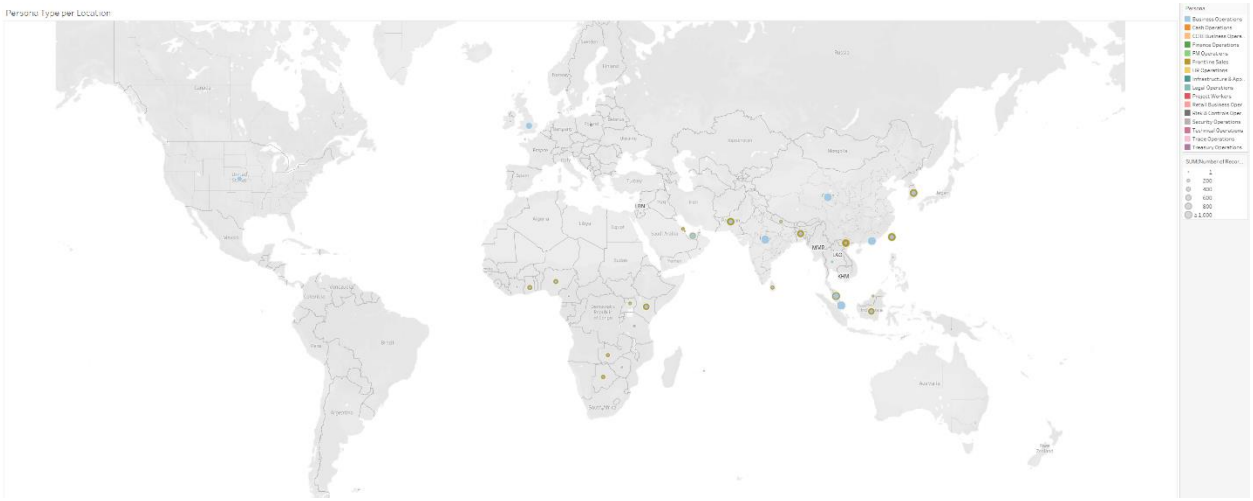
Frontline Sales	Customer Service
Frontline Sales	Sales Support
Frontline Sales	Relationship Mgmt.
Frontline Sales	Sales
Frontline Sales	Service and Advisory
Frontline Sales	Product Sales
Frontline Sales	Trading
Frontline Sales	Distribution
Frontline Sales	Origination&Execution
Frontline Sales	Structuring
Frontline Sales	Execution
HR Operations	Org. & People Capability
HR Operations	HRBP
HR Operations	HR Ops & Delivery
HR Operations	Retail Banking
HR Operations	Talent
HR Operations	PRB
HR Operations	HR Mgmt.
HR Operations	Cyber Defence
Infrastructure & Application Development	App Development & Support
Infrastructure & Application Development	Arch/ Tech Solution Design
Infrastructure & Application Development	Test Mgmt., Assurance & Eng'ng
Infrastructure & Application Development	User Experience Design
Legal Operations	Legal Documentation Mgmt.
Legal Operations	Business / Ctry Legal Counsel
Legal Operations	General Counsel
Legal Operations	Legal Practice Group
Project Workers	Proj. & Programme Management
Project Workers	Change Management & Delivery
Retail Business Operations	Private Banking
Retail Business Operations	Retail Banking
Retail Business Operations	Retail & Distribution Mgmt.
Retail Business Operations	Retail Products
Retail Business Operations	Wealth Management
Retail Business Operations	Corporate Partnerships
Risk & Controls Operations	Control, Process & Governance
Risk & Controls Operations	Risk Approval
Risk & Controls Operations	CEO Office
Risk & Controls Operations	Risk Ops
Risk & Controls Operations	Advisory
Risk & Controls Operations	Financial & Regulatory Rpting
Risk & Controls Operations	Risk Management Team
Risk & Controls Operations	Internal Audit
Risk & Controls Operations	CFCC Advisory
Risk & Controls Operations	Process & Ops Excellence
Risk & Controls Operations	Assurance
Risk & Controls Operations	Audit Mgmt.
Risk & Controls Operations	IMO

Risk & Controls Operations	Biz Continuity & Resilience
Risk & Controls Operations	Data Gov & Mgmt.
Risk & Controls Operations	Surv., Mon & Investigations
Risk & Controls Operations	Global Process Mgmt.
Risk & Controls Operations	CFCC Assurance
Risk & Controls Operations	Safety & Security
Risk & Controls Operations	CLDM
Risk & Controls Operations	Policy Professional
Risk & Controls Operations	Regulatory Compliance
Risk & Controls Operations	Risk Strategy
Risk & Controls Operations	Security Engineering
Risk & Controls Operations	Quality Assurance
Security Operations	Security Services Ops
Security Operations	Surv., Mon & Investigations
Security Operations	Cyber Defence
Technical Operations	Tech Mgmt.
Technical Operations	Tech Ops & Support
Technical Operations	Service Mgmt.
Technical Operations	Infra Eng'ng & Ops
Technical Operations	Data Centre Mgmt.
Technical Operations	Inno, Transformation&Ventures
Technical Operations	Network Management
Technical Operations	Network Eng'ng & Ops
Technical Operations	Cloud Eng'ng&Ops
Technical Operations	Enterprise Mon - Eng'ng & Ops
Technical Operations	Management Graduates
Trade Operations	Trade Documentary
Treasury Operations	Treasury Markets
Treasury Operations	Treasury Risk
Treasury Operations	Treasury BS Opt & Strategy
Treasury Operations	Treasury Capital
Treasury Operations	Treasury Liquidity
Treasury Operations	Rec, Res & Strat Proj.
Treasury Operations	Treasury
Treasury Operations	Modelling & Platforms

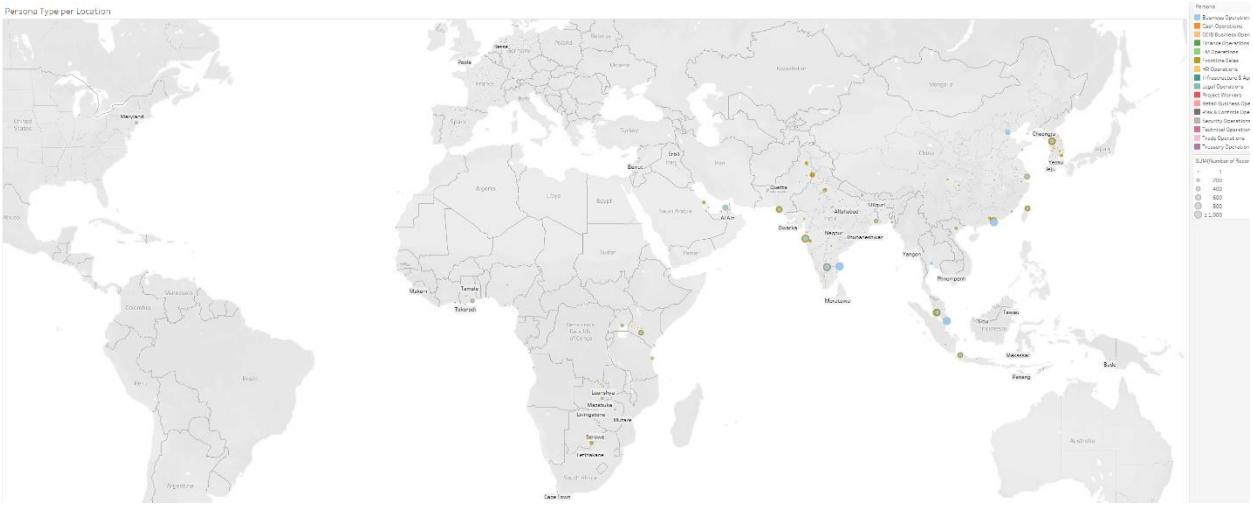
Global Persona Dispersion per Location

Global Persona & Location - raw data

Country view



City view



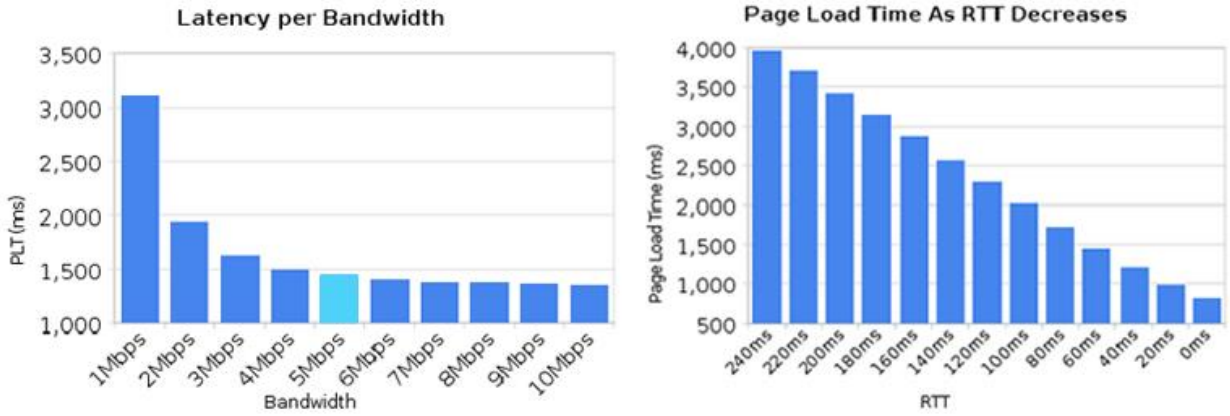
General Technical Considerations

Latency: The new web performance bottleneck

https://www.igvita.com/2012/07/19/latency-the-new-web-performance-bottleneck/

It is often misleadingly suggested that bandwidth = speed, the more bandwidth you have the faster you can consume services on the internet.

"However, the latency graph tells an entirely different story. For every 20ms improvement in latency, we have a linear improvement in page loading times. There are many good reasons for this: an average page is composed of many small resources, which require many connections, and TCP performance of each is closely tied to RTT."



PLTs of 750KB site

Latency Overheads

These overheads vary greatly country to country due to location specifics; for the purpose of this document we will use average values

Mobile Data (2G, 3G, 4G) Latency

50 - 200+ ms

Broadband (FTTP, CABLE, DSL) Latency

10 – 50 ms
https://www.igvita.com/2012/07/19/latency-the-new-web-performance-bottleneck/
https://www.opensignal.com/

Protocols

TCP and HTTP version 1.1

Either via a browser or an app that uses web views (none native app)
In addition to the overhead of latency, the existing transport layer (TCP) and protocol (http) both delays to the equation, this section gives an overview of what this means.

Each TCP connection needs to setup up a TCP session before a http request can be sent over it. This setup is not free (need to collate numbers), it takes time which eats in to the total time that is allotted for a given experience response. The time it takes for the TCP session to be established is also affected by latency, the higher the latency the slower this will take (RTT).

If a site has 10 assets that are needed for an initial page load, it's not that uncommon that the browser engine may use 10 connections to download the content in parallel, so that is 10 * TCP session setups,

which are typically done in parallel. Although this is better than using a single TCP session which must be setup and torn down for each request, it's still not overly efficient use.

There is a lot of complexity around TCP, which is not for this document, but to highlight one area is that short TCP sessions never reach their full potential due to a function called "Slow Start".

More detailed overview: https://en.wikipedia.org/wiki/TCP_congestion_control

Slow start prevents a network from becoming congested by regulating the amount of data that's sent over it. It negotiates the connection between a sender and receiver by defining the amount of data that can be transmitted with each packet, and slowly increases the amount of data until the network's capacity is reached. This ensures that as much data is transmitted as possible without clogging the network.

The point being that the longer the TCP session is up, the more it can self-optimise and use as much bandwidth as possible, latency permitting. Lots of short-lived connections are inherently slow.
How to get better utilization, HTTP2 has been designed with hindsight which has resulted in a much more efficient protocol.

HTTP2

HTTP2 establishes one TCP session, then all HTTP requests are then sent over the one connection using a multiplex technique. This offers several features but allows TCP to optimise itself.

Here are a few features that have been improved to solve the short comings of HTTP1.1

1. Multiplexed (multiple http requests are sent down the same TCP connection) instead of ordered and blocking requests
2. Uses header compression to reduce overhead, see below
3. Allows servers to "push" response proactively into client caches

Multiplexed

HTTP/1.x has a problem called "head-of-line blocking," where effectively only one request can be outstanding on a connection at a time.

HTTP/1.1 tried to fix this with pipelining, but it didn't completely address the problem (a large or slow response can still block others behind it). Additionally, pipelining has been found very difficult to deploy, because many intermediaries and servers don't process it correctly.

This forces clients to use several heuristics (often guessing) to determine what requests to put on which connection to the origin when; since it's common for a page to load 10 times (or more) the number of available connections, this can severely impact performance, often resulting in a "waterfall" of blocked requests.

Multiplexing addresses these problems by allowing multiple request and response messages to be in flight at the same time; it's even possible to intermingle parts of one message with another on the wire.
This, in turn, allows a client to use just one connection per origin to load a page.

Why Just One Connection

With HTTP/1, browsers open between four and eight connections per origin. Since many sites use multiple origins, this could mean that a single page load opens more than thirty connections.

One application opening so many connections simultaneously breaks a lot of the assumptions that TCP was built upon; since each connection will start a flood of data in the response, there's a real risk that buffers in the intervening network will overflow, causing a congestion event and retransmits.

Additionally, using so many connections unfairly monopolizes network resources, "stealing" them from other, better-behaved applications (e.g., VoIP).

Server Push

When a browser or a mobile app that uses web views requests a page, the server sends the HTML in the response, and then needs to wait for the browser to parse the HTML and issue requests for all the embedded assets before it can start sending the JavaScript, images and CSS.

Server Push potentially allows the server to avoid this round trip of delay by "pushing" the responses it thinks the client will need into its cache.

What this means is that, if after loading the initial landing page, using the idle time while the use is looking at the content, the server could push the assets for the next interaction. If we said that every time a user logs in, 80% of the time they want to check a balance, we could set the system up so that once logged in, the server can push the balance information page / assets so when the user selects that feature, the response is conceived as instant.

Some of the information on HTTP2 has been sourced from https://http2.github.io/faq/#general-questions

Networking Terms

Store-and-Forward

Store-and-Forward switching will wait until the entire frame has arrived prior to forwarding it. This method stores the entire frame in memory. Once the frame is in memory, the switch checks the destination address, source address, and the CRC. If no errors are present, the frame is forwarded to the appropriate port. This process ensures that the destination network is not affected by corrupted or truncated frames.

Cut-Through

Cut-Through switching will begin forwarding the frame as soon as the destination address is identified. The difference between this and Store-and-Forward is that Store-and-Forward receives the whole frame before forwarding. Since frame errors cannot be detected by reading only the destination address, Cut-Through may impact network performance by forwarding corrupted or truncated frames. These bad frames can create broadcast storms wherein several devices on the network respond to the corrupted frames simultaneously.

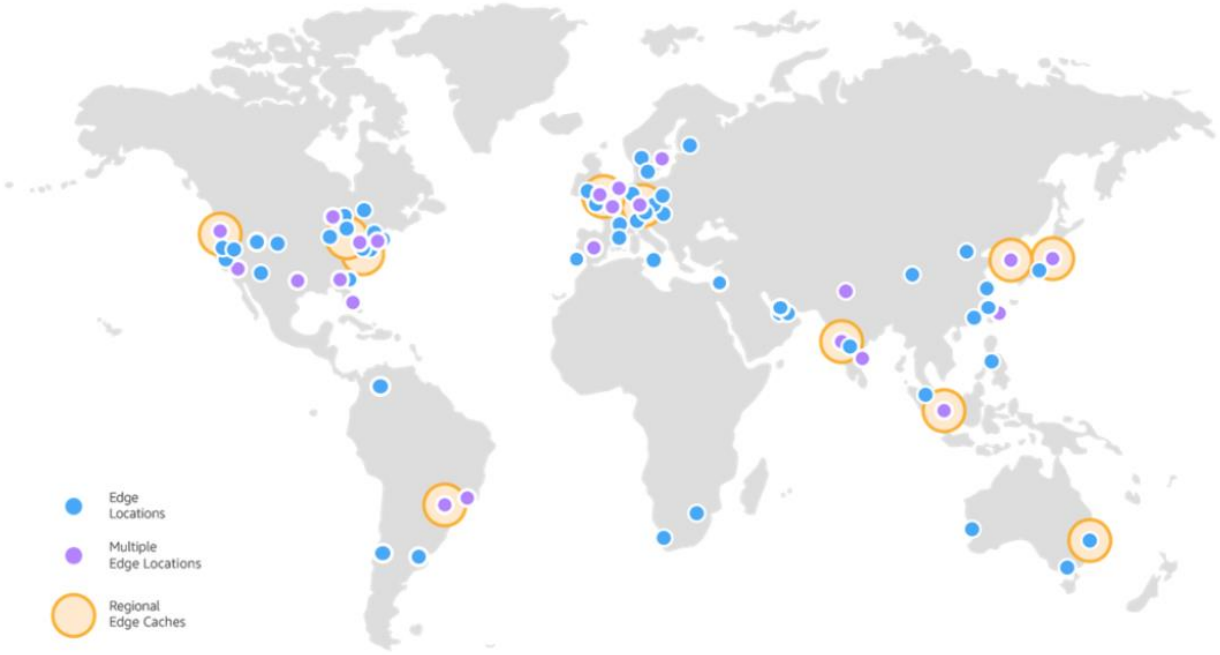
Geo Caching

Geo Cache Market Overview

Akamai

AWS

Amazon CloudFront Infrastructure



Geo Cache Conclusion Summary

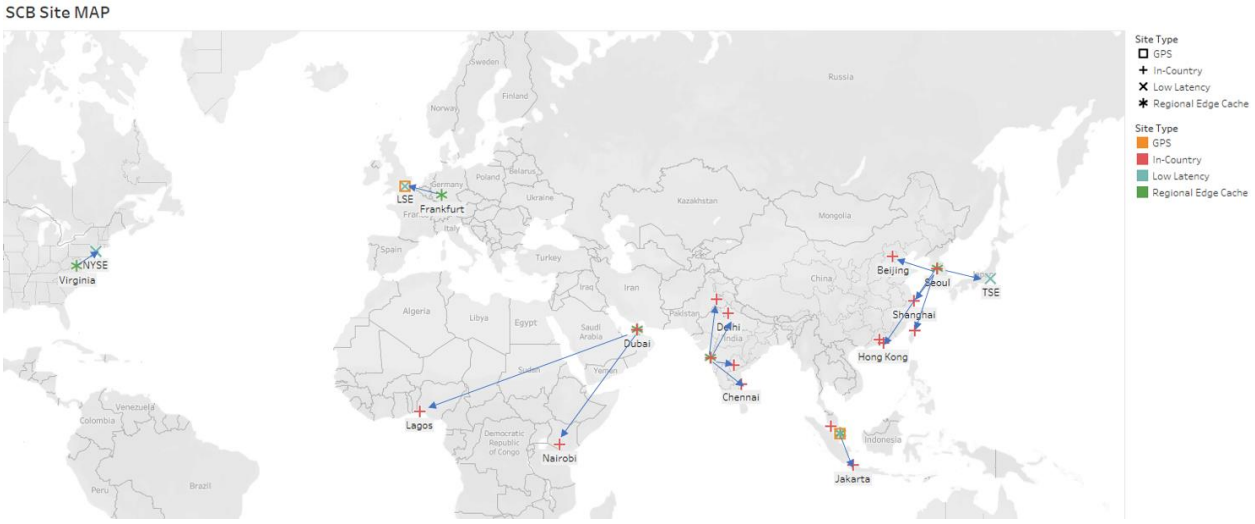
A good way to improve user experience (via performance) is to locate artifacts (i.e. components of the services they consume) geographically as close as possible to them, to reduce the latency. Static content should always be cached using CDNs (content delivery network) and the use of GPS sites should be limited to dynamic calls mostly.

The two leading CDN providers' (Akamai, Amazon) global location maps reveal that their locations, therefore, coverage broadly overlaps and cover most of our retail markets apart from Africa. Only Amazon has presence (limited) in a single country in Africa, South Africa, which may be too far to sufficiently reduce latency for both Kenya and Nigeria.

The African markets (currently Kenya and Nigeria) will most likely have to be served from in-country deployments.

Sample – AWS Regional Edge Caches

Regional Edge Caches reducing first-byte times for strategic markets



Global Processing Sites – Location Considerations – Retail, EUS & Functions

Theoretical Latency Analysis

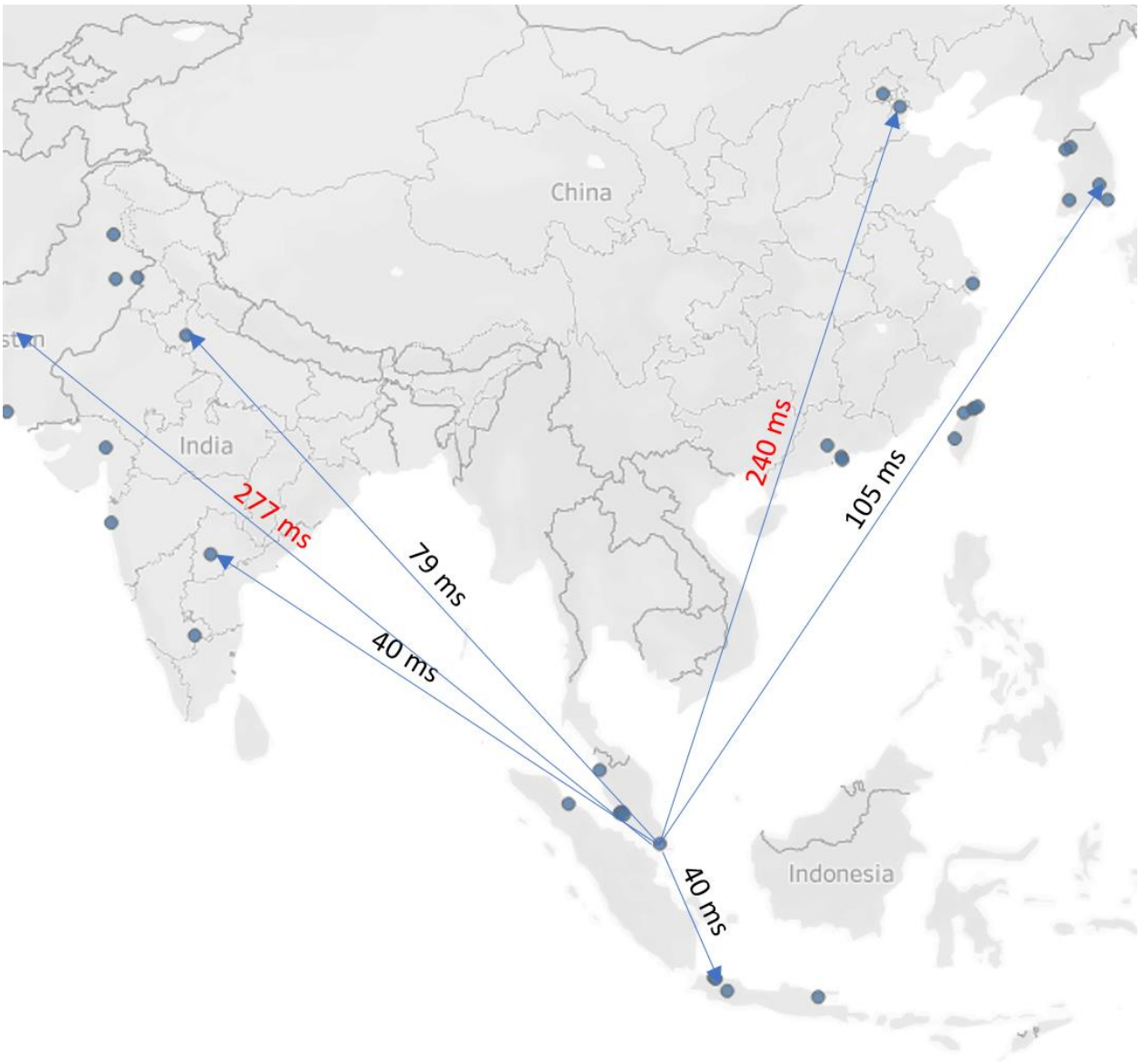
User experience is strongly related to latency, therefore distance. It is possible to employ technologies, such as CDNs, WAN accelerators, Geo caches to bring static content as well as optimise application experience in a manner that reduces the "distance effect" between consumer and application, calls to dynamic data sources like databases, however, will inevitably be impacted by latency. **SCB Global Processing Sites (GPS)**, hosting back-ends for business systems (amongst other things), **must therefore be positioned in a way that enables them to support a great user experience initiative for all strategic markets.** A moderate, sub 200 ms RTT mandates a theoretical distance of no greater than 3710km; depicted by 3710km radius circles.

The overlap of 3710km radius circles around SCB retail markets help determine the ideal positioning of SCB Global Processing Sites. The overlap of circles reveal darker, less transparent areas highlighting potential regional hotspot locations (Golden Triangles) for further consideration.

Simplified View of Golden Triangles

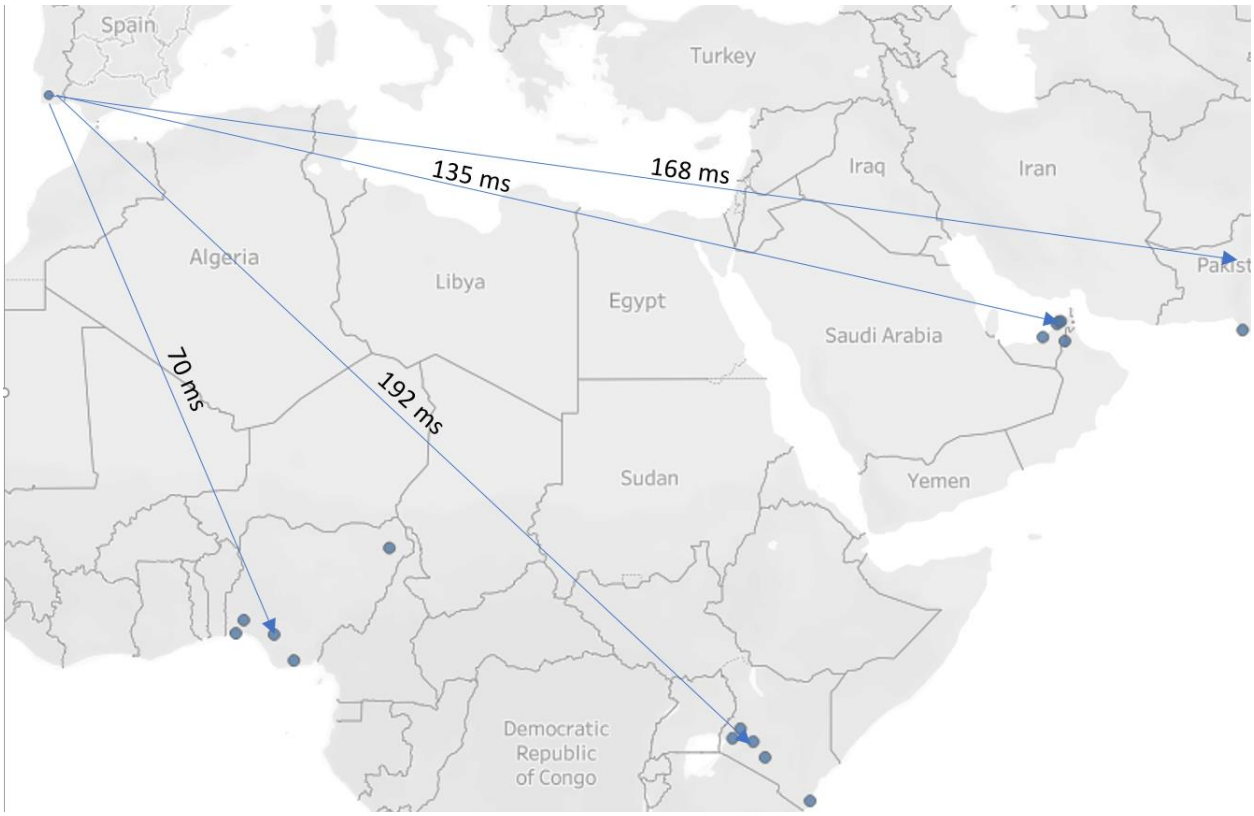
Actual APAC Latency View

	Hyderabad	Jakarta	Lahore	New Delhi	Seoul
Singapore	48.078ms	12.547ms	277.452ms	78.655ms	135.668ms



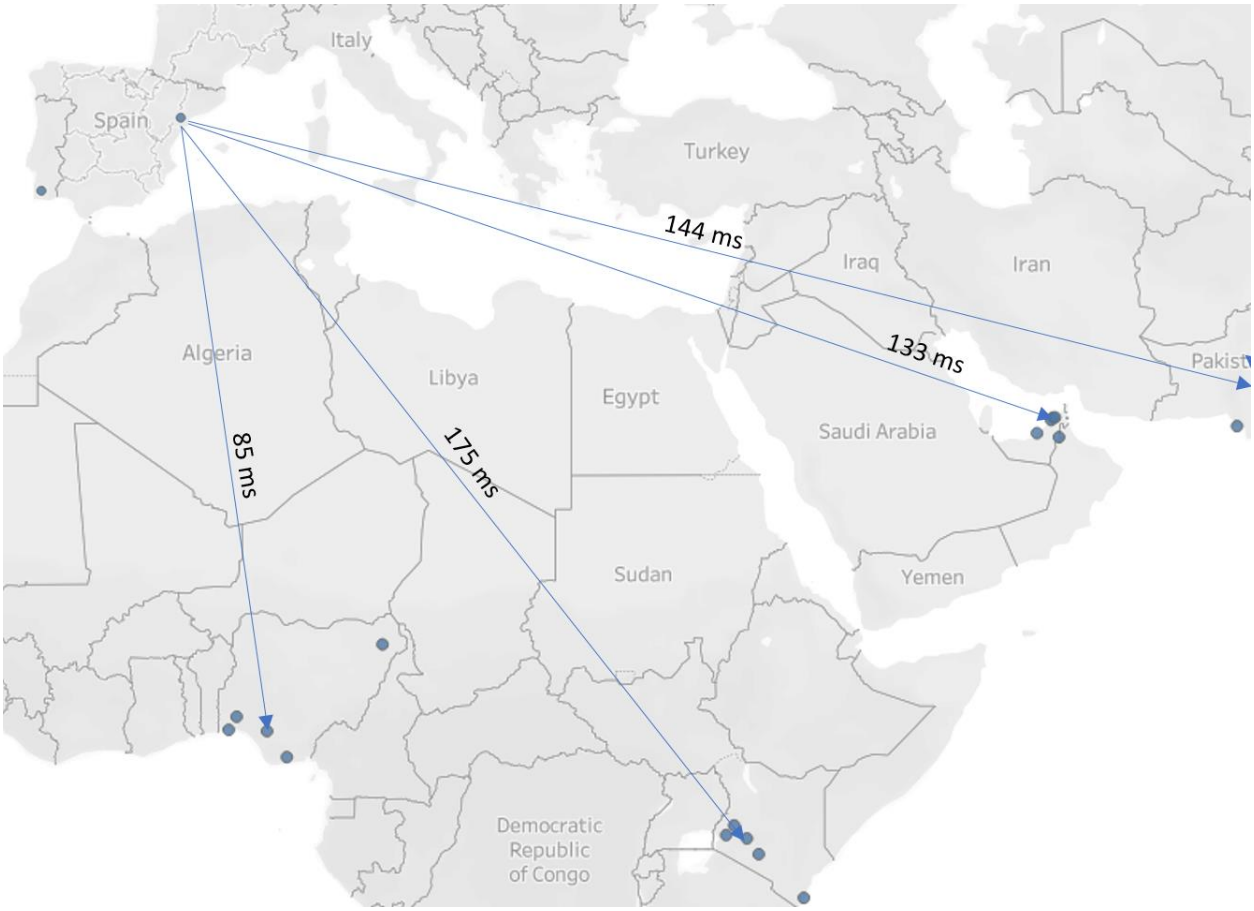
Actual EU1 Latency View

	Dubai	Lagos	Lahore	Nairobi
Lisbon	136.043ms	69.411ms	167.939ms	192.022ms



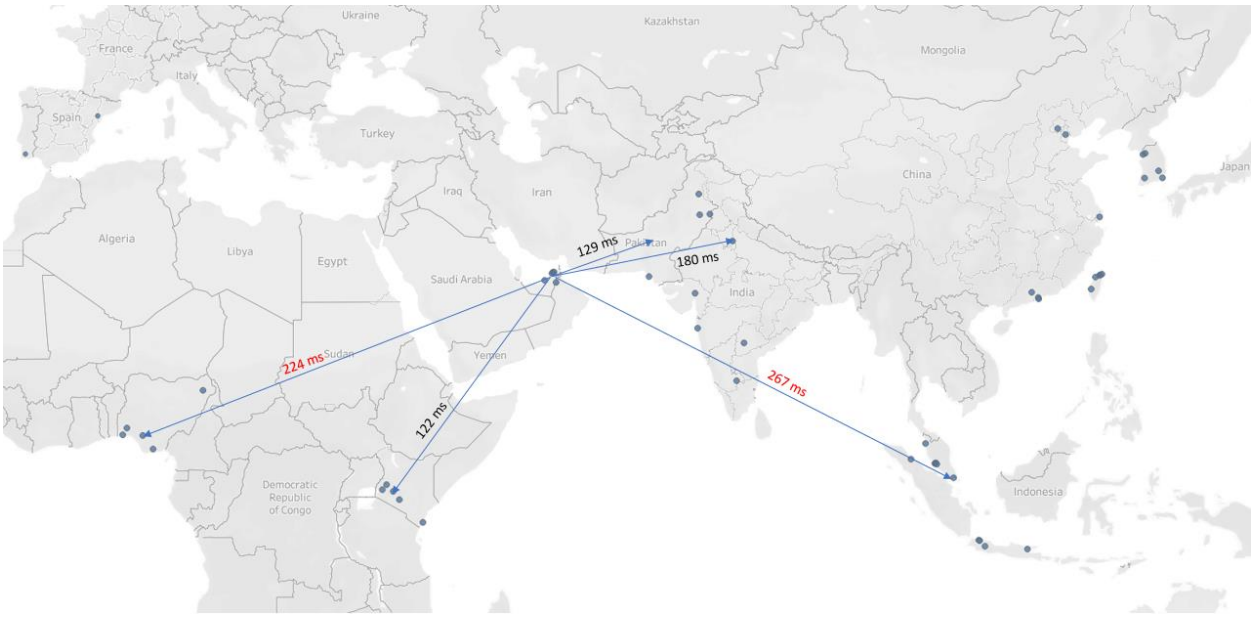
Actual EU2 Latency View

	Dubai	Lagos	Lahore	Nairobi
Barcelona	133.077ms	84.534ms	144.097ms	174.9ms
Lisbon	136.157ms	69.453ms	167.995ms	192.363ms

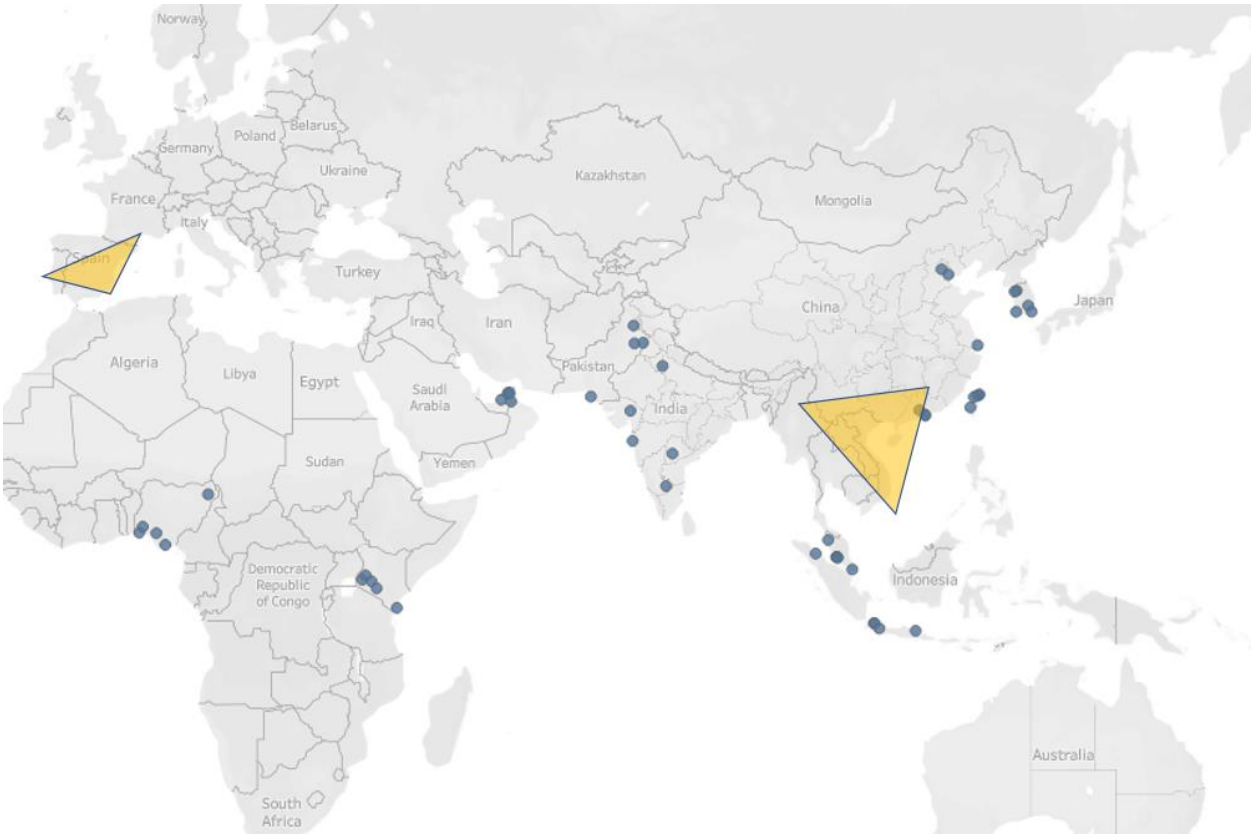


Actual ME Latency View

	Lagos	Lahore	Nairobi	New Delhi	Singapore
Dubai	223.855ms	130.253ms	121.889ms	180.733ms	265.953ms



Simplified View of Golden Triangles



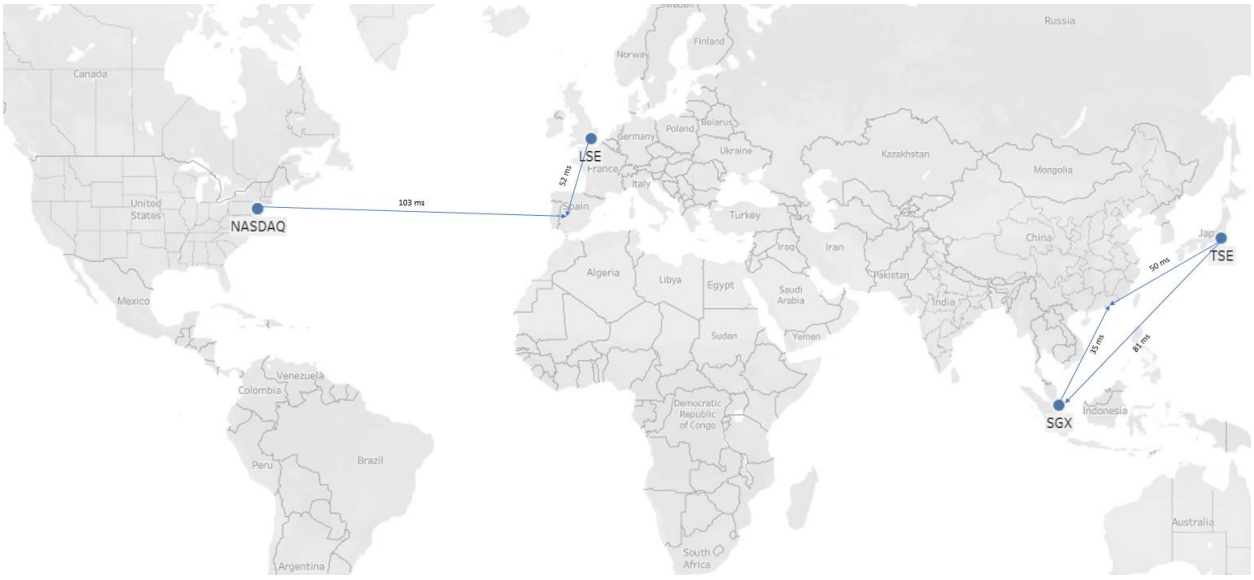
Global Processing Sites – Location Considerations – FM & CIB View

Theoretical Latency Analysis

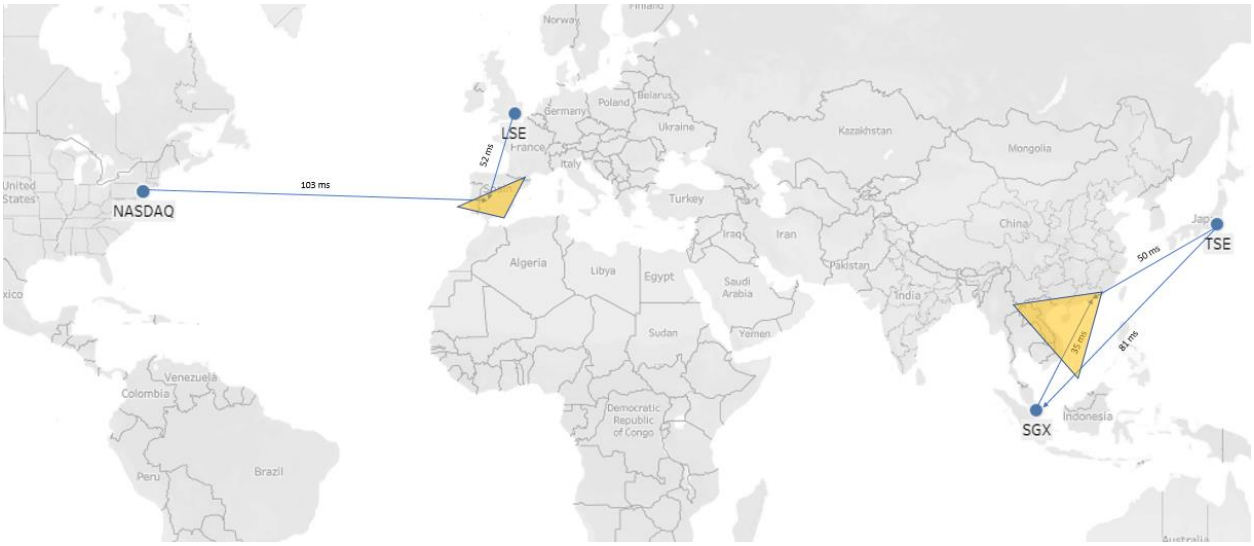
FM & CIB requires specialised **low-latency co-locations** as close to exchanges as possible. They are expected to back up to GPSs and be within 100ms latency.

Actual FM Latency View

	Barcelona	Lisbon
London	28.035ms	51.437ms
New York	103.28ms	113.824ms
	Hong Kong	**Singapore**
Singapore	34.497ms	—
Tokyo	50.171ms	80.63ms



FM adherence to golden triangles



NASDAQ, NYSE and LSE are within async tolerance of the EU golden triangle
Both TSE and SGX are within async tolerance of the APAC golden triangle

Global Data Processing Location Summary

APAC

The gold triangle for ASIA suggested VIETNAM & HK. I also included Singapore in the suitability assessment.
HK & Singapore seem the be the ideal location for the ASIA GPSs, both have downsides though
Latency to China is above the 200ms threshold from all locations but HK
Singapore has surprisingly low latency to all of India (east, west north, south)
HK to Mumbai is above the 200ms threshold
Hanoi is unable to service South Korea with circa 240ms latency, both HK and SG can do with sub 110ms

MEA

The original intension of placing a GPS was to service Africa and potentially west India and Pakistan.
Regardless of the close proximity from:
Dubai to India, most locations suffer from a 100ms-200ms latency, Mumbai @ 284ms
Dubai to Africa is also a controversial choice. While Kenya is within 157ms; Nigeria is above 220ms

EU

Against all odds backed by theory and intuition suggested by looking at the map an EU-based (south) GPS could be a very good option.
Lisbon and Barcelona are both within the 200ms tolerance for both Nigeria (sub 100ms) and Kenya (sub 200ms) as well as Dubai @ ~130ms and various locations in India all within 200ms.

Data Strategy Considerations

It is expected the SCB employs a sound data backup strategy which includes a 3rd Copy Site, that is geographically far enough to reduce geo-risk but close enough to facilitate sufficient data throughput and support asynchronous database backups along RTO & RPO aspirations of all business-critical applications not covered by synchronous backups.

Data Transfer and Latency

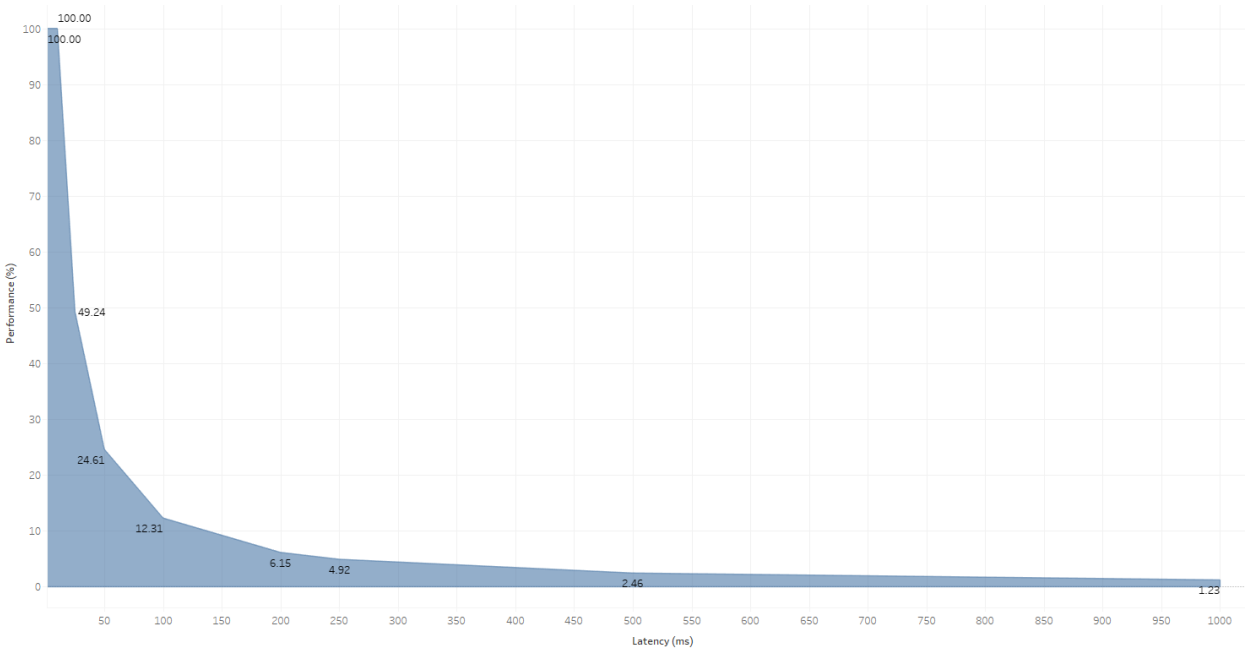
Maximum possible transfer rate, broadly speaking, is calculated as follows:
Maximum Possible Transfer Rate = TCP Window Size/RTT; where RTT is Ping Response in Milliseconds/1000
While TCP window size is a variable and some systems support dynamic TCP widow scaling many do not, therefore, we will treat it as a constant (64K)
As a result, the most significant factor determining data transfer rates is the distance between source and destination.
Examples:

1. Singapore – Singapore (0 km)

A low latency local Ping time from Singapore to Singapore: 1ms. Therefore, RTT= 1/1000= 0.001
Maximum Possible Transfer Rate = 64 / 0.001 = 64000 Kilobytes/sec or 512 Mbps (Remember: 1 byte = 8 bits)

2. Singapore – London (~10000 km)

Ping time from Singapore to London, UK: 200ms. Therefore, RTT= 200/1000= 0.2
Maximum Possible Transfer Rate = 64 / 0.2 = 320 Kilobytes/sec or 3.125 Mbps (Remember: 1 byte = 8 bits)
This suggests that for a single data stream (e.g. FTP) a circuit size exceeding maximum transfer rates will not result in faster transfer speeds. It doesn't matter how big the circuit is.
The distance (circa 10000km each way) results in 200ms latency which leads to significant performance degradation. The transfer rate over this proximity is 6.1% of the rate of local data transfer.
The diagram below describes the exponential nature of performance degradation over distance (latency)



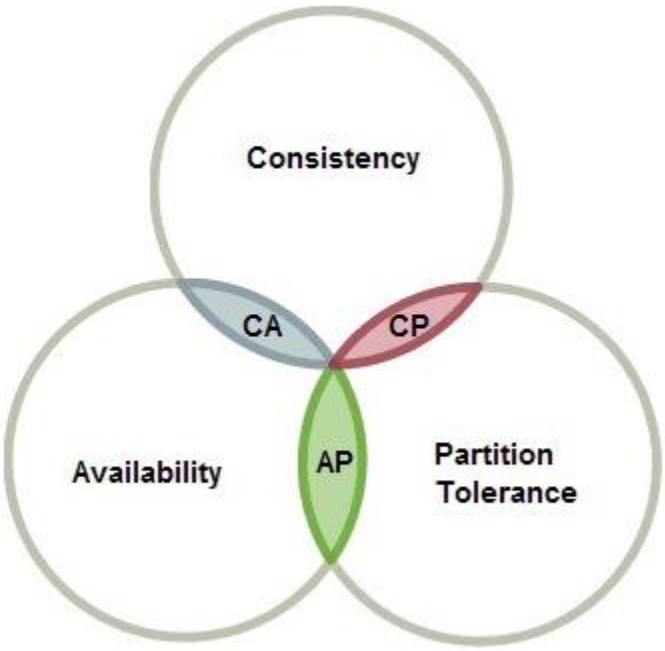
Effective Throughput.

Based on point to point connection through fibre. (theoretical maximums)

RTT in Ms-->	<=1	2.5	5	10	25	50	100	150	200	250
Distance in KM	74	185	371	742	1,855	3,710	7,420	11,130	14,840	18,550
Distance in Miles	46	115	231	461	1,153	2,306	4,611	6,917	9,223	11,529
Effective Bandwidth as %	100.00	97.46	94.92	89.85	49.24	24.61	12.31	9.24	6.15	4.92

CAP Theorem

"states that it is impossible for a distributed data store to simultaneously provide more than two out of the following three guarantees" – therefore a compromise must be made
https://en.wikipedia.org/wiki/CAP_theorem
https://towardsdatascience.com/cap-theorem-and-distributed-database-management-systems-5c2be977950e



ICS TRP Threat Scenarios

Threat Scenario Mitigation and CAP (CP) Adherence

Threat Scenario Title	Summarized Impacts: EAI (End Availability Impact) for Cyber Threats Potential Impact / System Risk Potential for Physical Threat	Resilience Mode (Available / Recovery)	CAP - Consistency	CAP - Partition Tolerance
Component Loss	Loss of standalone system	Available - Achieved through Resilience pattern	Preserved	Preserved
Deployment Loss	Loss of full stack of application	Available - Achieved through Resilience pattern	Preserved	Preserved
Hub Loss (Country Loss)	Country isolation due to loss of entire hub location	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved

Local data corruption	Loss of data due to corruption on local system	Available - Achieved through Resilience pattern	Compromised - cannot make RPO0 will be async	Preserved
Local Network Loss	Loss of local network	Available - Achieved through Resilience pattern	Preserved	Preserved
Major Data Corruption (Regional)	Loss of data due to major data corruption on infrastructure across entire region	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Major Network Loss (Country Isolation)	Country Isolation due to loss of network connectivity	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Major Network Loss (Regional Isolation)	Region isolation due to loss of network connectivity	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Primary Site Outage	Loss of entire primary site	Available - Achieved through Resilience pattern	Preserved	Preserved
Region Loss (Physical Disaster)	Loss of entire region due to physical disaster	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Compromised of Third-Party Software leading to Fraudulent Transfers	**Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover** **Hardware/ Firmware Destruction/ Corruption** **Hardware/ Firmware Manipulation**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved

Ransomware As a Smokescreen for Fraudulent SWIFT Transfers	**Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
DDoS Attack to Cause Operational Disruption + Data Exfiltration of Sensitive Information	**Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover** **Network Disruption/ Disconnection**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Web-based Attack to Steal Customer Data	**App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Firewall Misconfiguration leading to Data Breach	**Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Insider Collusion	**Business Data*** Manipulation/ Encryption**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved

Hacktivist Website Defacement	**App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	CyberVault	Compromised - cannot make RPO0 will be async	Preserved
Denial of Service Campaign	**Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover** **Network Disruption/ Disconnection**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
ATM Malware Campaign	**Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover** **Hardware/ Firmware Manipulation**	CyberVault	Compromised - cannot make RPO0 will be async	Preserved
Supply Chain Compromise of Banking Infrastructure	**Business Data*** Manipulation/ Encryption** **App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	CyberVault	Compromised - cannot make RPO0 will be async	Preserved

Insider Data Exfiltration	**Business / Systems Data Destruction/ Corruption** **Business Data*** Manipulation/ Encryption** **App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	N/A	N/A	N/A
Compromised Applications Leading to Loss of Service	**Business / Systems Data Destruction/ Corruption** **Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Corruption/ Encryption/ Destruction** **App/ System Identities or System Ownership Takeover**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Web-based Attack to Steal Funds	**Business Data*** Manipulation/ Encryption** **App/ System Identities or System Ownership Takeover**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Destructive Malware Causing Operational Disruption	**Business / Systems Data Destruction/ Corruption** **Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved

Operational Disruption of Online Trading Channels	**Systems Data*** Manipulation/ Encryption** **App/ System Software Corruption/ Encryption/ Destruction** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	Recovery - requires 3rd Site	Compromised - cannot make RPO0 will be async	Preserved
Insider Data Exfiltration	**Business Data*** Manipulation/ Encryption**	N/A	N/A	N/A
Compromise of Financial Regulator Leading to Fraud	**Business Data*** Manipulation/ Encryption** **Systems Data*** Manipulation/ Encryption** **App/ System Software Manipulation** **App/ System Identities or System Ownership Takeover**	NOT IN SCOPE	NOT IN SCOPE	NOT IN SCOPE
Breaks in internal process and controls	NOT IN SCOPE	NOT IN SCOPE		
Resiliency awareness	NOT IN SCOPE	NOT IN SCOPE		

Consistency

Recovery Point Objective

The recovery point objective (RPO) is the amount of time that a consistent copy of data at the secondary site can lag the current data at the primary site.
Availability RPO – Close to 0
Recovery RPO - 15

Recovery Time Objective

The recovery time objective (RTO) is the amount of time in which essential business processes must be up and running again after a disaster. The IT component of the RTO is the time it takes to recover the most recent consistent copy of data

We must prioritise CP

Consistency - A read is guaranteed to return the most recent write for a given client.
Partition Tolerance - The system will continue to function when network partitions occur

Partition Tolerance

Local Partition Tolerance

Where a network is partitioned locally, for example the loss of a write master or the loss of network then we must implement one of two mechanisms to protect.

1. Message replay – where the application understands the state of messages sent to the data layer for processing and is also able to store and replay when a failure event happens to mitigate the interruption of the infrastructure whilst it reconfigures to become available again
2. High availability – where the processing of data is made fault tolerant by the implementation of highly available architecture. In theory local high availability can be achieved in a single site but this is becoming less and less viable given the complexity and cost of bespoke clustering technologies.

In-Country Partition Tolerance

The configuration of the In-Country site will influence the response to recover from a total failure, these are
Single In-Country site setup:

1. High availability would not be available in a single site configuration, restoration would be required
2. restoration would be from the closest 3rd copy location to restore the most immediate data.
    a. this depends on if applications can function with the amount of data that is buffered in the 3rd copy (this is a rolling window of time)
    b. if applications need all historic data to function, then go to no 2
3. Historical data would be restored from the countries subscribed GPS

Multiple In-Country sites setup:

1. Message replay – where the application understands the state of messages sent to the data layer for processing and is also able to store and replay when a failure event happens to mitigate the interruption of the infrastructure whilst it reconfigures to become available again

2. High availability – where the processing of data is made fault tolerant by the implementation of highly available architecture
3. Restoration would be from the remaining In-Country site via resync. As having multiple In-Country sites inherently means they are a redundant pair.

If there is corrupted data or data loss due to a human error, then restoring from the 3rd Copy, falling back to the subscribed GPS for data restore

Regional Partition Tolerance

If we have a region failure, the only option we have is to either:

1. Design a highly available system which build in fault tolerance across regions, but due to the complexity involved and data residency issues we have to resort to a restore
2. Restore from:
    a. The remaining healthy GPS
    b. Cyber vault

Global Partition Tolerance

In the event we lose East or West due to a unexpected event, though very unlikely, but if it did happen, you can argue, you have bigger / other problems to worry about. However, the only course of action for this would be to restore from the Cyber Vault which is hosted in between the east and west.

Replication Types

https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/Storage_Networking_Across_The_MAN_WAN.pdf

Synchronous Replication

I/O service time is defined as follows

Transaction	Local Storage Sequence	Remote Storage Sequence
Commit 1st Transaction	Write request to LUN	
	LUN ready for transfer	
	Transfer data	
		Write request to LUN
		LUN ready for transfer
		Transfer data
		Confirm write
	Confirm write	
Commit 2nd Transaction		

The 2nd transaction cannot be committed until the first transaction has both write confirmations, the time between the first and second transaction time is the I/O service wait time

Asynchronous Replication

I/O Service time is defined as follows

Transaction	Local Storage Sequence	Remote Storage Sequence
Commit 1st Transaction	Write request to LUN	
	LUN ready for transfer	
Commit 2nd Transaction	Transfer data	
		Write request to LUN
		LUN ready for transfer
		Transfer data
		Confirm write
	Confirm write	

The 2nd transaction does wait for the first transaction confirmations, the time between the first and second transaction time is the I/O service wait time.
Synchronous replication guarantees data consistency but comes with a performance overhead that is predicated by the size of the data being transferred and the distance it needs to cover. Data is consistent, and its state is known by knowing the state of the master.
Asynchronous replication does not guarantee data consistency and comes with the issue of eventual consistency, that is the data is not guaranteed to be at a known state at any time the flow of transactions. The data state can only be known upon inspection of the replica.

Replication Latency Tolerance

https://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-080-art-data-replication-487868.pdf
https://www.oracle.com/technetwork/database/availability/sync-2437177.pdf
Data replication and its tolerance to latency is not an exact science, multiple factors limit a systems tolerance to latency including the protocol(s) used, the size of data transferred, the physical distance travelled and the application tolerance to latency.
It is therefore impossible to give a "one size fits all" concept of latency tolerance however the rule of thumb that is generally accepted across the industry is that 5ms is the largest latency that synchronous replication mechanisms can tolerate – given we cannot factor all of the workload types and data sizes in scope it is safer to half this number to 2.5ms for synchronous; this is from the second paper:

"Each application will have a different tolerance for synchronous replication. Differences in application concurrency, number of sessions, the transaction size in bytes, how often sessions commit, and log switch frequency – result in differences in impact from one application to the next even if round-trip network latency (RTT), bandwidth and log file write i/o performance are all equal. In general Oracle sees customers having greater success with synchronous transport when round trip network latency is less than 5ms, than when latency is greater than 5ms. Testing is always recommended before drawing any specific conclusions on the impact of synchronous replication on your workloads."

For Asynchronous replication:
https://www.dell.com/community/Replication-Manager/Distance-for-sucessful-replication/td-p/6782307?attachment-id=21098

and as the accepted rule of thumb is 50ms for asynchronous replication, again to be cautious we will use 25ms

Replication Type	Maximum Return Trip Time (RTT)	Maximum Distance in Miles / KM
Synchronous(+)	**2.5 ms**	77 / 124
Asynchronous(*)	**50 ms**	1440 / 2,474

(+) (2.5ms * (Speed of light 299,000KM's * Glass Attenuation Factor @ 66%) / 2 RTT)
(*) (15ms * (Speed of light 299,000KM's * Glass Attenuation Factor @ 66%) / 2 RTT)

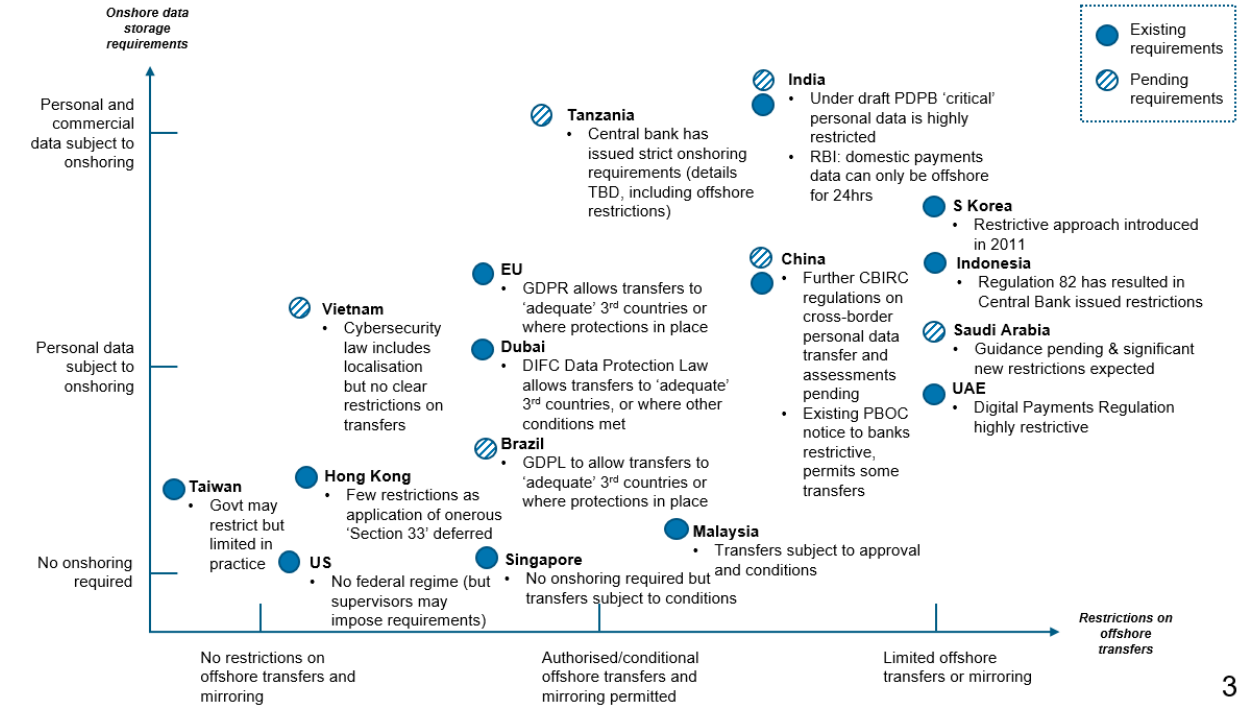
Implication to BC Rating of Applications
BC5 applications are obliged to maintain an RPO of 0 (or close to). Therefore BC 5 applications Production and Disaster Recovery (Availability) sites may be no more than 77miles / 124 Km apart.
BC4 applications are obliged to maintain an RPO of 0 (or close to). Therefore BC 5 applications Production and Disaster Recovery (Availability) sites may be no more than 77miles / 124 Km apart.

Data Localisation

Regulation governing data localisation varies on a country-by-country basis and expected to be a constant moving target. The scatter plot below depicts the understanding as of Q4 2019.
Thorough understanding of country-by-country regulatory requirements will have to inform data backup and replication strategies.

Data localisation - comparing key markets

A snapshot of onshore storage requirements and additional restrictions on offshore transfers



3

Bank Processing Run Levels

Bank Processing Run Levels categorise the Bank's capabilities to function viably to meet the needs of Regulators and to service the needs of its clients.
The Run levels also have associated rules with them about how and where processing can be executed, where pilot light infra must be maintained and where original configurations must be stored.

Run Level One

Run level one is the technology services that enable basic communication and collaboration between SCB staff and whose recovery must be prioritised first in the event of a major disruption.
The establishment of run level one services acts as enablement of all other services that the Bank must establish to regain functionality in the event of disaster.

Run Level Two

Run Level Two is the technology services that enable the Bank to bring up Business Critical Services and Systemic Risk Applications.
The establishment of Run Level Two services allows for the establishment in a cascading order of more complex services in order to restore Regulatory and Bank Critical Processing.

Run Level Three

Run Level Three is Systemic Risk Applications and Business Critical Services.
The establishment of Run Level Three allow the Bank to fulfil its obligations to our various regulators and to the market. The second phase of run level three established critical BAU processing to re-establish BAU and client processing.

Run Level Four

Run level Four is Business Defined client servicing Applications and Services.

Run Level Five

Run Level Five is Business Defined non-client servicing Applications and Services

Run Level Six

Run Level Six is any other Application and Services

Run Level Detailed Table

Level	Capabilities	Gold Configuration Held	Initial Recovery Target	BAU Workload Execution
1	1. SCB Core Services 1.1. Active Directory (end user and system) 1.2. Network Services 1.2.1.DNS 1.2.2.DHCP 1.2.3.User Proxy's 1.2.4.System Proxy's 1.2.5.Firewalls 1.2.6.Network Load Balancing 1.3. End User Services 1.3.1.Critical Voice Services 1.3.2.Skype for business 1.3.3.Email 1.3.4.Documentation Systems	• Global Processing Site (GPS)	• Global Processing Site (GPS)	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – performance replicas only. • Cloud Service Providers (CSP) – performance replicas only.
2	1.1. Platform Hardware 1.1.1.Private Cloud, 1.1.2.VMWare 1.1.3.Solaris/AIX 1.1.4.Physical servers 1.2. Platforms 1.2.1.Build 1.2.2.Provisioning 1.2.3.Automation tools 1.3. Shared Services 1.3.1.DAAS 1.3.2.WAAS 1.3.3.EMS – Monitoring tools 1.3.4.Security – PIM, NIDS 1.4. Cyber Vault – air gap replay service to recover bank config and business 1.5. Security	• Global Processing Site (GPS)	• Global Processing Site (GPS) • In-Country Processing Site	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – performance replicas only. • Cloud Service Providers (CSP) – performance replicas only.

	1.5.1.PIM 1.5.2.NIDS 1.5.3.AVM 1.5.4.DLP 1.5.5.MP 1.5.6.CTI 1.5.7.CDC 2. Application & Infrastructure config – 2.1. Vx and 2.2. Ancillary pipeline tools 3. Platform tools – 3.1. Automation tools 3.2. SCCM 3.3. SCOM, 4. EMS – Monitoring tools 5. Foundation Services – 5.1. MQ, 5.2. EDMI/P, 5.3. FileNet, 5.4. CBIS, 5.5. MDIS			
3	1. Bank Wide Systemic Risk Applications 2. Shared Business Critical Applications 3. Retail Business Critical Applications 4. FM/CIB Business Critical Applications 5. Functions Client Servicing Applications	• Global Processing Site (GPS)	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – execution only • Cloud Service Providers (CSP) – execution only	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – execution only • Cloud Service Providers (CSP) – execution only
4	1. Retail Client Servicing Applications 2. FM/CIB Client Servicing Applications 3. Functions Client Servicing Applications	• Global Processing Site (GPS)	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – performance replicas only.	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – performance replicas only.

			• Cloud Service Providers (CSP) – performance replicas only.	• Cloud Service Providers (CSP) – performance replicas only.
5	1. Retail BAU Business Applications 2. FM/CIB Business Servicing Applications 3. BAU Business Applications	• Global Processing Site (GPS	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – performance replicas only. • Cloud Service Providers (CSP) – performance replicas only.	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – performance replicas only. • Cloud Service Providers (CSP) – performance replicas only.
6	Everything else	• Global Processing Site (GPS	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – performance replicas only. • Cloud Service Providers (CSP) – performance replicas only	• Global Processing Site (GPS) • In-Country Processing Site (CPS) – performance replicas only. • Cloud Service Providers (CSP) – performance replicas only.

Data Processing Site Types

Processing Site Types Specifications

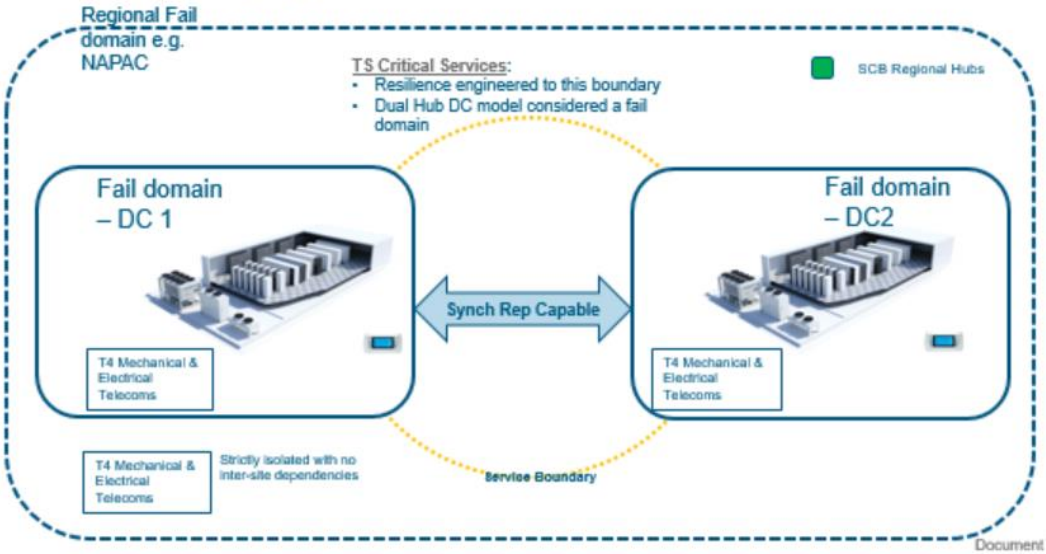
Site Type	Global Processing Site (GPS)	In-Country Processing Site (CPS)	Low Latency Site	3rd Copy Site	Cyber Vault
Description	• House core services • Offers a great experience for end user and resiliency • Offers core services (see run levels)	• 1 or 2 locations depending on size and strategic relevance of the country • if cloud, min two AZs • 1 or more 4 tier locations used in country if: • a GPS too far away to provide great service • data sovereignty • data processing must occur in country • will subscribe to a GPS for core services • if distance is an issue, then CPS will also hold local	Specialist use case • Mostly for low latency trading • Minimum set of services required. • most likely have local caches / supporting services • may Subscribe to SPS to backend processing / fulfilment	• Site to support GPS with off-site data storage capabilities for DR scenarios • Data must not be authored at this site • Data must e	• Site specific to serve as “air gapped” store of all backups from 3rd copy sites

		read only caches or core services			
Specification	• two or more tier 3+ certified DCs • 8 km - 124 km apart (within synchronous tolerance of sub 2.5 ms) • synchronously replicated → RPO0 • "3rd copy site" connected for asynchronous replication	Within async tolerance (variable – data change rate dependent) of GPS Must back up to GPS	• location is as close to the exchange as possible secured co-colocation • Within async tolerance (variable – data change rate dependent) of GPS Must back up to GPS or 3rd Copy site	two or more tier 3+ certified DCs distinct from GPS sites within async tolerance (within 50ms latency) of GPS sites	two or more tier 3+ certified DCs • minimum Logically, ideally Physically distinct from 3rd copy sites • air gapped – read and write permissions are mutually exclusive • within async tolerance (within 50ms latency) of 3rd Copy sites
Initial Configuration & Recovery	**Config:** Physical Site Only **Initial Recovery:** Physical Site Only	**Config:** Physical Site Only **Initial Recovery:** Cloud or Physical	**Config:** Physical Site Only **Initial Recovery:** Physical Site Only	**Config:** Physical Site Only **Initial Recovery:** Cloud or Physical	**Config:** Physical Site Only **Initial Recovery:** Cloud or Physical
Ephemeral Run	Cloud Permitted	Cloud Permitted	Physical Site Only	Cloud Permitted	Cloud Permitted
Backup Type	Operational Backup: Configuration DataTransaction Data	Operational Backup - Configuration Data - Transaction Data	Operational Backup: - Configuration Data - Transaction Data	All data	N/A
Backup Target	3rd Copy Site	GPS	GPS	Cyber Vault / Archive	N/A

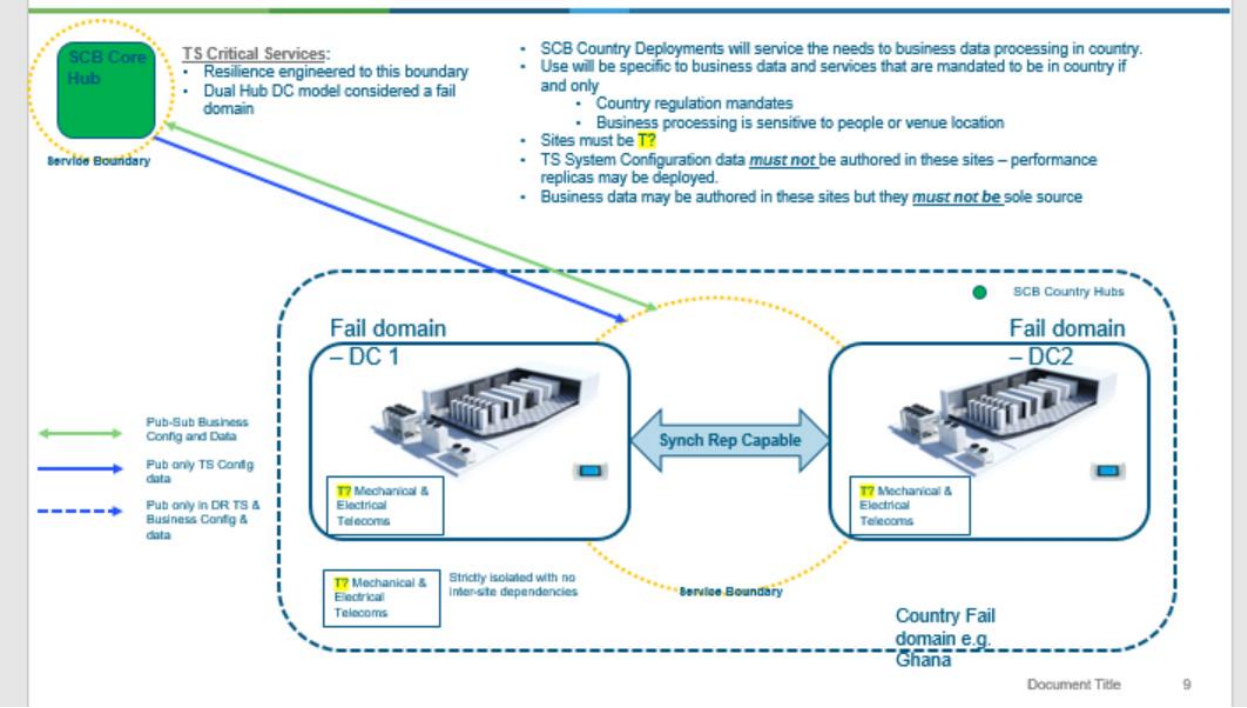
Connectivity Type	>= 10 Gbps	1 – 500 Mbps	>= 1 Gbps	>= 10 Gbps	>= 10 Gbps
Run Level Mapping	1, 2, 3, 4	>3	5,6,7	N/A	N/A

Global Processing Site (GPS)

- SCB Regional Hubs will be the backbone of the Global Processing Resilience Strategy and are the "mothership" of SCB Configuration and Business Data.
- They must be Tier 4 (system level concurrent maintenance) protected
- They will be a Synchronous Capable pair so we can run RPO0 applications and services across them
- They will be form a Globally Available Golden Source Ring of SCB Authored Data.
- Each SCB Regional Hub will provide services to a Region where the Region is considered by SCB TVRA analysis to be a fault domain.
- Foundational systems and operating systems in SCB Regional Hubs ***must not*** be 3rd Party Controlled, systems may report back to 3rd Party and isolated Services may be controlled by 3rd party.



In-Country Processing Site (CPS)



Low-Latency Site

No details provided by CCIB.

Third Copy Site Strategy - options

Option One – Regional Ready to Go

Gives a Regionally balanced 3rd Copy giving 'good' performance to markets it recovers, this option is ready to go – meaning applications will keep a copy of data and also an always on copy of their infrastructure at the third site

APAC 3rd Copy – Ready to Go
EMEA 3rd Copy – Ready to Go

Pros:

- Gives best RTO for business recovery
- Gives best recovery experience for end users (when recovered)
- Has possibility web and app to balance prod traffic over three sites for apps that can do it (this will not be many)
- Replication lag will be lower than Global so RPO will be best we can achieve for recovery

Cons:

- Data replication is hard for always on apps and multi master problem will mean most apps cannot be always on at 3rd copy.
- Data replication is complicated
- Most expensive option

Constraints:

- Could be achieved in Cloud – apps and services would need to transform to use and have permission
- Cross border data transfer
- Applications need to move to Vx
- Applications will need to practice rigid failure and recovery drills

Cost Structure

1. Most expensive Option
2. Set up costs for 2 x Sites (or use existing) OR for 2 x CSPs
3. 1/3 extra of all in scope apps current infra costs
4. Cost of application transformation
5. Extra cost of people doing failure and recovery drills

Option Two – Regional Ready to Recover

Gives a Regionally balanced 3rd Copy giving 'good' performance to markets it recovers, this option is ready to recover – meaning applications will keep a copy of data but not a copy of their infrastructure (will need to be provisioned) – with this option we could use the concept of DEV which we would re-provision.

Designations
APAC 3rd Copy – Ready to Recover
EMEA 3rd Copy – Ready to Recover

Pros:

- Gives OK RTO for business recovery
- Gives best recovery experience for end users (when recovered)
- Replication lag will be lower than Global so RPO will be best we can achieve for recovery
- Allows for the possibility of a Regional DEV site – will offset cost.

Cons:

- Data replication is complicated
- Most expensive option (but can be offset)

Constraints

- Could be achieved in Cloud – apps and services would need to transform to use and have permission
- Cross border data transfer
- Applications need to move to Vx
- Applications will need to practice rigid failure and recovery drills
- Availability of resource to recover (if you don't have always on infra then you need to find infra when you want to recover – in CSPs this is a lesser issue but there are still no guarantees – provisioning and repurposing DEV solves this)

Cost Structure

1. Second most expensive option
2. Set up costs for 2 x Sites (or use existing) OR for 2 x CSPs
3. 1/3 extra of all in scope apps infra costs (variable cost)
4. Cost of application transformation
5. Extra cost of people doing failure and recovery drills
6. Costs can be offset by using 3rd copy resources for DEV

Option Three – Global Ready to Go

Gives a Globally balanced 3rd Copy giving the ability to markets but will not be a particularly 'good' experience for any market, this option is ready to go – meaning applications will keep a copy of data and also an always on copy of their infrastructure at the third site.

Designations

Global 3rd Copy – Ready to Go – find somewhere that is equidistant between markets in scope (EMEA and APAC)

Pros:

- Gives best RTO for business recovery
- Replication is simpler
- Network costs will be less
- Probably the cheapest base cost structure

Cons:

- Creates a SPoF for Global Recovery
- Gives less optimum recovery experience for end users (when recovered)
- Replication lag will be higher than Regional option so RPO will be worse for recovery

- Likely that the "sweet spot" will be Middle East or surrounds – will be hard to find somewhere with low risk
- Middle East is very expensive for both real estate and comms (though will probably be lower in totality than regional options)

Constraints

- Could be achieved in Cloud – apps and services would need to transform to use and have permission
- Cross border data transfer
- Applications need to move to Vx
- Applications will need to practice rigid failure and recovery drills

Cost Structure

Second least expensive option – cost structure

1. Third most expensive option
2. Set up costs for 1 x Sites (or use existing) OR for 1 x CSPs
3. 1/3 extra of all in scope apps infra costs (variable cost)
4. Cost of application transformation
5. Extra cost of people doing failure and recovery drills
6. Costs can be offset by using 3rd copy resources for DEV

Option Four – Global Ready to Recover

Gives a Globally balanced 3rd Copy giving the ability to markets but will not be a particularly 'good' experience for any, this option is ready to recover – meaning applications will keep a copy of data but not a copy of their infrastructure (will need to be provisioned) – with this option we could use the concept of DEV which we would re-provision

Designations

Global 3rd Copy – Ready to Go – find somewhere that is equidistant between markets in scope (EMEA and APAC)

Pros:

- Gives OK RTO for business recovery
- Replication lag will be lower than Global so RPO will be best we can achieve for recovery
- Allows for the possibility of a Global DEV site – will offset cost.

Cons:

- Gives less optimum recovery experience for end users (when recovered)
- Creates a SPoF for Global Recovery
- Replication lag will be higher than Regional option so RPO will be worse for recovery
- Likely that the "sweet spot" will be Middle East or surrounds – will be hard to find somewhere with low risk
- Middle East is very expensive for both real estate and comms (though will probably be lower in totality than regional options)

Constraints

- Could be achieved in Cloud – apps and services would need to transform to use and have permission

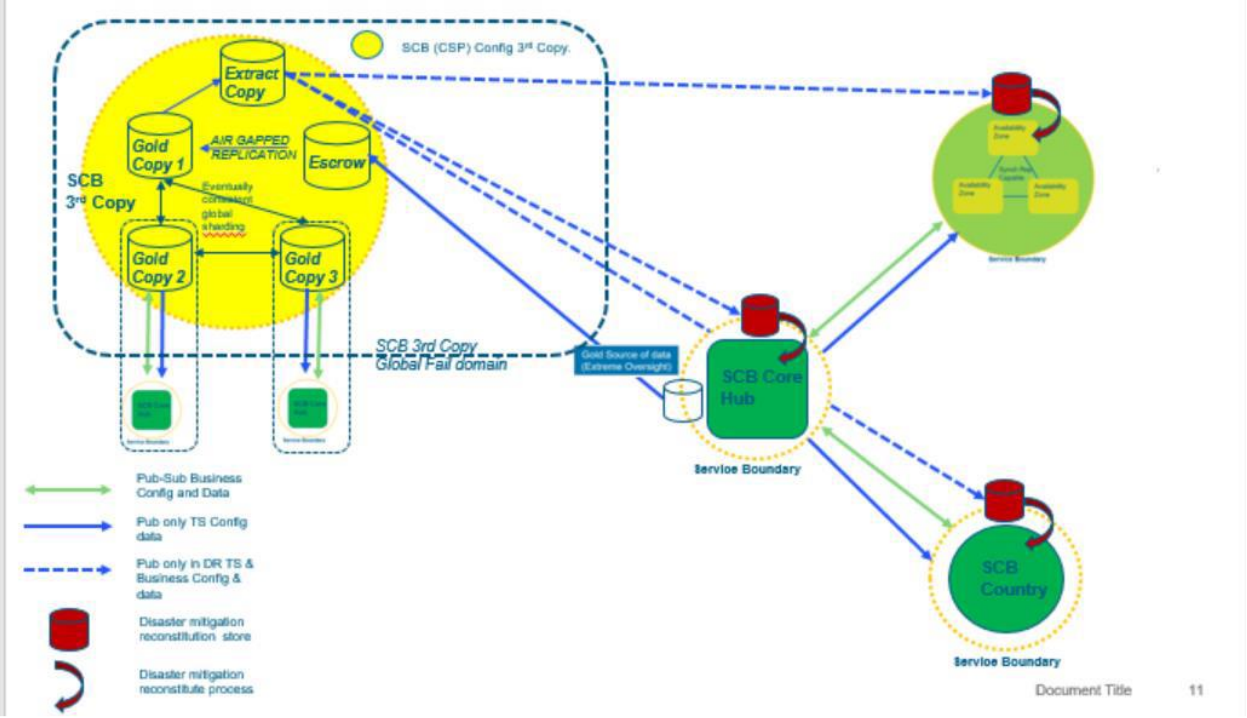
- Cross border data transfer
- Applications need to move to Vx
- Applications will need to practice rigid failure and recovery drills
- Availability of resource to recover (if you don't have always on infra then you need to find infra when you want to recover – in CSPs this is a lesser issue but there are still no guarantees – provisioning and repurposing DEV solves this)

Cost Structure

Most expensive option – cost structure

1. Least expensive option
2. Set up costs for 1 x Sites (or use existing) OR for 1 x CSPs
3. 1/3 extra of all in scope apps infra costs
4. Cost of application transformation
5. Extra cost of people doing failure and recovery drills
6. Costs can be offset by using 3rd copy resources for DEV

Regional Ready to Recover Analysis



Third Copy Location Analysis

EU

SCB would leverage CSPs to establish 3rd copy and to transit data to our CyberVault Solution

Both AWS and Azure offer regions in Western Europe and Central Europe within the 50ms latency tolerance from the EU SCB GPS. (*AWS BARCELONA announced)

	Frankfurt	Paris
Barcelona	24.827ms	23.219ms
Lisbon	44.408ms	44.084ms

ASIA

SCB GPS based in SG has far fewer options within the 50ms latency radius.
The only suitable CSP sites are AZURE South India, based in Chennai and Hong Kong Based AWS AP-EAST-1 or Azure counterpart.
As the aim here is to locate 3rd Copy sites as close to each other as possible, the Azure South India is the prevalent choice. AWS' AP-SOUTH-1 Mumbai, India–based region while falling short of the 50ms criteria, should be considered as a runner-up with 66 ms latency.

	Chennai	Hong Kong	Mumbai
Singapore	33.314ms	34.425ms	65.866ms

1. Cyber Vault

Functional Requirements

The cyber vault has several stages before data is considered safe and valid.
Definitions in the context of Cyber Vault

Definition	Description
External Source	A bank system outside the Cyber Vault
Cyber Vault	Not to be confused with Hashicorp Vault

Security

- Encryption in flight
- Encryption at Rest
- Encryption Keys managed by the bank
- A new root certificate to be used for the Cyber Vault, it should not use a certificate that have been derived from an existing root certificate, e.g. a root key that provides the public TLS certificate that for sc.com or the root cert that is used to generate the keys that are used for AWS encryption.

This is to ensure that if the existing root key / certificate has been compromised, the cyber vault will not be affected.

- This root key should be held off site in another location ideally in an HSM (Hardware Security Module)
    - One common way is to split the key / passphrase between several people who must come together to allow the key to be used and re constructed

Data Zones

This describes the logical data zones that may be required. They do not necessarily mean that we need to make multiple copies at each state. E.g. between Landing and Verification may just be a state change to say that data is verified. The data would then be copied to the Escrow Zone and removed from the Landing Zone

Zone Type	Data State	Description	Access
Landing	un-verified	Initial destination of data that is being sent to the cyber vault.	Write only from external source. No other operations allowed. Read access from the Verification Process allowed
Verification	verified	Data in this stage is either in: • Verifying • Verified • Failed STS or approved method of data / config validation	Read only access to Landing Zone required No write access
Escrow	locked	Once data is in the verified state. Daily ceremonies will be responsible to promoting the verified data in to the escrow area.	Read only access to Verification Zone. Notify Landing zone that the current data set that has been verified can be scheduled for removal

- Data Zone:
    - Highly restricted ACL, only trusted system to system access should be allowed
    - Separate Networks. There should be only one way into the Escrow Area
    - Data must remain unmolested
    - Tamper mechanism required
- Data storage for (calling each potential type out):
    - Transactional data with millisecond time accuracy
    - Unstructured data
    - binary blob data (could be considered unstructured data)
    - virtual tape libraries (maybe)

- Virtual Airgap between data areas
    - ACL's
    - Firewalls
    - User ACL's
    - If using Physical Networking using only allowing receive only on the wire
- Data promotion from the verified zone to the escrow zone is to be done via a human. In a controlled manor. Extracting access credentials from the TPAM system, sessions recorded etc….

Data Ingestion to Landing Zone

- Data ingestion is "write only" an external system can write/send data but, reading and deleting is not permitted from an external source.
- Data gets stored in the landing zone area (this is fresh data that has been sent from an external system)
- Including Data Areas requirements

Verification Processes

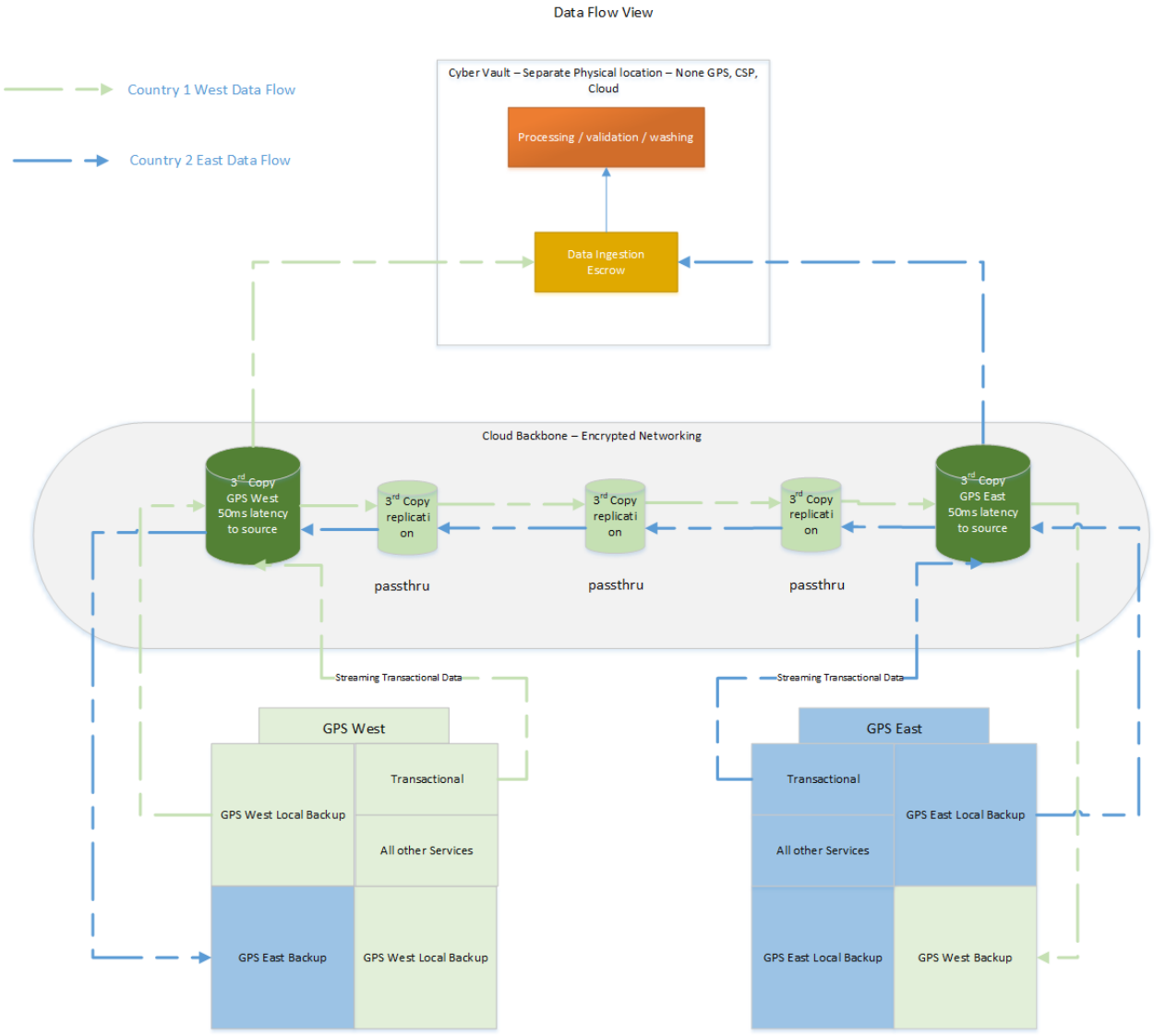
Data Type	Validation	Latency
Transactional	A counterpart to the authoring system that knows how to replay each transaction and validate that its result is what is expected	Real Time – in the sense that the vault should be able to cope with the transactional load maximum of all source transactional systems
Unstructured data	Ensure that the data uploaded is valid and what is expected. Checksum process SHA512	Depends on the Application
Binary blob data	A counter to the authoring system that knows how to read and validate the data it is as expected	Depends on the application
Virtual tape library	Software to restore the virtual tapes, then another process is required that has knowledge of the restored data as per other types in this table	Depends on the application, although this method if verification will be slower due to having to restore the data before the application level validation can take place

Extract

This refers to if we need to rebuild a system or data centre due to a disaster or systemic cyber event. The extract copy data zone would be considered a staging area for restore.

- Data would be requested out of near offline storage from the escrow zone and stored in the extract zone in a segmented manor. If two systems needed to be restored, they would have their own secure section of the extract zone
- Initially the extract zone would inherit the data zone requirements. Access would be granted to the correct zone for the system being restored, then data would be download for restore

Data Flow



Sizing

The variables informing the sizing exercise are broadly speaking the amount of data to be shifted from A to B and vice versa (initial and ongoing), the latency between those locations and the expected time for the exercise to complete.

Option 1 – all data including SRM replicated volumes

Data quantity

Repl. Type	GDCW		GDCE	
Block	ARK	25 TB	SG	105 TB
Block	WF	57 TB	SG	4 TB
File	ARK	0.5 TB	SG	10 TB
File	WF	0.5 TB	SG	1 TB
DB		32 TB		??? TB
Daily Total		115 TB		120 TB

Network requirements

It is expected that all daily data is backed up within 24 hrs.

In order to shift 120 TB within the 24-hr window 11.4 Gb/s throughput is required. To support this a minimum of 2 x 10 Gb/s dedicated circuits would be necessary [along with appropriate resilience (N+1 or N+N)].

The result is 3-4 x 10 Gb/s Direct Connect circuits provisioned between GDCW and AWS Frankfurt &
3-4 x 10 Gb/s Direct Connect circuits provisioned between GDCE and AWS Mumbai

Indicative Costs

Excluded - CAPEX

Initial data load is currently excluded as further technical details will be required.

Infrastructure investment on both GDCE and GDCW are currently not included

Costs within this section are broad estimates. The current scope is the data transfer to and from AWS as well as storage and cross-regional replication costs assuming S3 will be used primarily – subject to change

OPEX estimate

AWS 3rd copy storage and transit costs

Service Type	Components	Region	Component Price	Service Price
Amazon S3 Service (Asia Pacific (Mumbai))				$1298301.85
	S3 Standard Storage:	Asia Pacific (Mumbai)	$5949.44	
	Inter-Region Data Transfer Out:	Asia Pacific (Mumbai)	$327598.08	
	Inter-Region Acceleration Data Transfer Out	Asia Pacific (Mumbai)	$479969.28	
	Acceleration Data Transfer Out	Asia Pacific (Mumbai)	$457823.13	

	Cross Region Replication - Storage:	Asia Pacific (Mumbai)	$5826.56	
	Cross Region Replication - Inter Region Data Transfer:	Asia Pacific (Mumbai)	$21135.36	
Amazon S3 Service (Europe (Frankfurt))				$656030.63
	S3 Standard Storage:	Europe (Frankfurt)	$5585.92	
	Inter-Region Data Transfer Out:	Europe (Frankfurt)	$73011.2	
	Inter-Region Acceleration Data Transfer Out	Europe (Frankfurt)	$219033.6	
	Acceleration Data Transfer Out	Europe (Frankfurt)	$332441.51	
	Cross Region Replication - Storage:	Europe (Frankfurt)	$5703.68	
	Cross Region Replication - Inter Region Data Transfer:	Europe (Frankfurt)	$20254.72	
AWS Direct Connect Service (Asia Pacific (Mumbai))				$372317.44
	Ports:	Asia Pacific (Mumbai)	$7261.44	
	Data Transfer In:	Asia Pacific (Mumbai)	$0	
	Data Transfer Out:	Asia Pacific (Mumbai)	$365056	
AWS Direct Connect Service (Europe (Frankfurt))				$83447.04
	Ports:	Europe (Frankfurt)	$7261.44	
	Data Transfer In:	Europe (Frankfurt)	$0	
	Data Transfer Out:	Europe (Frankfurt)	$76185.6	

AWS Data Transfer Out				$491871.04
	Asia Pacific (Mumbai) Region:	Global	$305451.93	
	Europe (Frankfurt) Region:	Global	$186419.11	
AWS Support (Business)				$93959.04
	Support for all AWS services:		$93959.04	
		Total Monthly Payment:		**$2,995,927**

Option 2 – all data excluding SRM replicated volumes

This option focuses on application data, DB backups and transactions and does not concern SRM volumes for point and click system failover.

Data quantity

Repl. Type	GDCW		GDCE	
File	ARK	0.5 TB	SG	10 TB
File	WF	0.5 TB	SG	1 TB
DB	Combined	16 TB		16 TB
Transactions	Combined	16 TB		16 TB
Daily Total		33 TB		43 TB

Network requirements

It is expected that all daily data is backed up within 24 hrs.
In order to shift 43 TB within the 24-hr window 10 Gb/s throughput is required. To support this a minimum of 2 x 10 Gb/s dedicated circuits would be necessary [along with appropriate resilience (N+1 or N+N)].
The result is 2 x 10 Gb/s Direct Connect circuits provisioned between GDCW and AWS Frankfurt &
4 x 10 Gb/s Direct Connect circuits provisioned between GDCE and AWS Mumbai

Indicative Costs

Excluded - CAPEX
Initial data load is currently excluded as further technical details will be required.
Infrastructure investment on both GDCE and GDCW are currently not included

Costs within this section are broad estimates. The current scope is the data transfer to and from AWS as well as storage and cross-regional replication costs assuming S3 will be used primarily – subject to change

OPEX Estimate

AWS 3rd copy storage and transit costs

Service Type	Components	Region	Component Price	Service Price
Amazon S3 Service (Asia Pacific (Mumbai))				$459933.62
	S3 Standard Storage:	Asia Pacific (Mumbai)	$2164.74	
	Inter-Region Data Transfer Out:	Asia Pacific (Mumbai)	$117389.32	
	Inter-Region Acceleration Data Transfer Out	Asia Pacific (Mumbai)	$171989	
	Acceleration Data Transfer Out	Asia Pacific (Mumbai)	$164508.57	
	Cross Region Replication - Storage:	Asia Pacific (Mumbai)	$2120.71	
	Cross Region Replication - Inter Region Data Transfer:	Asia Pacific (Mumbai)	$1761.28	
Amazon S3 Service (Europe (Frankfurt))				$186639.28
	S3 Standard Storage:	Europe (Frankfurt)	$1639.43	
	Inter-Region Data Transfer Out:	Europe (Frankfurt)	$20951.04	
	Inter-Region Acceleration Data Transfer Out	Europe (Frankfurt)	$62853.12	
	Acceleration Data Transfer Out	Europe (Frankfurt)	$98170.79	
	Cross Region Replication - Storage:	Europe (Frankfurt)	$1673.22	
	Cross Region Replication - Inter Region Data Transfer:	Europe (Frankfurt)	$1351.68	
AWS Direct Connect Service (Asia Pacific (Mumbai))				$112016.64
	Ports:	Asia Pacific (Mumbai)	$7261.44	
	Data Transfer In:	Asia Pacific (Mumbai)	$0	
	Data Transfer Out:	Asia Pacific (Mumbai)	$104755.2	
AWS Direct Connect Service (Europe (Frankfurt))				$34561.28

	Ports:	Europe (Frankfurt)	$7261.44	
	Data Transfer In:	Europe (Frankfurt)	$0	
	Data Transfer Out:	Europe (Frankfurt)	$27299.84	
AWS Data Transfer Out				$166177.6
	Asia Pacific (Mumbai) Region:	Global	$109908.89	
	Europe (Frankfurt) Region:	Global	$56268.71	
AWS Support (Business)				$35679.86
	Support for all AWS services:		$35679.86	
		Total Monthly Payment:		**$995,008.28**

Escrow and Gold Data Scanning Service - tool and process does not exist – circa $100 000 / month

OPEX total / month – circa $1.1M

As we expect to include BC4/5 applications only; 435 of 1416 total applications, assuming there is a linear relationship, 31% of the Total Monthly AWS costs (above) are applicable as well as the Escrow and Gold Data Scanning Service cost, bringing to total monthly OPEX to circa $ 400 000

CAPEX Estimate

- On Prem storage requirements:

14 days' worth of daily transfer total
14 days* 76000 GB * $0.1/ GB = $638,400

- Escrow and Gold Data Scanning Service - tool and process does not exist – circa $1M to set up (estimate)

CAPEX total – circa $2M

SCB Data Processing Site Map

GPS: Two global processing sites can cover SCB's requirements summarised within the "site types specification" section (above). GPS WEST will be EU (south) based – either in Lisbon or In Barcelona. GPS EAST should either be located in Hong Kong or Singapore.

In-Country Site: It is expected that we will have one or more In-Country sites within each strategic market (currently showing) as well as within countries that cannot be serviced remotely due to regulatory requirements (e.g. data sovereignty)

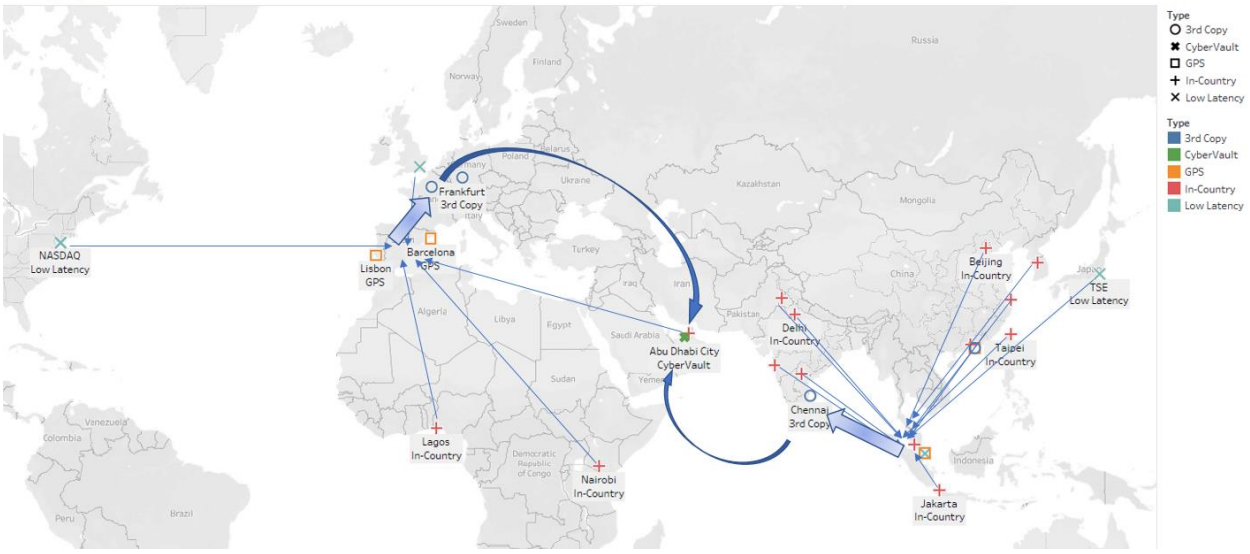
Low Latency site: one per exchange, located as close as possible to the exchange

3rd Copy site: CSP hosted availability zone within 50ms tolerance of GPS

Cyber Vault: will be a consolidated regional replica of 3rd copy sites

Global Topology

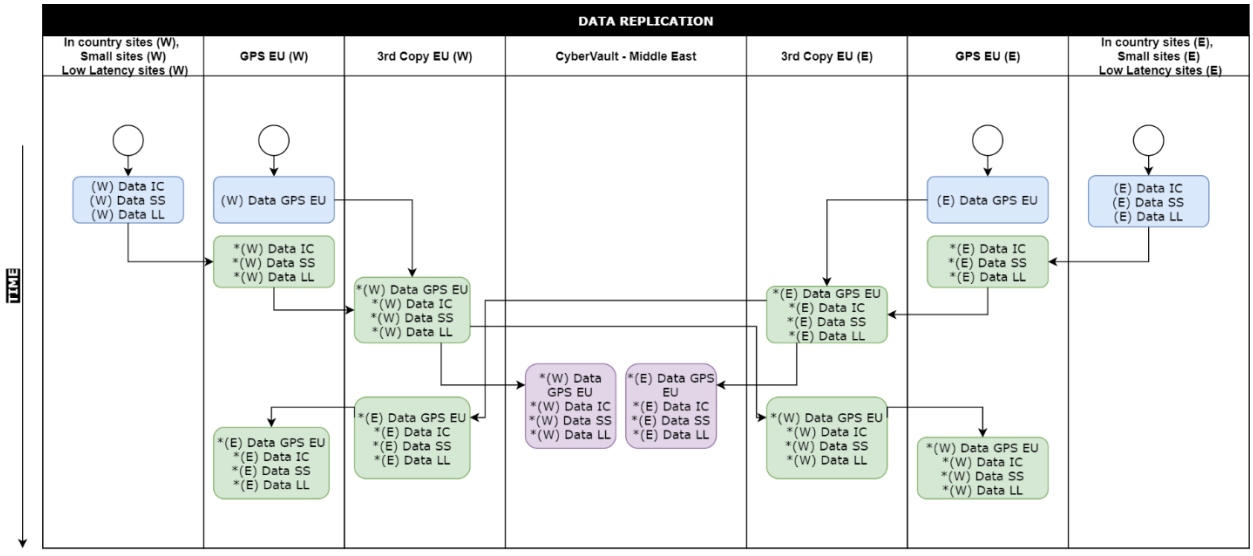
SCB Site MAP



As per "site types specification":

- in-country sites, small sites and low latency sites must back up to GPSs
- GPSs must back up to 3rd copy sites
- 3rd Copy sites must replicate data to CyberVault
- 3rd Copy sites must replicate data to distant GPS also

Data Replication overview



Location Intelligence

This section should concentrate on ratings – defined by experts in this field

Geo Considerations

Risk of natural disasters

- Seismic activity rating
- Flood / Tsunami
- Tornado / Hurricane

Physical Risk assessments: The bank has partnered with Munich Re, (one of the world's largest reinsurers) and uses their NATHAN Hazards Edition risk assessment tool to perform a granular physical risk assessment. Each assessment is at the specific location of individual properties (i.e., latitude and longitude of the site location) – so representing unprecedented granularity in our risk assessment capabilities.
The physical risk identification considers the risk and hazard for chronic and acute climate events by location at present day, and in the future (2050, 2100) under different Representative Concentration Pathways (RCP) scenarios. The results are informed by a complex network of underlying natural catastrophe and climate models.

Mandatory Requirement: All new properties (ATMs, Branches etc) ongoing from 1st April 2022 and new data processing locations globally (from 1st April 2023) will require relevant teams to reach out to the climate risk team (Email: ClimateRiskTeam@sc.com) for a granular physical risk assessment of the location to factor the impacts of climate risk. This will help us understand how exposed our locations are to physical risk (e.g., floods, storm, severe weather events) and allow us to implement appropriate mitigation measures.

The physical risk report from Munich Re is to be attached to the assessment being undertaken. The reports provide one Overall Risk Score as well as individual Risk Scores for flood, storm, earthquake, and wildfire risks.
• Flood risk - Includes River Flood, Flash Flood and Storm Surge Risk.
• Storm risk - Includes the Tropical cyclone, Extratropical storm, Hail, Tornado and Lightning Risk.
• Earthquake Includes the Earthquake, Volcano and Tsunami Risk.

Caution about the metrics: The metrics are based on outputs from Munich Re's natural catastrophe model and do not assume adaptation measures such as building quality, hazard protection infrastructure (such as flood defences) or government adaptation policies.

Political Stability

- Rating / recent events

Business Environment

- Face value costs
- Tax breaks / investment incentives

- Regulatory climate

Infrastructure

- Road network (motorway?)
- Proximity to major airports
- Proximity to Exchange

APPENDICES

Ping Tests

Asia – Asia

	Bangalore	Chennai	Hanoi	Hong Kong	Hyderabad	Jakarta	Lahore	Malaysia	Mumbai	Seoul	Shanghai	Singapore	Taipei
Hanoi	101.977ms	88.152ms	—	36.35ms	96.282ms	80.21ms	282.236ms	79.154ms	125.818ms	241.982ms	214.144ms	70.958ms	56.936ms
Hong Kong	74.524ms	67.256ms	36.381ms	—	84.506ms	48.664ms	235.011ms	46.463ms	233.654ms	76.019ms	99.792ms	33.871ms	27.084ms
Singapore	39.898ms	33.203ms	71.461ms	34.188ms	50.474ms	12.591ms	277.832ms	43.964ms	53.273ms	105.56ms	220.925ms	—	83.808ms

Asia -China

	Hangzhou	Shanghai	Shenzhen	Zhangjiakou
Hanoi	222.959ms	214.144ms	242.115ms	217.742ms
Hong Kong	155.869ms	99.792ms	171.774ms	174.054ms
Singapore	301.077ms	220.925ms	322.915ms	315.33ms

Asia-India

	Bangalore	Chennai	Hyderabad	Indore	Mumbai	New Delhi	Pune
Hanoi	101.977ms	88.152ms	96.282ms	142.676ms	125.818ms	131.844ms	123.358ms
Hong Kong	74.524ms	67.256ms	84.506ms	97.129ms	233.654ms	115.251ms	96.248ms
Singapore	39.898ms	33.203ms	50.474ms	64.788ms	53.273ms	79.475ms	66.216ms

MEA-ASIA

	Hanoi	Hong Kong	Singapore
Cairo	323.449ms	264.663ms	210.866ms
Dubai	149.769ms	115.264ms	266.615ms
Riyadh	192.248ms	276.597ms	258.376ms
Tel Aviv	353.974ms	245.601ms	213.732ms

MEA-India

	Bangalore	Chennai	Hyderabad	Indore	Mumbai	New Delhi
Cairo	251.112ms	212.973ms	247.454ms	177.907ms	220.922ms	247.255ms
Dubai	122.886ms	158.947ms	124.355ms	38.059ms	284.829ms	180.958ms
Riyadh	154.166ms	223.549ms	141.344ms	134.832ms	204.801ms	216.376ms
Tel Aviv	198.912ms	261.716ms	199.488ms	248.778ms	184.252ms	203.503ms

MEA-Africa

	Lagos	Nairobi
Cairo	187.897ms	261.344ms
Dubai	223.961ms	122.039ms
Riyadh	253.633ms	157.516ms
Tel Aviv	157.46ms	250.37ms

EU-Africa

	Lagos	Nairobi
Barcelona	84.485ms	187.288ms
Lisbon	69.386ms	179.211ms
Madrid	91.88ms	181.051ms

EU-ME

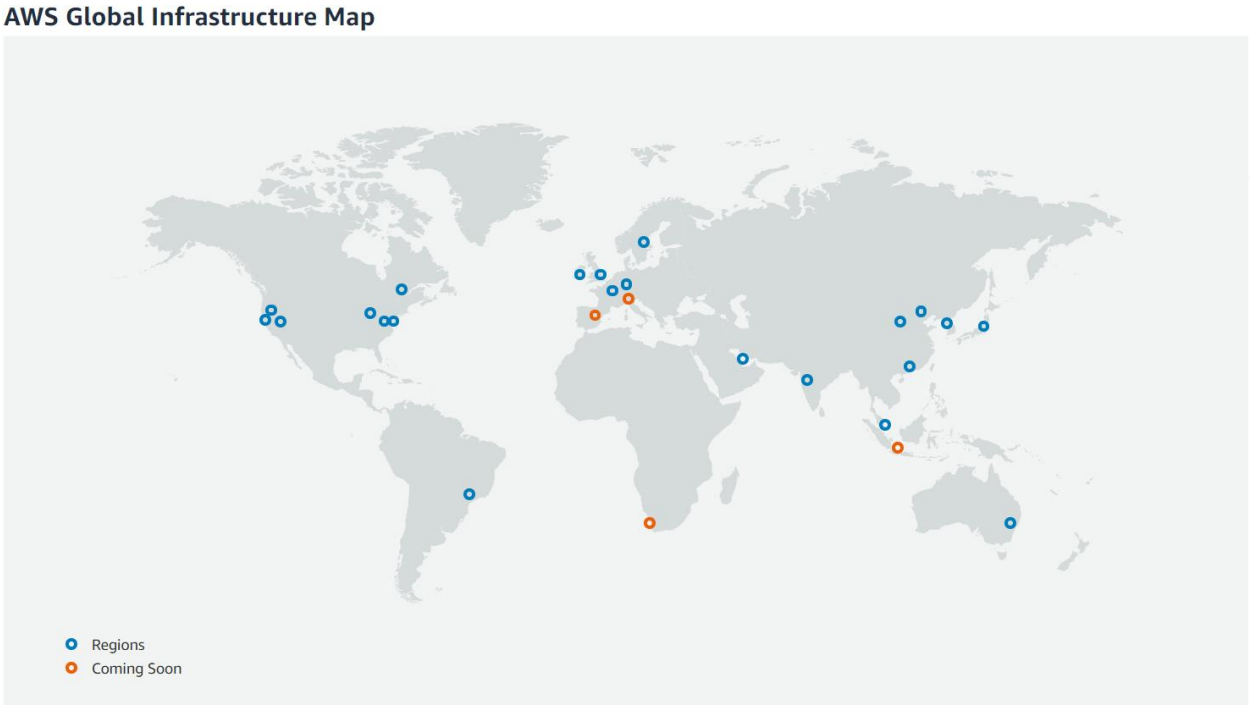
	Dubai	Riyadh
Barcelona	132.979ms	109.981ms
Lisbon	135.942ms	130.281ms
Madrid	181.233ms	116.14ms

EU-India

	Bangalore	Chennai	Hyderabad	Indore	Mumbai	New Delhi
Barcelona	187.305ms	161.612ms	168.066ms	155.831ms	144.395ms	144.045ms
Lisbon	186.993ms	188.411ms	169.894ms	152.393ms	168.281ms	163.007ms
Madrid	151.792ms	156.827ms	143.07ms	129.396ms	135.403ms	132.462ms

Azure Global Infrastructure

AWS Global Infrastructure



Data Onshoring – Requirements

Data localisation – systems onshoring (1)

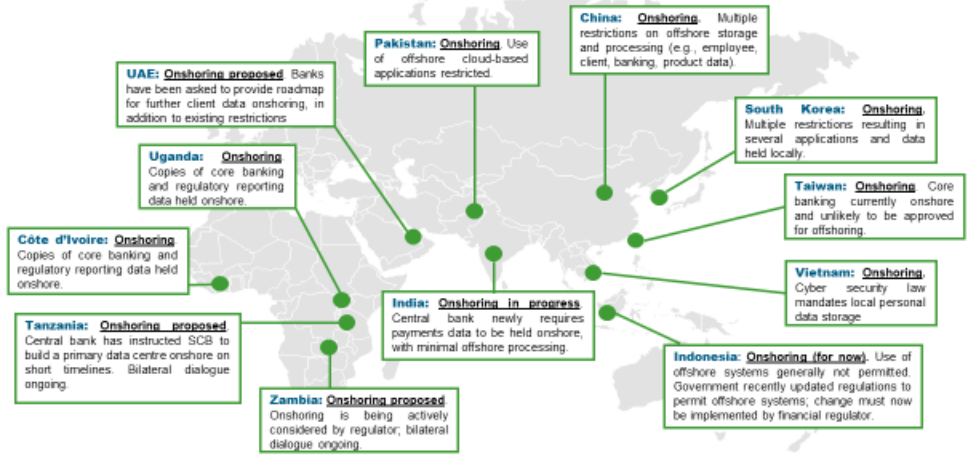
Where have regulatory requirements resulted in systems being pulled onshore?

Standard Chartered

Overview: *Several markets have notification and approval requirements for cross-border data transfers and offshore data processing and storage. These requirements may sit in data protection and privacy frameworks, or outsourcing, use of cloud, and general data management rules.*

Where these approvals for cross-border transfers are denied, or regulations impose data onshoring requirements without such exceptions, the result is onshoring of data storage and/or processing systems. Supervisors may also directly impose onshoring requirements, e.g., making their expectations clear after on-site inspections.

The type of impacted data and system varies across markets.



Data localisation – systems onshoring (2)

Additional details on the regulatory requirements driving onshoring in these 12 markets

Standard Chartered

Market	Additional details on onshoring
China	• CBIRC notice from 2009 requires core/critical systems for client, accounting, and product information onshore • In 2011 PBOC further mandated onshoring of personal financial information • Established onshoring requirements continue to be refined and potentially expanded under new rules for cyber and cloud
Côte d'Ivoire	• Banks are expected to maintain a data centre onshore • Onshored tertiary copies of core banking and regulatory reporting data warehouse implemented in Nov 2019, to enable operational continuity albeit on a very restricted basis
India	• RBI notice requires onshore payments data storage; foreign legs of transactions may be processed offshore and FCC systems not expected to be in scope • Banks expected to use panel auditing firms to confirm approach • Separate personal data protection legislation pending; may expand onshoring requirement to other sectors and systems
Indonesia	• Data onshoring law introduced 2012 with effect from 2017 • Recent positive movement, as new 'Government Regulation 71' allows 'private system owners' to place systems offshore • Financial regulator (OJK) now needs to implement – TBD
Pakistan	• Use of offshore cloud is technically permitted subject to approvals, but regulators have generally not approved our use of offshore cloud service providers
South Korea	• Prohibition on offshore systems that contain 'identifiable' customer information • Further, related prohibitions on use of offshore cloud for personal customer credit information

Market	Additional details on onshoring
Taiwan	• Offshore systems permitted but regulatory approval is required on an application basis – time and resource intensive process that can require external due diligence (USD 150k) • Core banking must still be hosted in country; global dialler system recently approved for offshore after 8 months
Tanzania	• Central bank circular of 23 Aug 2019 gave financial institutions 3 months to establish a primary data centre in Tanzania; 250k USD monthly fine where not in place • Previous agreement was that SCB hosts secondary data and certain key systems onshore to ensure operational continuity • Bilateral discussions on requirements and timing ongoing
Vietnam	• Recent cybersecurity law requires personal data and data created by users of digital services to be stored in Vietnam, although scope not entirely clear; driven by surveillance/security concerns
Uganda	• All supervised institutions required to establish in-country primary data centres and disaster recovery site • Tertiary copies of core banking and regulatory reporting data warehouse now replicated to Uganda on-line to enable operational continuity, albeit on a very restricted basis
UAE	• In the local market (not DIFC), personal data legislation allows consent-based transfers, but digital payments rules prohibit offshore storage or outsourcing for payment systems users' data • Regulator has asked banks to prepare roadmap for further UAE client personal data onshoring – dialogue is ongoing
Zambia	• No formal regulatory requirements at present but regulators have recently suggested systems onshoring may be needed • SCB scheduling a visit to the UK Global Data Centres for Zambian authorities, to demonstrate advantages