MINISTRY OF HEALTH
SINGAPORE

MOH Health Innovation (MHI) Fund
- Guide to Fill Out Key Information in MHI Application

Apr 2022

Project Overview

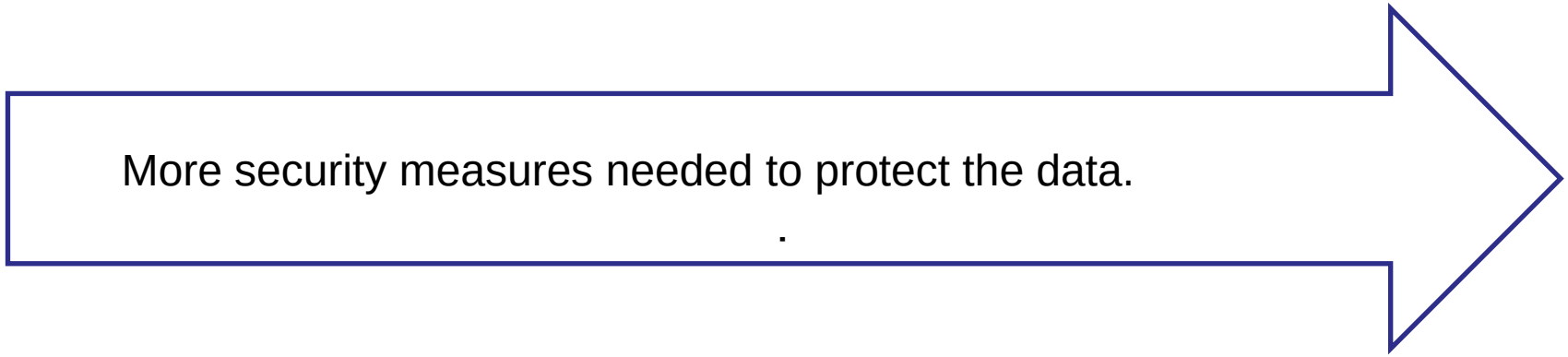
. PROJECT OVERVIEW

Project Name	<Limit to 20 Characters>				
Project Type	<New /Enhancement>				
System Criticality	Non Govt-owned systems: <Mission Critical / Business Critical / Standard> Govt-owned systems: <CII / SII / Non CII or SII>				
Data Classification	<Unclassified-Non Sensitive | Restricted-Non Sensitive| Restricted-Sensitive Normal | Restricted-Sensitive High >				
Ownership	**Business Owner** <ministry/agency/ cluster/ institution>/ <dept> / <role>	**System Owner** <ministry/agency/ cluster/ institution>/ <dept> / <role>	**System Operator** <ministry/agency/ cluster/ institution>/ <dept> / <role>	**Data Owner** <ministry/agency/ cluster/ institution>/ <dept> / <role>	**Data Manager** <ministry/agency/ cluster/ institution>/ <dept> / <role>
Project Delivery Team					
Project Cost for Endorsement	**Total (S$)**	**CAPEX (S$)**	**One-Time OPEX (S$)**	**Contingency (S$)** (if applicable)	
Project Schedule	**Timeline** From MM/YYYY> to <MM/YYYY>		**Duration** *<Project must be completed within 18 months from the day the letter of award is issued by MOH>*		

Pls choose one

Pls choose one

Data Classification- Determining the Information Security Classification (RCST)*



Information Security (RCST) Framework			
Unclassified	**Restricted**	**Confidential**	**Secret**
Will **not** result in damage/ negative impact to PHI/Agency's interest/function, national interest/ security if leaked	Results in damage/ negative impact to PHI/Agency's interest/function, national interest/ security, if leaked		

*Refer to HIM- Data Management for further details

Data Classification- Determining the information sensitivity of data*

More user access restrictions , access approvals to safe guard info

ISF	Data Categories	
	Individual	Business Entity
Non-Sensitive	Does not cause physical, financial, or emotional injury to the individual if data is leaked; OR is personal information that is socially expected to be openly available. • **Public Data** • **Anonymised Data**	Does not impact a business' processes or operations if data is leaked; OR is business information that is socially accepted as openly available. • **Employment & business activity data** e.g. course enrolment, business contact info • **Transactional data** e.g. address, bank account details, mobile numbers
Sensitive-Normal	Causes temporary and minor emotional distress or disturbance to the individual if data is leaked. • **Clinical Information** e.g. General Medical Information • **Personal Identifiable Information (PII)** e.g. birth dates, NRIC • **Genomic information** excluding Whole Genomic Sequence (WGS) & Whole Exome Sequence (WES) • **Health/Social Information (**Socially acceptable to be shared) eg behavioral, relationships	Causes a reduction in competitiveness or a compromise of business interests if data is leaked. E.g.: Loss of potential business opportunities, some damage to reputation
Sensitive-High	Causes serious physical, financial, or sustained emotional injury or social stigma to the individual if data is leaked. **Sensitive Clinical Information** e.g. VVIP medical records **Sensitive Genomic information** e.g. WGS, WES **Sensitive Health/Social Information** e.g. sexual preferences	Causes sustained financial loss if data is leaked. E.g.: Inability to conduct normal business operations, significant and irreversible loss of competitive advantage, major damage to reputation.

*Refer to HIM- Data Management for further details

Data Classification- Putting it all together

ISF*	Information Security (RCST) Framework*			
	Unclassified	**Restricted**	**Confidential**	**Secret**
	Will **not** result in damage/ negative impact to PHI/Agency's interest/function, national interest/ security if leaked	Results in damage/ negative impact to PHI/Agency's interest/function, national interest/ security, if leaked		
Non-Sensitive	**Public Data** **Anonymised Data** **Employment & business activity data** **Transactional data**		Not Applicable for PHIs and Agency	
Sensitive-Normal		**Clinical Information** **Personal Identifiable Information (PII)** **Genomic information** **Health/Social Information**		
Sensitive-High		**Sensitive Clinical Information** **Sensitive Genomic information** **Sensitive Health/Social Information**		

*Refer to HIM- Data Management for further details

Project Overview – Recap

Indicate if project is New POC/ Enhancement to existing system

Indicate the Business Owner, System Owner, System Operator, Data Owner, Data Manager (Ref - ownership responsibilities in HIM- Leadership and Accountability policy

Review your submission with the Business/system Owner, System Operator, reviewing architect and include their name in the deck

Project Background- Good sample (Tech Refresh)

Project Background

- Vesalius is a legacy bespoke system used in NSC and DSC. Vesalius is a all-in-one system which has :-
- - Clinical documentation.
- - Test order & Results
- - Lab management
- - Pharmacy management (outpatient prescribing & dispensing)
- - Patient management & accounting
- - Procurement, Inventory Management
- Vesalius is planned to be replaced by NGEMR, BT, NHIPS (estimated from Oct 2023, subject to confirmation)

A. Background

As-Is State

- Vesalius in Cold Fusion version 2016
- Extended support for Vesalius Cold Fusion 2016 is 17 Feb 2022

To-Be State

- Vesalius Tech Refresh with Cold Fusion version 2021

B. Scope

According to NAO, Cold Fusion version 2021 is not the supported Application Framework and Programming Language

Project team was advised by NAO to seek SRB endorsement to continue use of Cold Fusion.

Project Background

Current Problem:

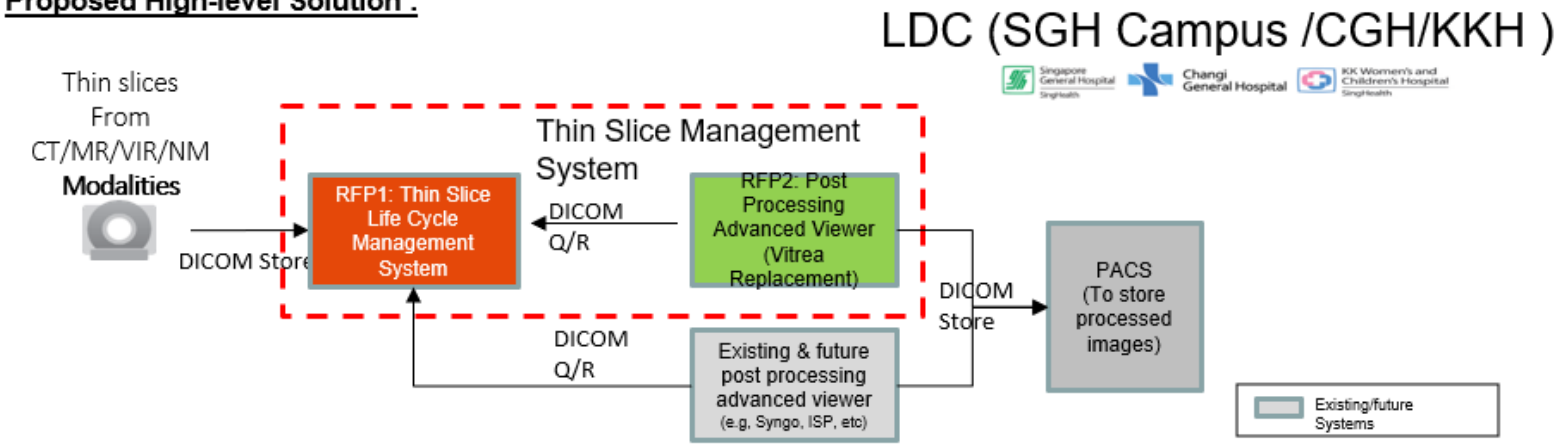
1. Thin slice images are not stored in a centralized system for SingHealth Institutions.
2. The existing Vitrea Post processing viewer system (used by SGH campus, KKH and CGH) couldn't meet security requirement and servers are EOL. It is due for replacement.

Project Scope:

There are two open RFPs called and currently at pre-award stage. The project scope is to implement 2 systems for SGH campus, CGH and KKH as separate instance:

1. RFP1: Thin Slice Lifecycle Management system. It is to integrate with multiple post processing advanced viewers.
2. RFP2: Post Processing Advanced Viewer system. It is for processing of thin slice images (CT/MR/VIR/NM)

Proposed High-level Solution :



* The solution will include an option to be extended to SKH in future who opt not to proceed now.

Objective

To seek approval from SRB for the solutions provided by the 2 selected vendors by RFP evaluation committee:

1. RFP1 Thin Slice Lifecycle Management system: to award to Philips Electronics Singapore Pte Ltd.
2. RFP2 Post Processing Advanced Viewer system: to award to Canon Medical Systems Asia Pte Ltd.

Project Background- Good sample (New System)

Project Background

A. Background

As-Is State

- SSMC is operated in the following 3 sites (current systems).

Site	Application	Hosting	Remarks
SSMC CGH	SCM, OAS, Ancillary (RISPACS, PHIS)	HDC	
SSMC Novena	CA	On-Site	Standalone system, target to use SCM.
SSMC SSI	MRS	GDC	Site operated for SSI 5 + 5 years, catered only for national athletes, not CGH patient

- SSMC took over SSI sports clinic in 2019. The clinic is currently using a Medical Record System (MRS) application (managed by GovTech, in SportSG DC) similar to a clinic EMR standalone system with no external interfaces. As the MRS application is due for technology refresh in terms of hardware and software, both CGH and SSI management is looking to replace it with other solution.
- Team have assessed other options like SCM, Plato, GPConnect and CA, user have decided that CA can fit the bill.
- Total active patient volume is approximately 5k for SSI, expect a 15%-25% growth annually.

To-Be State:

- CA instance to be hosted in Healthcare Commercial Cloud (HCC) Azure as MVP.

B. Scope

- Implement a new CA instance in Azure.
- Migration data from existing system.

Project Background- Good sample (New Facilities)

The Eastern General Hospital Healthcare Living Laboratory (EGH-HLL) is a 3-storey temporary facility with setup of MOHH Site Office, Mock-Up Centre, Office Areas to facilitate planning, simulation and building for the future EGH/CH (Eastern General Hospital/Community Hospital). See slide 6 for the locations of EGH/CH and EGH-HLL.

Building construction has commenced in Apr 2021 and target to complete by Feb 2022. It will be in use for an estimated duration of 8 years throughout the planning, design and construction of EGH/CH. EGH-HLL is located at Lot 05230N MK28 @ Bedok North Road.

There will be no patients onsite EGH-HLL.

Floor Layout of HLL: (See slide 7, 8 & 9)

- EDU (Engineering Design Unit) shall occupy Level 1
- MOHH site office shall occupy Level 2
- EGH users shall occupy offices in Level 2 and 3
- Mockup sites shall occupy Level 1, 2 and 3

Corporate network to be managed by IHIS is requested for the 3 floors in HLL

EGH-HLL network design is similar to Eunos Polyclinic (2 tiers network design; SRB Sitting 2 Oct 2018)

Project Background- Good sample (New Facilities)

IT Scope of work:

- Tapping of existing SGH Clustered Shared Services (Print Servers, DHCP, AntiVirus, BigFix and Jump Host server)
- Procurement, delivery, setup and deployment of all IT Network hardware/devices for EGH HLL Corporate Network
- Procurement, delivery, setup and deployment of NAS Storage (EMC isilon) at SGH LDC for file sharing
- Procurement, delivery, setup and deployment of EUC hardware/software
- No System application requested
- There are 2 LAN Rooms in HLL located at level 1 & 2
- IHIS IT Network equipment will be in Level 1 and Level 2 LAN rooms in separate racks with separate lock. All HLL facilities services and security systems (e.g. CCTV) will be connected to MOHH network and managed by MOHH
- For this SRB, we are focusing on IHIS aspect

Project Background- Good sample (solution updates to SRB)

<Updated>

Project Background

- A BME RFP was called to replace 180 units of Vital Signs Machines (VSM) that was due for replacement (EOL, 2014 Q4) in TTSH.
- Mindray VS-900 was selected as the replacement model.
- The award is bundled with an eGateway implementation to enable the MDI integration with Capsule SmartLink servers upon TTSH NGEMR goes-live.
- Solution has been endorsed by SRB in 24 Nov 2020

New

- The eGateway solution during implementation, after review with the vendor, does not comply with HIM-ISP w.r.t. Multi-Tier architecture, Application and Database are on same tier.
- Mindray will make changes to the existing eGateway database, removing any persistent data storage and also will instead poll the ADT data from SAP through ESB, instead of receive a push of all patient ADT.
- The Mindray database will be set to clear patient data locally every 1 hour (up to a maximum of 72 hours), and poll ADT data again, only for Patient ID's enrolled at the VSM.

Project Background- Recap

Do

- Present background in clear concise manner
- Indicate clearly the problem, solution and what approval is being requested from SRB/PPSC
- Leverage existing system within cluster or across other cluster where applicable/feasible to reduce system fragmentation
- For new platforms: Include evaluation and rationale why tool/ product was chosen as well as deployment schedule

Don’t

- Write lengthy story
- Just copy content from another deck / source presented for a different purpose without applying the context of the submission
- Propose solution/product/system without going through proper procurement practices
- Assume what has been implemented in the past will justify support for new project

Solution Components

S/N	System / Application / Hardware [1]	Name & Purpose	Buy / Build / Extend[2]	Hosting Location[3]	Standard / Non-Std [4]
1					
2					
3					

Buy – New Components or subscribing to new service
Build – Developing capability
Extend – Reusing or making changes on top of an existing component

HCC- H-Commercial Cloud (Virtualised resources)
HPC- H-Private Cloud (Virtualised resources)
HDC- H-Data Center (Co-location)
LDC- Local Data Center
CC – Commercial Cloud

Standard
Refer to IHiS SRB Intranet Technology Roadmap
Non-Standard
To be supported by Vendor/ App team

Note:
1. Categorize each component type with one of the following "System", or "Application", or "Hardware"
2. Indicate "Buy" for purchasing new components or subscribing to commercial cloud service or "Build" for developing a capability or "Extend" when making changes ontop of an existing component.
3. Specify hosting location as "HCC" (H-Commercial Cloud), "HPC" (H-Private Cloud), "HDC" (H-Data Center Co-location) or "LDC" (Local Data Centre) or "CC" (Commercial Cloud) or "GCC" (Govt Commercial Cloud) or "GDC Segregated" or "GDC Hosted" (Govt Data Center) or specify any other actual hosting site.
4. Indicate "Standard" if the component is under IHiS Technology Roadmap, otherwise indicate as "Non-Std".

Solution Components- Sample

S	/ Hardware [1]	& Purpose	Buy / Build / Extend[2]	Hosting Location[3]	Standard / Non-Std [4]
1	Application	FORUM Archive v4.2 is an Opthalmology PACS COTS from Carl Zeiss which embeds following core technology. • Glassfish 3.1.2.20 3.1.2.20 • Java 8 • Microsoft Win 2019	Buy	HDC	Non-Std
2	Hardware	Server to host FORUM Archive v4.2 1VM, 4 CPU, RAM 16GB C:100GB, D:80GB	Build	HDC	Standard
3	Application	Clinician Dashboard for • User login • Patient Enrollment **Technology:** ReactJS 16.8.6, Windows 2019	Extend	HCC	Non-Std
4	Application	NBSM system – Blood inventory tracking, distribution and cold chain management for blood products in HSA and BBLs n Microsoft Win 2019, .NET CORE 3.1	Build	GDC Segregated	Standard

The purpose of the components is clearly stated.

Corresponding hardware entries are included

Details of subcomponents are clearly stated.

The hosting locations are stated

At least 1 subcomponent is unsupported

Note:
1. Categorize each component type with one of the following "System", or "Application", or "Hardware"
2. Indicate "Buy" for purchasing new components or subscribing to commercial cloud service or "Build" for developing a capability or "Extend" when making changes ontop of an existing component.
3. Specify hosting location as "HCC" (H-Commercial Cloud), "HPC" (H-Private Cloud), "HDC" (H-Data Center Co-location) or "LDC" (Local Data Centre) or "CC" (Commercial Cloud) or "GCC" (Govt Commercial Cloud) or "GDC Segregated" or "GDC Hosted" (Govt Data Center) or specify any other actual hosting site.
4. Indicate "Standard" if the component is under IHiS Technology Roadmap, otherwise indicate as "Non-Std".

Solution Components- Sample (Updated Solution Components)

Updated

S/N	System / Application / Hardware [1]	Name & Purpose	Buy / Build / Extend[2]	Hosting Location[3]	Standard / Non-Std [4]
1	Application	EvaSign Web CMS server OS: Windows Server 2019 Standard Web Server: IIS 10.0	Buy	Microsoft Azure	Non-Std
2	Application	EvaSign App & Admin Server OS: Windows Server 2019 Standard App Server: IIS 10.0	Buy	Microsoft Azure	Non-Std
3	Application	EvaSign Database OS: Windows Server 2019 Standard DB: SQL Server 2019	Buy	Microsoft Azure	Non-Std
4	Hardware	Media Players (estimated: 104) OS: Win 10 64-bit	Buy	Institution Premises	Standard
5	Hardware	Internet Dongle (estimated: 104)	Buy	Institution Premises	Non-Std

Applicable for:
1) Submissions that are retabling their solution after a previous SRB review session
2) Previous SRB endorsed solutions that have changes in design (i.e. updating SRB on changes)
3) Leveraging from a previous SRB endorsed solution for your project implementation

Note
1. C
2. In
w
3. Sp
D
sp
4. Indicate "Standard" if the component is under IHiS Technology Roadmap, otherwise indicate as "Non-Std".

d"
or

Solution Components- Sample (Extension of Facility)

S/N	System / Application / Hardware [1]	Name & Purpose	Buy / Build / Extend[2]	Hosting Location[3]	Standard / Non-Std [4]
1	Hardware	802.11ax Wireless Access Point Provision of wireless network	Buy	NA	Standard
2	Hardware	Distribution & Access Network Switches Provision of wired network	Buy	NA	Standard
3	Hardware	Wireless Access Controller (WLC) Manage WAPs	Extend	NA	Standard
4	Hardware	MPLS Firewall Maintain segregation of VRFs	Extend	LDC	Standard
5	Hardware	NTP Server Provide time sync to network equipment	Extend	LDC	Standard
6	Hardware	NAC Server Authenticates users & devices accessing network	Extend	LDC	Standard
7	Hardware	TACACS (ISE) Server Authenticates network admins	Extend	LDC	Standard
8	System	PAM Server Network Admin Jumphost	Extend	HDC	Standard
9	System	Network Management System (NMS) RHEL 7.4	Extend	LDC	Standard

1. Categorize each component type with one of the following "System", or "Application", or "Hardware"
2. Indicate "Buy" for purchasing new components or subscribing to commercial cloud service or "Build" for developing a capability or "Extend" when making changes ontop of an existing component.
3. Specify hosting location as "HCC" (H-Commercial Cloud), "HPC" (H-Private Cloud), "HDC" (H-Data Center Co-location) or "LDC" (Local Data Centre) or "CC" (Commercial Cloud) or "GCC" (Govt Commercial Cloud) or "GDC Segregated" or "GDC Hosted" (Govt Data Center) or specify any other actual hosting site.
4. Indicate "Standard" if the component is under IHiS Technology Roadmap, otherwise indicate as "Non-Std".

Solution Components- Sample (Extension of Facility)

S/N	System / Application / Hardware [1]	Name & Purpose	Buy / Build / Extend[2]	Hosting Location[3]	Standard / Non-Std [4]
1	Application	Outpatient Administration System (OAS) – Patient administration	Extend	HDC	Standard
2	Application	1Queue – Queue System	Extend	HDC	Standard
3	Application	Workforce Optimizer System – Staff attendance system	Extend	HDC	Standard
4	Application	Ophthalmic Equipment Interface (OEI) – System for doctor to view patient's eye image taken from different medical systems	Extend	LDC & HDC	Standard
5	Application	SCM – Cluster electronic medical records system	Extend	HDC	Standard
6	Application	SAP-ISH - financial counselling and medical record function	Extend	HDC	Standard

All the above applications are existing applications and we are extending this to the new clinics

Applicable for:
1) Extension of facility/ ward.
2) New Buildings

Note
1. C
2. In … d" w…
3. Specify hosting location as "HDC" (IHiS Commercial Cloud), "IPC" (IHiS Private Cloud), "LDC" (IHiS Data Center Co-location) or "LDC" (Local Data Centre) or "CC" (Commercial Cloud) or "GCC" (Govt Commercial Cloud) or "GDC Segregated" or "GDC Hosted" (Govt Data Center) or specify any other actual hosting site.
4. Indicate "Standard" if the component is under IHiS Technology Roadmap, otherwise indicate as "Non-Std".

Solution Components- Quiz

What is wrong with the submission?

S/N	System / Application / Hardware [1]	Name & Purpose	Buy / Build / Extend[2]	Hosting Location[3]	Standard / Non-Std [4]
1	Operating System	Window Server 2016	Extend	HDC	Non-Std
2	System Software	MS SQL Server 2017	Build	HDC	Standard
3	Application	Clinician Dashboard for • User login • Patient Enrollment **Technology:** ReactJS 16.8.6	Extend	HCC	Non-Std
4	Application	NBSM system – Blood inventory tracking, distribution and cold chain management for blood products in HSA and BBLs	Build	GDC Segregated	Standard

This belongs to which App component?

Only specify System, Application or Hardware

Note:

1. Categorize each component type with one of the following "System", or "Application", or "Hardware"
2. Indicate "Buy" for purchasing new components or subscribing to commercial cloud service or "Build" for developing a capability or "Extend" when making changes ontop of an existing component.
3. Specify hosting location as "HCC" (H-Commercial Cloud), "HPC" (H-Private Cloud), "HDC" (H-Data Center Co-location) or "LDC" (Local Data Centre) or "CC" (Commercial Cloud) or "GCC" (Govt Commercial Cloud) or "GDC Segregated" or "GDC Hosted" (Govt Data Center) or specify any other actual hosting site.
4. Indicate "Standard" if the component is under IHiS Technology Roadmap, otherwise indicate as "Non-Std".

Solution Components- Recap

- Categorize components by system, application or hardware
- Include the purpose of each component
- Include the version, platform, specs, sizing (where applicable) for each component
- Include user login mechanisms like AD, SingPass, CorpPass etc

- Reuse existing components where possible.
- For New systems, there should be a corresponding hardware entry to support the platform.

- For solutions with a thick client accessing data repository:
  - Include no of clients and the location
  - Adopt application/ desktop virtualisation to access DB

- Refer to Hosting Guidelines for criteria to host systems in LDC

- Use MDM/MAM to manage and enforce policies on mobile devices

- Refer to latest Technology Roadmap and highlight deviations

Data Management- Overall Technical Controls

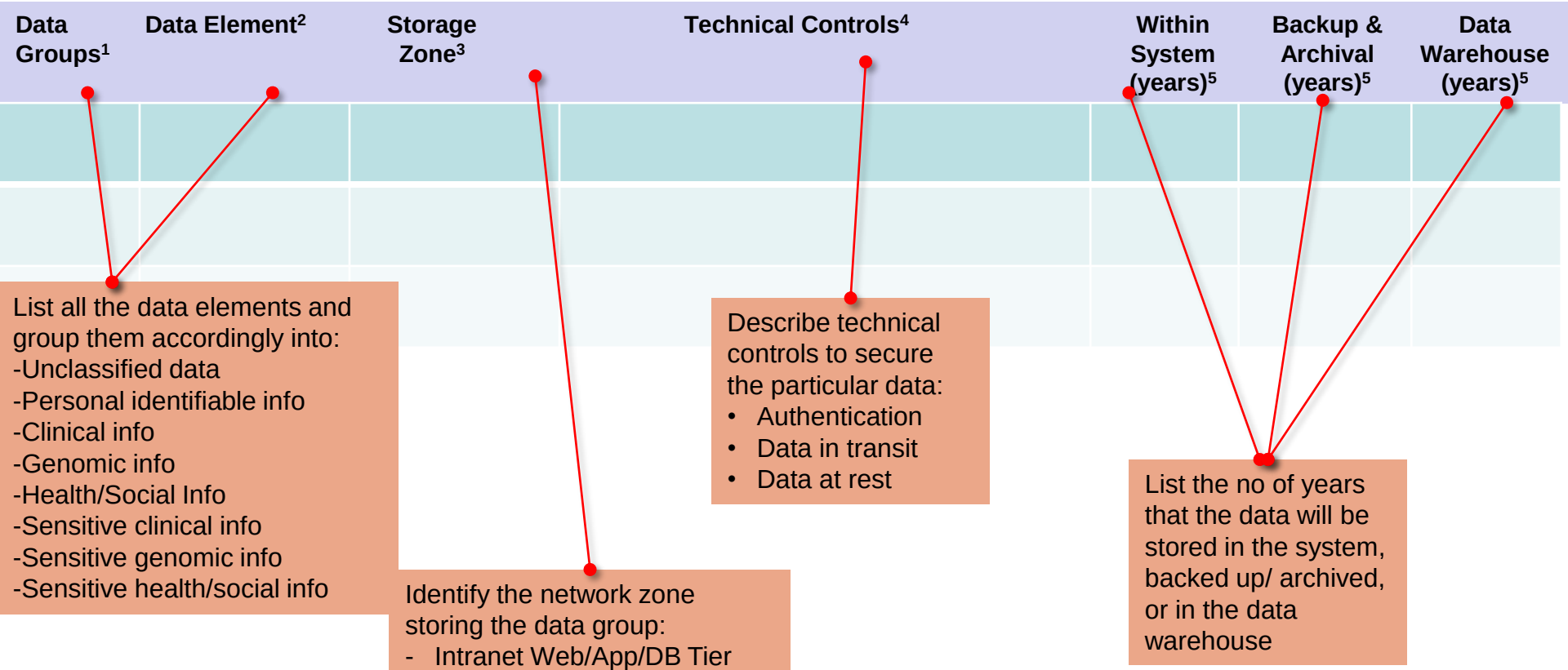
	Overall Technical Controls to secure the dataset **(Adapt controls for solution and remove non-applicable ones)**
Authentication	❑ IPSEC VPN authentication ❑ User account and password authentication ❑ 2FA authentication using SingPass/ CorpPass/ SGID ❑ Server side authentication with digital certificates ❑ Mutual authentication between source and destination digital certs using TLS 1.2 ❑ Others (elaborate)
Data in Transit	❑ Leased line AES256 encryption between Source and Destination sites ❑ Data is encrypted using TLS 1.2 when sent between Source and Destination system (e.g. HTTPS, SFTP ❑ Others (elaborate)
Data at Rest	❑ Application-level en ❑ SQL/ Oracle datab ❑ File based encryption: <Specify encryption method> ❑ DAM monitoring of DB activities ❑ Endpoint detection – use of SEP, ATP or EDR agents ❑ Others (elaborate)

- Include overall technical controls to secure the entire dataset:
  - Authentication
  - Data in transit
  - Data at rest
- Remove non-applicable controls.

Data Management- Overall Technical Controls Sample

	Overall Technical Controls to secure the dataset **(Remove non-applicable controls)**
Authentication	❑ AD authentication (SHS domain)
Data in Transit	❑ Data is encrypted using TLS 1.2 when sent between Source and Destination system ❑ SMB Encryption
Data at Rest	❑ SQL database TDE encryption ❑ Storage disk level encryption

Data Management



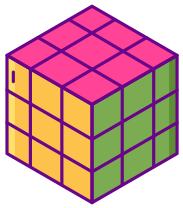
Note:

1. Categorize data into "Unclassified", "Personal Identifiable Info" (PII). "Clinical Info", "Genomic Info", "Health/Social Info", "Sensitive Clinical Info", "Sensitive Genomic Info" or "Sensitive Health/Social Info".
2. List down data elements in the data group.
3. Identify the network zones storing these data: "Intranet Web Tier", "Intranet App Tier", "Intranet DB Tier", "Internet Web Tier" "Internet App Tier", "Internet DB Tier" or others.
4. List the technical controls used to secure the data.
5. No of years of data that will be stored within the system, in backup & archive media and in the Data Warehouse (if any).

Data Management- Good sample

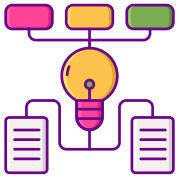
Data Groups[1]	Data Element[2]	Storage Zone[3]	Technical Controls[4]	Within System (years)[5]	Backup & Archival (years)[5]	Data Warehouse (years)[5]
1	RFP1: Thin Slice Management Lifecycle system					
Clinical Info	DICOM (images)	Intranet DB Tier	1. Authentications: Access to data is restricted to specific users identified by the Institution 2. Data at Rest: Storage disk level encryption. 3. Data in Transit: Data is encrypted using TLS 1.2 when sent between Source and Destination system. SMBv3 Encryption.	Study creation date + 2 years	2 year. No archival required as processed images will be stored at PACS.	N.A Data is not stored in DW
Personal identifiable info	Patient Master Data including Name, Age, Gender, NRIC;	Intranet DB Tier	1. Authentications: Access to data is restricted to specific users identified by the Institution 2. Data in Transit: Data is encrypted using HL7 over TLS 1.2	Study creation date +2 year	1 year retention period for backup and no archival is required.	N.A Data is not stored in DW
2	RFP2: Post processing advanced viewer					
Clinical Info	DICOM (images)	Intranet DB Tier	1. Authentications: Access to data is restricted to specific users identified by the Institution 2. Data at Rest: Storage disk level encryption. 3. Data in Transit: Data is encrypted using TLS 1.2 when sent between Source and Destination system. SMBv3 Encryption.	Study creation date + 6 months	<6 months. No archival required as processed images will be stored at PACS.	N.A Data is not stored in DW

Data Management- Recap



List down data elements and categorize them according to “Unclassified”, “Personal Identifiable Info”, “Clinical Info”, “Genomic Info”, ”Health/Social Info“, “Sensitive Clinical Info”, “Sensitive Genomic Info” or “Sensitive Health/Social Info”.

Indicate the network zone/tier storing the data



Provide the technical controls for authentication and measures to secure the data in transit and at rest

Overall technical controls – Measures to secure entire dataset
Specific technical controls – Measures to secure that particular data group

Always apply the technical requirements for high classification if the dataset contains data of different sensitivity levels e.g. diagnosis field may include records with sensitive health information

Solution Interfaces

S/N	Interface From	Interface To	Operation & Data Elements [1]	Protocol & Port No [2]	Daily Txn Load & ave payload size [3]
1					
2					
3					

Note:
1. Describe the purpose of the interface followed by the data subjects sent with reference to the Data Management slide.
2. Specify the protocol which would be used for the interfacing such as SFTP, HTTPS, LDAP, HL7, etc.
3. Provide the estimated median/average load per day. Include the average message payload.
4. The solution components mentioned in this interface table should be reflected in the solution components slide

Solution Interfaces- Sample

S/N	Interface From	Interface To	Operation & Data Elements [1]	Protocol & Port No [2]	Daily Txn Load & ave payload size [3]
1	HSA NBSM	NHG Cluster Blood Bank	• Get Blood product inventory status - Blood product details	HTTPS, REST (TLS 1.2 port 443)	Estimated about 100 txns (ave 15kb/ msg)
2	NGEMR EPIC	PIB App Server Via ESB	To send patient's admission, discharge and transfer info to PIB PII like NRIC is sent from EPIC. Medical conditions like drug allergies, fall risks etc	HL7 (Mutual TLS1.2 port 443)	Estimated 1085 beds * 10 times = 10,850 txns (ave 15kb . txn)
3	PIB Web Server	NHG Active Directory	To authenticate administrator's login with Active Directory	LDAPS (port 636)	Estimate 20 users 20*2 login a day =40 txns
4	PIB App Server	Hmail	To send notification alerts when interfaces or devices are down	SMTP (port 25)	1 email a day

Indicate intermediary middleware platforms (ESB/ API Gateway/ SFTP)

Purpose of interface and data sent (ref from data mgt slide) are stated

Protocol version, port nos, daily loads and ave payload are stated.

Note:

1. Describe the purpose of the interface followed by the data subjects sent with reference [illegible] t slide.
2. Specify the protocol which would be used for the interfacing such as SFTP, HTTPS, LDAP, HL7, etc.
3. Provide the estimated median/average load per day. Include the average message payload.
4. The solution components mentioned in this interface table should be reflected in the solution components slide

Solution Interfaces- Sample (Extension of Facility)

S/N	Interface From	Interface To	Operation & Data Elements [1]	Protocol & Port No [2]	Daily Txn Load & ave payload size [3]
1	Network switches	TACACS (ISE)	Put administrator credentials	TACACS+ TCP/49	- 5min interval
2	Wireless Access Point	Wireless Access Point Controller	Transport wireless traffic over encrypted tunnel Transport wireless control plane traffic over encrypted tunnel	CAPWAP UDP/5246 UDP/5247	- 3 – 5mins 1406 bytes
3	Wireless Access Point	Wireless Access Point	Wireless device telemetry (for user mobility)	UDP/16666	- 3-5 mins 1406 bytes
4	Network Switch, Wireless Access Point	NTP Server	For time synchronisation for accurate logging	UDP/123	- Every login or connection established
5	Network Switches, Wireless Access Point	NAC Server	Put user credentials Put machine credentials	RADIUS TCP/1645 TCP/1646	- Every user login - 3 to 5 mins intervals
6	PAM Server (Jumphost)	Network switches	Put administrator credentials, configurations Get configurations	SSH TCP/22	- Every user login
7	NMS (SNMP Manager)	NMS Network Switches	Get telemetry data – SNMP-Poll	UDP/161	- 5 mins interval, under 1480 bytes
8	NMS Network Switches	NMS (SNMP Manager)	Put telemetry data – SNMP Traps	UDP 162	- 5 mins interval, under 1480 bytes

3. Provide the estimated median/average load per day. Include the average message payload.
4. The solution components mentioned in this interface table should be reflected in the solution components slide

Solution Interfaces- Sample (Extension of Facility)

S/N	Interface From	Interface To	Operation & Data Elements [1]	Protocol & Port No [2]	Daily Txn Load & ave payload size [3]
1	EUC Devices	AD	Domain Controllers	TCP/UDP 53, TCP/UDP 88, TCP/UDP 123, TCP 135, UDP 137, UDP 138, TCP 139, TCP/UDP 389, TCP/UDP 445, TCP/UDP 464, TCP 636, TCP 3268, TCP 3269, TCP 9389, TCP/UDP 49152 – 65535	<100MB
2	EUC Devices	BigFix	Pushing patches to endpoints	UDP 52311	<100MB
3	EUC Devices	SEP	Corporate Anti Virus	TCP 443	<10MB
4	EUC Devices	EDR	Endpoint detection and response	TCP 443	<400MB
5	EUC Devices	ATP	Advance threat protection	TCP 2125 &	<10MB
6				137	
7	EUC Devices	DHCP	Assigning IP to the devices	UDP 67/68	<1MB

Applicable for:
1) Extension of facility/ ward.
2) New Buildings

Solution Interfaces- Recap

- The operation and data for of each interface are clearly stated.
- Data sent for each interface are referenced from the Data Management slide

- Components listed in the interface table are reflected in the Solution Components list.
- All interfaces in the table should appear in the architectural diagram.

- Ensure the interfaces between the sub-systems within a system is complete. If there many interfaces, attach an excel sheet listing all of them.

- Include the daily load and average payload size
- Indicate the unit of measurement when providing load info like ”6000 transactions per day” instead of just ”6000”
- Avoid giving load estimates like "> x messages per day"". Where possible, give a close estimates "~ x messages per day“. Show how you arrived at your estimates.

Target Solution Architecture Diagram

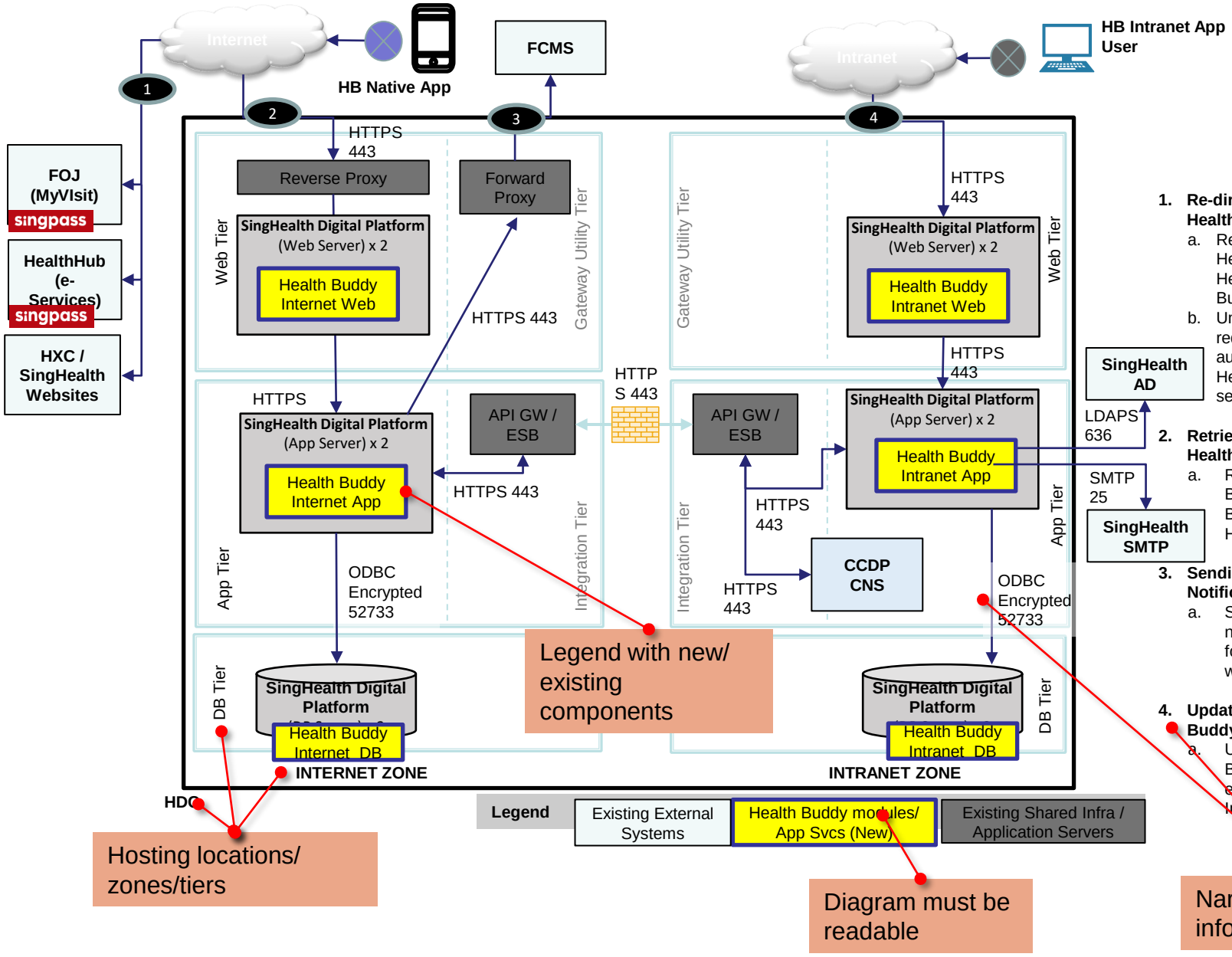
1. Proposed high-level application architecture diagram highlighting the solution components with their hosting location and information flow between them.

2. Highlight what is in scope in the diagram as well as the new and / or changed components.

3. Include a short narration to describe the information flows

4. Ensure that the diagram is readable. If required, break it down into logical sections for better readability.

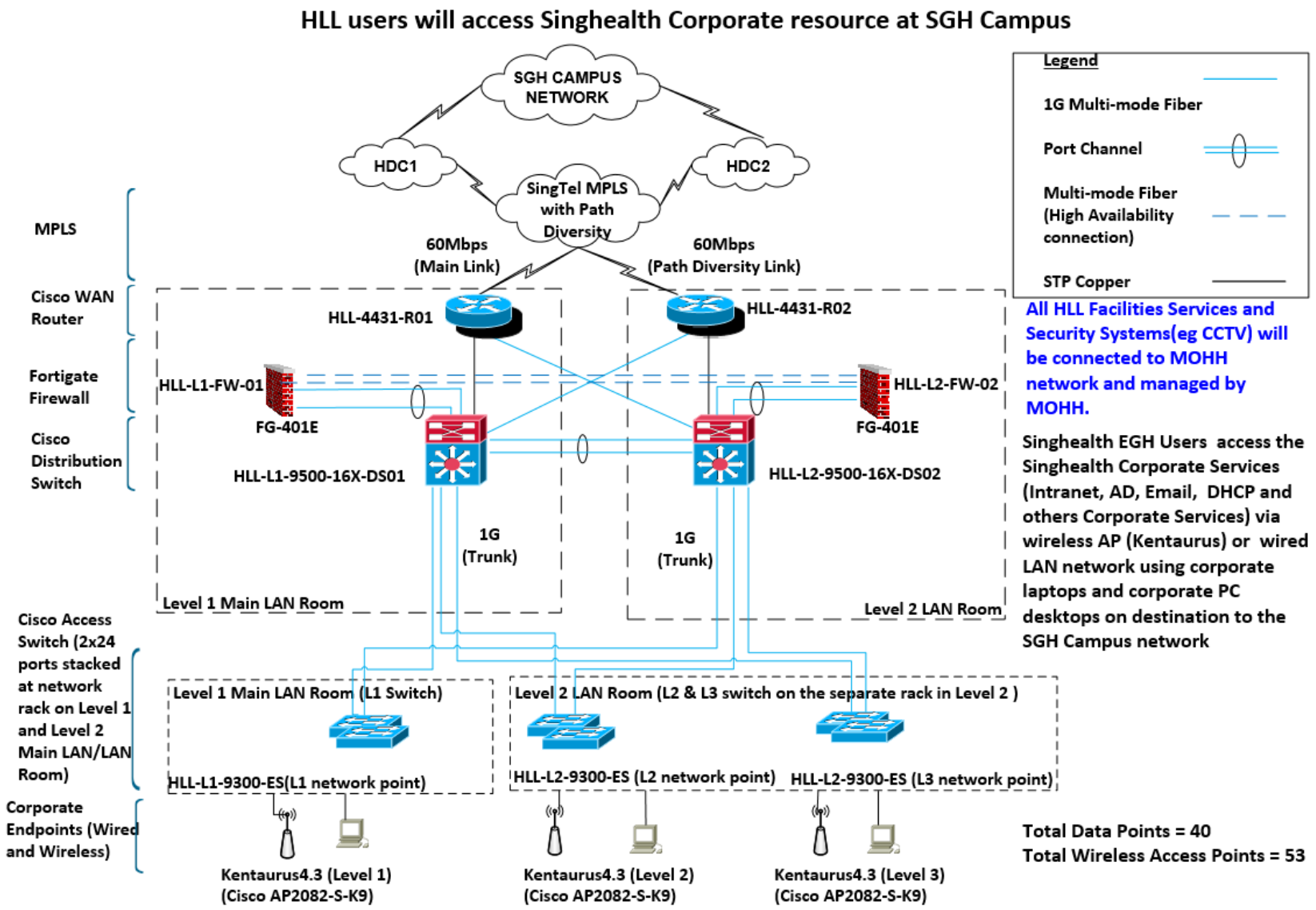
Target Solution Architecture Diagram - Sample



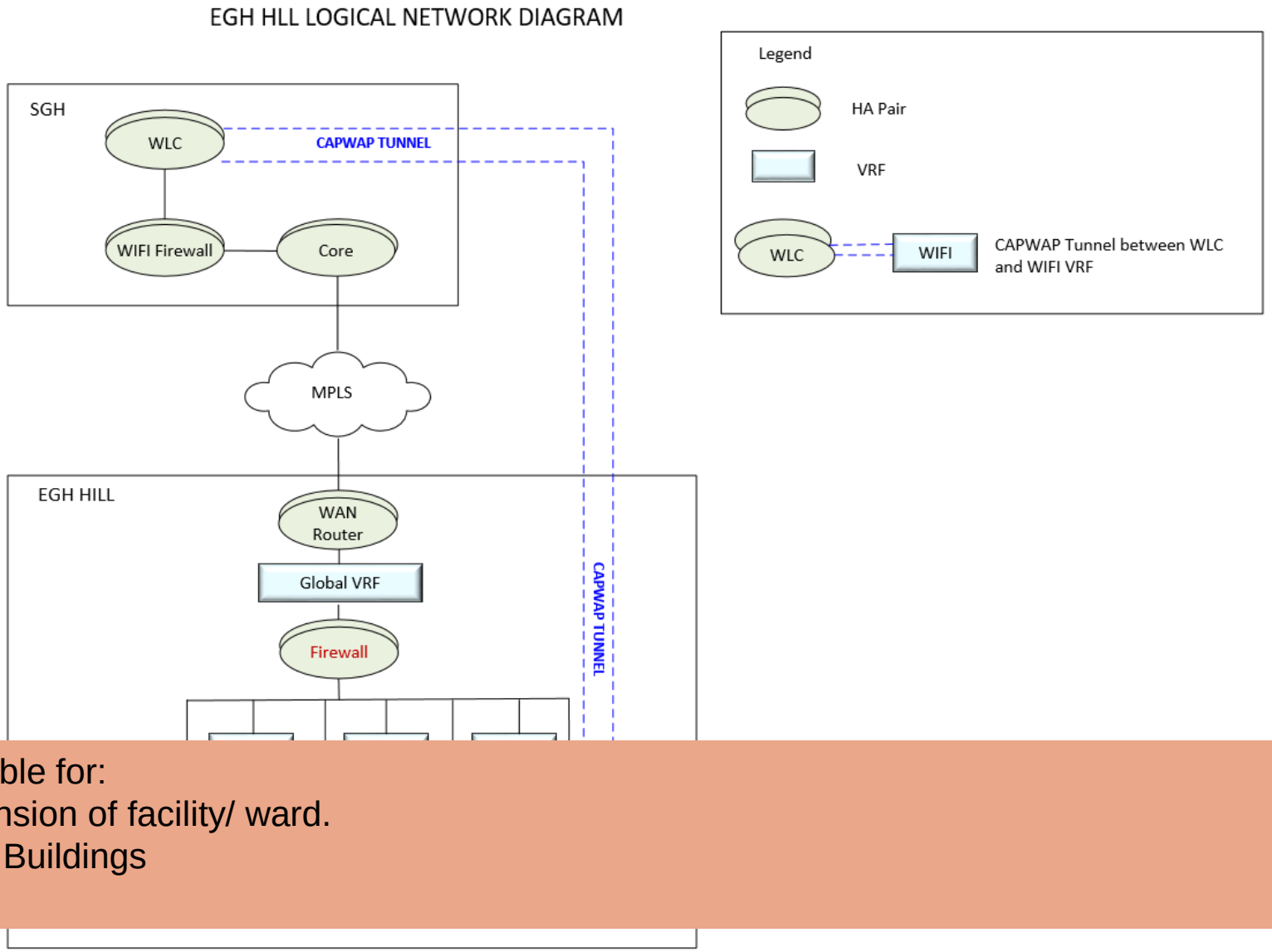
Notes

1. **Re-direction to MyVisit, HealthHub, HealthXchange**
   a. Redirection to MyVisit e-services, HealthHub e-services and HealthXchange using the Health Buddy web component
   b. Unauthenticated users will be redirected to Singpass for authentication before accessing HealthHub and MyVisit e-services.
2. **Retrieval of content for display on Health Buddy Native app**
   a. Retrieval of content by Health Buddy Intranet App from Health Buddy Intranet DB for display on Health Buddy Native app
3. **Sending of Broadcast Push Notification**
   a. Sending of broadcast push notification messages to FCMS for delivery to devices installed with Health Buddy
4. **Updating of content for Health Buddy Native app**
   a. Updating of content in Health Buddy Internet DB using APIs exposed by Health Buddy Internet App

HLL Architecture Network Diagram – Physical



Target Solution Architecture Diagram – Sample (New Facilities)



Applicable for:
1) Extension of facility/ ward.
2) New Buildings

Target Solution Architecture Diagram - Recap

- All components in the Solution components slide should appear in the architectural diagram.
- All interfaces in the Solution interfaces slide should appear in the architectural diagram.
- There should NOT be additional components or interfaces found in the diagram, but not in the Solution components and interfaces list. They should tally.

- When leveraging on existing system/solution, highlight what is new/changed to differentiate from what is existing

- Interface should be drawn to show the data initiation flow. (e.g. Sys A → Sys B if System A is initiating this interface to system B)

Responsibility for Non-Functional Requirements

Implementation Task	Agency/Vendor/Use*
Secure Code Review	
Data Migration	
Integration Test - Include Source and Destination parties	
High Availability Test	
Load Test	
Penetration Test	
Operation Acceptance Test	
End-to-End DR Testing	

Operational Task	Agency/Vendor/Use*
User Provisioning	
User Access Matrix Review	
End of Support Review	
Audit Log Review - Include Application and System logs	
App Health Check[1]	
L1 Support (Helpdesk)	
App L2 Support[1]	
App L3 Support[1]	
App Patch Management[1]	
System L2 Support[2]	
System L3 Support[2]	
System Patch Management[2]	

Indicate parties responsible for respective Apps

Indicate parties responsible for respective systems

Note:
*Indicate the Agency department/team, vendor, or business department/team who are responsible for the task.
[1]Indicate responsible party for every application
[2]Indicate responsible party for every system

Responsibility for Non-Functional Requirements- Sample

Implementation Task	Agency/Vendor/Use*
Secure Code Review	Deloitte
Data Migration	N.A. – Migration not in scope
Integration Test - Include Source and Destination parties	ST Engineering Mission Software & Svcs (ST MSS)
High Availability Test	N.A, - No H.A requirements
Load Test	ST MSS
Penetration Test	Deloitte
Operation Acceptance Test	ST MSS & IHiS iConnect
End-to-End DR Testing	Psychology Dept, IMH

Operational Task	Agency/Vendor/Use*
User Provisioning	IHiS iConnect
User Access Matrix Review	Psychology Dept, IMH
End of Support Review	MOHT + IHiS iConnect
Audit Log Review - Include Application and System logs	App log: User's HOD System log: ST MSS
App Health Check[1]	ST MSS
L1 Support (Helpdesk)	ST MSS
App L2 Support[1]	ST MSS & IHiS iConnect
App L3 Support[1]	ST MSS & IHiS iConnect
App Patch Management[1]	ST MSS & IHiS iConnect
System L2 Support[2]	H-Cloud and HCC
System L3 Support[2]	H-Cloud and AWS
System Patch Management[2]	H-Cloud and AWS

Where are the other parties?

Responsible Parties are clearly defined

Not clear on what these parties are responsible for!

Note:
*Indicate the Agency department/team, vendor, or business department/team who are responsible for the task.
[1]Indicate responsible party for every application
[2]Indicate responsible party for every system

Responsibility for Non-Functional Requirements- Recap

- All NFR are addressed completely; any N/A item must be justified
- All NFR responsible parties are unambiguous; indicate specific dept/team/ name of person

- Where multiple parties are involved for the same task, identify the main responsible party; else indicate specific area each party is responsible for.

- Where there are multiple platforms involved, identify the responsible party for each platform.

Risk Management

S/N	Risk Description	Gross Risk Rating (Likelihood, Consequence)#	Avoidance & Mitigation[2]	Residual Risk Rating (Likelihood, Consequence)#
Technology Risk				
1				
Implementation Risk				
1				
Security Risk				
1				

Level of risk before taking into account the effect of any planned controls

Technology risks are related to use of a technology or component in the solution
Implementation Risks are related to a development or deployment failure

Level of risk remaining after the inherent risk has been reduced by the planned controls
Residual risk rating has to be lower than gross risk

Populate from CyberSecurity Risk Mgt Worksheet

Planned action to reduce or mitigate inherent risk

eview the "Source of Solution Risk", and select those that apply to your solution. Refine by
me of the non-standard component. Include others not found in the list as well.
efine.

3. Use the likelihoc
4. Review the sugg
5. Use the likelihoc
6. Use the above t

t.

Notes
Input format: Risk
Risk rating = "Very
Likelihood = Range
Consequence = Ra

A well-structured risk description should articulate the following four (4) key elements:
(a) Asset
(b) Threat event
(c) Vulnerability
(d) Consequence
E.g. "**Attacker performs an SQL injection** on an **unpatched legacy web application** to **download sensitive patient medical records**"

Risk Management- Sample

S/N	Risk Description	Gross Risk Rating (Likelihood, Consequence)#	Avoidance & Mitigation[2]	Residual Risk Rating (Likelihood, Consequence)#
Technology Risk				
1	RFP1: Thin Slice Life Cycle Management system does not support TDE due to product limitation	L (1.2)	Known existing product limitation. This product limitation is on the roadmap for version 15 release.	L (1,2)
Implementation Risk				
1	Project delay due to impact from COVID-19	M (3.3)	Expedite the implementation by configuring the virtual machines while waiting for hardware delivery. Project implementation for 3 sites will be carried out concurrently.	L (2,2)
Security Risk				
1	RFP1: Thin Slice Life Cycle Management System depends on certain 3rd party software (7Zip, Apache, Redit, etc) as part of its system functionalities that could potentially contain security vulnerabilities	M (3.3)	Conduct regular review and patching for these 3rd party tools with vendors. Include this as part of vendor maintenance scope.	L (1,2)
2	RFP1: Thin Slice Life Cycle Management System requires a thick client to directly access the DB server for admin module activities from end user workstations. In the event of user endpoints are compromised, it could result in data breach/leakage from the DB server.	M (2.3)	Install admin module on Citrix server which is a secured environment at application tier. Users will not directly access the admin module from their client PC.	L (1,2)
3	RFP2: Post Processing Advanced Viewer System “Vitrea Solution Health Server” (statistics server) database component cannot be separated from its other tiers therefore end users access the web portal that is located together with its database component. In the event of user endpoints are compromised, it could result in data breach/leakage from the database component.	L (2.2)	There is no sensitive data stored in this server. This server will not be connected to SQL database.	L (1,1)

Risk Management- Sample 2

S/N	Risk Description	Gross Risk Rating (Likelihood, Consequence)#	Avoidance & Mitigation[2]	Residual Risk Rating (Likelihood, Consequence)#
1	Cloud connector patches - Patches are released once in a Quarter; If patches are not applied timely, the connector will cease working	3,5	Vendor to liaise with SAP on the release data periodically. Cloud connector will have active-passive HA setup so that patches can be applied in passive and can be made active once completed	3,5
2	Cloud Connector: Operating System Windows 2016 EOS is Nov 22	3,3	Extended support is until Dec 2027 Project team to do tech refresh in FY22	3,3
Security Risk				
1	SAP BTP connection to SAP Cloud connector (SCC) on premise (internet Zone) - Potential Data leakage in internet zone	1.1	The connection will be opened to specific IP Encrypted tunnel (TLS 1.2) between SCC and SCP Data is encrypted at rest and in transit	1.1
2	"Lack" of API gateway is security risk	3,3	2-way SSL between internet ESB and intranet ESB	3,3

Notes
Input format: Risk Rating (Likelihood, Consequence). e.g. H (3,4)
Risk rating = "Very High" (VH), "High" (H), "Medium" (M), "Medium High" (
Likelihood = Range of 1 (Low) to 5 (High)
Consequence = Range of 1 (Low) to 5 (High)

1) Gross Risk and Residual Risk rating are the same!
2) Wrong format.

CyberSecurity Risk Management Tool

- For Security risks: Teams should use the Cybersecurity Risk Management tool and seek help from their TISO.

S/N	Date of risk identified	(A) Threat (What)	(B) Risk/ Vulnerability (How)	(C) Gross Risk	(D) Existing Controls	(E) Current Risk	(F) Risk Tr		
		Risk Scenarios	Vulnerability	Gross Risk (L/ M/ H/ V	Existing Controls	Current Risk (with existi controls)	Treatment Plan	Residual Risk after Treatmer	Target Implementatio
Example: RS1	Example: 8/11/2020	Example: Adversary exploits unpatched or poorly configured CII applications, systems, and infrastructures to compromise the confidentiality, integrity and availability of CII Assets and Information.	Example: "- Lack offinadequate patch management tools to ensure that operating systems are running the most recent security updates/patches provided by the software vendor - Lack offinadequate hardening configuration tools to ensure that all CII databases are hardened against standardized hardening templates on a regular basis - Lack offinadequate network device configuration tools to ensure that the latest stable version of any security-related updates are installed on all network devices. - Lack offinadequate automated VA scans conducted to identify vulnerabilities for networks and servers - Lack offinadequate PT performed to verify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully	High	Example: - Annual hardening compliance scan (configuration scan) - Patch management process to patch applications, systems, and infrastructures - VA to address and close any known vulnerability and VA scan to cover all devices in the asset dossier (indicated in the new HIM-ISP requirement to cover Apps, network and OS) - Penetration Testing - Existing mechanism of Doer and Verifier for any approved change (Infrastructure change and Application software change) - Existing Defence-in-depth security measures to address any exfiltration of data such as SEP, TRAPS, DAM, PAM, 24x7 security monitoring, physical security of DC, etc. - Next Generation Firewall - IPS/IDS features deployed - VLAN/logical segmentation of network - Whitelist of software installation on servers and endpoints (for Hcloud only) - Security baselines are redeployed to Citrix servers on a weekly basis - Obtained third party cybersecurity attestation from the vendors - CSM 18 -Completed review and hardening of Citrix Architecture	Medium	Example: 'The following measures will be implemented to reduce the risk rating to Low: 1. Data Encryption 2. DAM - data access policy implementation	Low	Example: 8/11/21
RS1		Add new risk scenario as applicable	Add vulnerabilities as applicable	to Be evaluated	Add controls as applicable	to Be evaluated		to Be evaluated - For the risks beyond the tolerance	
RS2		Add new risk scenario as applicable	Add vulnerabilities as applicable	to Be evaluated	Add controls as applicable	to Be evaluated		to Be evaluated - For the risks beyond the tolerance	
RS3		Add new risk scenario as applicable	Add vulnerabilities as applicable	to Be evaluated	Add controls as applicable	to Be evaluated		to Be evaluated - For the risks beyond the tolerance	
RS4		Add new risk scenario as applicable	Add vulnerabilities as applicable	to Be evaluated	Add controls as applicable	to Be evaluated		to Be evaluated - For the risks beyond the tolerance	
RS5		Add new risk scenario as applicable	Add vulnerabilities as applicable	to Be evaluated	Add controls as applicable	to Be evaluated		to Be evaluated - For the risks beyond the tolerance	
RS6		Add new risk scenario as applicable	Add vulnerabilities as applicable	to Be evaluated	Add controls as applicable	to Be evaluated		to Be evaluated - For the risks beyond the tolerance	
RS7		Add new risk scenario as applicable	Add vulnerabilities as applicable	to Be evaluated	Add controls as applicable	to Be evaluated		to Be evaluated - For the risks beyond the tolerance	

Solution Risk Tool- Introduction

- This tool is meant to help project teams to identify the risks for the project presented at SRB and PPSC.

- Based on the risks highlighted during SRB and is not exhaustive. Welcome additions and suggestions to further refine the tool.

RIsk ID	Source of Risk	Risk Description	Gross Risk Rating (Likelihood, Severity of Impact)	Avoidance (A) & Mitigation (M)	Residual Risk Rating (Likelihood, Severity of Impact)
	Implementation Risk				
1					
2					
3					
	Security Risk				
1					
2					
3					
	Technology Risk				
1					
2					
3					
	RIsk Rating = L, M, MH, H, VH				
	Likelihood = 1 to 5				
	Severity of Impact = 1 to 5				
	Values				
	M (1,5)				
	L (1,4)				

Introduction | Risk Samples | Risk Matrix and Tolerance | **Risk Worksheet** | Risk sample | Compl ...

Solution Risk Tool- Step 1 Solution Risk Source

- Review the "Source of Solution Risk“ (Risk Canvas) and select those that apply to your solution. Filter by Solution Risk Categories, then select the actual source of risk, e.g. use of the non-standard component.

		Source of Solution Risk	Risk Description	Avoidance (A) & Mitigation (M)
A		Components		
A	1	Non-standard OS or middleware components	Extended outage due to lack of skilled internal resources or poor configuration	(A) Use equivalent standard components. (M) Vendor has sufficient skilled resources to support. There is evidence of this from the vendor's recent projects. This resourcing will be reviewed periodically. (M) Purchase premium support from product principal.
A	2	Open source platform components	Extended outage due to lack of support;	(A) Use well established, commercially supported equivalents. (M) Vendor or internal team has sufficient skilled resources to support. The budget has been revised upwards to support this. The resourcing will be reviewed periodically. (M) Establish periodic monitoring of community support forum for patches and EOS. Establish patching cycle and monitoring of compliance to patch cycle.
A	3	Open source with copyleft	Unable to meet copyleft licensing obligations; cost and risk to	(A) Purchase well established, commercially supported equivalent.

1. Filter based on Solution Risk Categories
A) Components
B) Interfaces
C) Deployment Architecture
D) Non-Functional Requirements
E) Implementation

2. Select Source of Risk that is applicable for your project

3. Copy Risk Descriptions and Avoidance and Mitigation Actions into Risk worksheet tab

Solution Risk Tool- Step 2 Refine Risk Description

- Review the risk description and refine.

RIsk ID	Source of Risk	Risk Description	Gross Risk Rating (Likelihood, Severity of Impact)	Avoidance (A) & Mitigation (M)	Residual Risk Rating (Likelihood, Severity of Impact)
	Implementation Risk				
1	Skilled or certified resources required, e.g. software platform, network, security.	Use of under qualified or role-mismatched staff for critical roles, leading to widespread quality issues and rework.		(A) Pre-qualified and certified staff will be hired as part of resource mobilisation, and there is sufficient runway for the hiring, e.g. 6 months. (A) Provision for early training and certification for identified staff. (M) Engage and control external certified professionals to augment the team	
1A	Skilled or certified resources required to implement NeMSW Pega platform	Use of under qualified or role-mismatched staff for critical roles such as UI designer/ System Architect may lead to widespread quality issues and rework.		(A) Pre-qualified and certified staff will be hired as part of resource mobilisation, and there is sufficient runway for the hiring, e.g. 6 months. (A) Provision for early training and certification for identified staff. (M) Engage and control external certified professionals to augment the team	

Solution Risk Tool- Step 3 Assess likelihood and impact

	Tolerance of Solution Risks
Very High	• Risk should not be accepted. • Immediate corrective action is required if the system is already live. • For inflight implementations, the solution must be corrected to reduce risk to an acceptable level before go-live.
High	(same as Very High)
Medium High	• Risk can be accepted, if there are no solutions due to technical, operational and cost feasibility constraints. • The acceptance needs to be documented in the product risk register, with reasons and justifications, and with appropriate management approval.
Medium	(same as Medium-High)
Low	• Risk can be accepted.

Risk Matrix

Severity of impact		Likelihood of Occurrence				
		Rare 1	Unlikely 2	Possible 3	Likely 4	Highly Likely 5
Very Severe 5		Medium	Medium High	High	Very High	Very High
Severe 4		Low	Medium	Medium High	High	Very High
Moderate 3		Low	Medium	Medium	Medium High	High
Minor 2		Low	Low	Medium	Medium	Medium High
Negligible 1		Low	Low	Low	Low	Medium

Solution Risk Tool- Step 3 Assess likelihood and impact

- Use the likelihood guide to calculate gross risk.

Likelihood Parameters	(1) Rare	(2) Unlikely	(3) Possible	(4) Likely	(5) Almost Certain
Frequency of Occurrence	May occur once every 5 years or more	May occur once every 2 – 4 years	May occur once a year up to a few times a year (i.e. 1 – 4 times a year)	Will probably occur several times a year up to once a month (i.e. 5 – 12 times a year)	Expected to occur more than 12 times a year
Probability	< 5% chance of occurring within the 3 years horizon	Between 5% and 25% chance of occurring within the 3 years horizon	Between 25% and 50% chance of occurring within the 3 years horizon	Between 50% and 75% chance of occurring within the 3 years horizon	≥ 75% chance of occurring within the 3 years horizon
Qualitative Descriptor	Remote and not expected to occur, conceivable only under extreme circumstances	Conceivable but no indications or evidence to suggest occurrence under normal circumstances	Has occurred before, and some indications to suggest possibility of re-occurrence	Some evidence to suggest expected occurrence	Strong evidence to suggest the risk will occur or may occur repeatedly

Solution Risk Tool- Step 3 Assess likelihood and impact

- Use the impact guide to calculate gross risk.

Descriptor	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Severe
Strategic / Reputation	• No significant adverse publicity • No impact on credibility and key stakeholders' confidence	• Publicity on adverse event contained / Limited media exposure • Limited impact on credibility and key stakeholders' confidence	• Unfavourable publicity in multiple media (including social media) • Damage to reputation from key stakeholders' perspective • Some public discussions and calls for specific actions	• Negative publicity in multiple media (including social media) • Damage to reputation from a healthcare industry perspective • Loss of credibility and key stakeholders' confidence • Widespread negative public discussions	• Company's credibility and effectiveness called to question at the national level and beyond • Negative publicity or damage to reputation from a national perspective • Total loss of credibility and key stakeholders' confidence • Political intervention required
Legal and Regulations	• No adverse legal and regulatory consequence	• Verbal warning by authorities	• Formal warning from regulatory body	• Sanction or penalty from regulatory body (e.g. fines)	• Statutory punishment resulting in suspension / removal of license, prison term or criminal liability • Ministerial censure or direct intervention from authorities

Solution Risk Tool- Step 3 Assess likelihood and impact

- Use the impact guide to calculate gross risk.

Descriptor	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Severe
Financial	< 0.5% of total operating expenses	0.5-1% of total operating Expenses	1-2%* of total operating Expenses	2-5%* of total operating Expenses	> 5% of total operating expenses
Human Capital	• Attrition Rate- Sporadic (<5%) • Normal staff turnover, as compared to national average for last quarter • No impact on critical business functions	• Attrition Rate - Intermittent (5-9%) • Turnover higher than national average for last quarter • Minor short term staff discontent readily resolvable • Minimal impact on critical business functions	• Attrition Rate – Frequent (10-14%) • Turnover higher than national average for last quarter with short term negative impact on staff morale and productivity • Staff discontent causing short term negative impact on staff morale and productivity • Substantial impact on critical business functions	• Attrition Rate – Regular (15-19%) • Turnover consistently higher than national average for past two consecutive quarters with negative impact on staff morale and productivity • Significant staff discontent causing negative impact on staff morale and productivity. • Significant impact on critical business functions	• Attrition Rate – Massive (>20%) • Prolonged staff turnover issues, turnover consistently higher than national average for past three consecutive quarters, with long-term negative impact on staff morale and productivity • Prolonged staff discontent causing long term negative impact on staff morale and productivity. • Prolonged significant impact on critical business functions

Solution Risk Tool- Step 3 Assess likelihood and impact

- Use the impact guide to calculate gross risk.

Descriptor	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Severe
Workplace Health And Safety	• Negligible injury • Hospitalisation not required	• Minor non-permanent injury • Reversible disability / impairment / disorder • First Aid / Medical Treatment • Hospitalisation not required	• Semi-permanent injury • Moderate irreversible disability / impairment / disorder • Loss time or restricted duty	• Major permanent injury • Severe disability / impairment / disorder • Significant loss time or prolonged restricted duty	• Death
Project Schedule and Cost	≤ 5% schedule slip or cost overrun	5-10% project schedule slip or cost overrun	10-15% project schedule slip or cost overrun	15-20% project schedule slip or cost overrun	> 20% project schedule slip or cost overrun
Mission Critical System Disruption (Unplanned)	Downtime < 22 min (99.95%)	Downtime < 44 min (99.9%)	Downtime 44-120 min	Downtime 120 min - 3.6 hrs (99.5%)	Downtime > 3.6 hours

Solution Risk Tool- Step 3 Assess likelihood and impact

- Use the impact guide to calculate gross risk.

Descriptor	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Severe
Information & IT Security – IT Security (System Breaches)	Unsuccessful attempts to gain access to systems or data	Breach of security or virus attack resulting in warnings.	Breach of security or virus attack resulting in temporary disruption of services (2 to <4 hours)	Breach of security or virus attack resulting in suspension of services (≤ 1 day).	Breach of security or virus attack resulting in suspension of services (>1 day)
Information& IT Security – Leakage or Corruption of Information / Data	• Personal data loss that only involves business contact information • Inadvertent disclosures to other staff or other persons under obligation to confidentiality	• Administrative errors that can be recovered in time such that the data recipient is unlikely to make further data disclosure • Inconsequential data loss, such as loss of data protected by encryption and strong passwords in portable storage media	• Unauthorised disclosure of personal data that is unlikely to give rise to discrimination or any other negative impact against a person and affecting less than 100 individuals • Calls for specific actions to notify affected individuals whose personal data have been compromised	• Unauthorised disclosure of personal data that is unlikely to give rise to discrimination or any other negative impact against a person and affecting more than/ equal to 100 individuals • Unauthorised disclosure involving health information that could (a) lead to stigmatization or discrimination, or (b) warrants special protection by legislation and affecting less than 100 individuals	• Unauthorised disclosure involving health information that could (a) lead to stigmatization or discrimination, or (b) warrants special protection by legislation and affecting more than/ equal to 100 individuals

Solution Risk Tool- Step 3 Assess likelihood and impact

- Use the impact guide to calculate gross risk.

Descriptor	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Severe
Patient Safety	• Patients with no injury or increased level of care or length of stay. • Will include near misses.	• Patients requiring increased level of care, including the following: • Review & evaluation • Additional investigation • Referral to another clinician	• Patients with permanent lessening of bodily functioning (sensory, motor, physiologic or intellectual) unrelated to the natural course of the illness and differing from the expected outcome of patient management or any of the following: • Increased length of stay • Additional operation or procedure	• Patients with major permanent loss of function (sensory, motor, physiologic or intellectual) unrelated to the natural course of the illness and differing from the expected outcome of patient management or any of the following: • Disfigurement • Surgical intervention required	• Patients with death, unrelated to the natural course of the illness & differing from the immediate expected outcome of the patient management or any of the following: • Procedures involving the wrong patient or body part • Suicide • Retained instruments or other material requiring surgical procedure • Intravascular gas embolism resulting in death or neurological damage • Haemolytic blood transfusion • Medical effort leading to death • Material death or serious morbidity associated with labour or delivery • Infant abduction or discharge to wrong family

Solution Risk Tool- Step 3 Assess likelihood and impact

- Use the impact guide to calculate gross risk.

Descriptor	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Severe
Impact to Environment	No impact or negligible impact to the environment	Minor damage to the environment; damage may take some time to recover	• Some damage to the environment; damage may take a significant time to recover • Warnings may be imposed by regulator(s)	• Major damage to the environment which may lead to irreversible impact to the environment • Warnings and fines imposed by regulator(s)	• Severe damage to the environment; damage is irreversible • Severe fines imposed by regulator(s) and/or organisation is forced to stop its work process

Solution Risk Tool- Step 3 Assess likelihood and impact

	Tolerance of Solution Risks
Very High	• Risk should not be accepted. • Immediate corrective action is required if the system is already live. • For inflight implementations, the solution must be corrected to reduce risk to an acceptable level before go-live.
High	(same as Very High)
Medium High	• Risk can be accepted, if there are no solutions due to technical, operational and cost feasibility constraints. • The acceptance needs to be documented in the product risk register, with reasons and justifications, and with appropriate management approval.
Medium	(same as Medium-High)
Low	• Risk can be accepted.

Risk Matrix

Severity of impact	Rare 1	Unlikely 2	Possible 3	Likely 4	Highly Likely 5
Very Severe 5	Medium	Medium High	High	Very High	Very High
Severe 4	Low	Medium	Medium High	High	Very High
Moderate 3	Low	Medium	Medium	Medium High	High
Minor 2	Low	Low	Medium	Medium	Medium High
Negligible 1	Low	Low	Low	Low	Medium

Likelihood of Occurrence

Gross risk rating assessed as H(4,4)

Solution Risk Tool- Step 4 Review actions

- Review the suggested avoidance and mitigation and select those that are feasible and will be <u>implemented</u> for your project.

RIsk ID	Source of Risk	Risk Description	Gross Risk Rating (Likelihood, Severity of Impact)	Avoidance (A) & Mitigation (M)	Residual Risk Rating (Likelihood, Severity of Impact)
	Implementation Risk				
1	Skilled or certified resources required, e.g. software platform, network, security.	Use of under qualified or role-mismatched staff for critical roles, leading to widespread quality issues and rework.		(A) Pre-qualified and certified staff will be hired as part of resource mobilisation, and there is sufficient runway for the hiring, e.g. 6 months. (A) Provision for early training and certification for identified staff. (M) Engage and control external certified professionals to augment the team	
1A	Skilled or certified resources required to implement NeMSW Pega platform	Use of under qualified or role-mismatched staff for critical roles such as UI designer/ System Architect may lead to widespread quality issues and rework.	(H4,4)	- Pre-qualified and certified staff will be hired as part of resource mobilisation. - Provision for training and certification for existing staff. - Engage external certified professionals to augment the team	

Solution Risk Tool- Step 5 Re-assess likelihood and impact

	Tolerance of Solution Risks
Very High	• Risk should not be accepted. • Immediate corrective action is required if the system is already live. • For inflight implementations, the solution must be corrected to reduce risk to an acceptable level before go-live.
High	(same as Very High)
Medium High	• Risk can be accepted, if there are no solutions due to technical, operational and cost feasibility constraints. • The acceptance needs to be documented in the product risk register, with reasons and justifications, and with appropriate management approval.
Medium	(same as Medium-High)
Low	• Risk can be accepted.

Risk Matrix

Severity of impact	Rare 1	Unlikely 2	Possible 3	Likely 4	Highly Likely 5
Very Severe 5	Medium	Medium High	High	Very High	Very High
Severe 4	Low	Medium	Medium High	High	Very High
Moderate 3	Low	Medium	Medium	Medium High	High
Minor 2	Low	Low	Medium	Medium	Medium High
Negligible 1	Low	Low	Low	Low	Medium

Likelihood of Occurrence

Residual risk rating Assessed as M(2,4)

Solution Risk Tool- Step 6 Repeat for rest of identified risks

RIsk ID	Source of Risk	Risk Description	Gross Risk Rating (Likelihood, Severity of Impact)	Avoidance (A) & Mitigation (M)	Residual Risk Rating (Likelihood, Severity of Impact)
	Implementation Risk				
1	Skilled or certified resources required to implement NeMSW Pega platform	Use of under qualified or role-mismatched staff for critical roles such as UI designer/ System Architect may lead to widespread quality issues and rework.	(H4,4)	- Pre-qualified and certified staff will be hired as part of resource mobilisation. - Provision for training and certification for existing staff. - Engage external certified professionals to augment the team	M(2,4)
2	Multiple parties in the delivery	Highly serialised work structure and tight dependencies that may result in missed dependencies leading to project delays.	M(3,3)	-Tasks are broken down further to reduce hard dependencies, and dependencies are closely monitored.	M(2,3)
	Security Risk				
1	Impending EOS components	Critical defects not addressed leading to system vulnerable to security compromises	H(4,4)	Upgrade to latest stable supported versions.	L(1,4)
2	Open source platform components	Extended outage due to lack of support;	H(4,4)	Use well established, commercially supported equivalents.	L(1,4)
	Technology Risk				
1	Non-standard OS and components	Extended outage due to lack of skilled internal resources	M(3,3)	Purchase premium support from product principal.	L(1,3)
2	Batch interfaces	Functional failure because data received at Smart DataHub is incomplete.	M(3,3)	Reconcile data when receive and implement monitoring and alerts during batch job completion	M(2,3)
3	Non-standard application monitoring	Slower response to problems due to skills gaps in application level monitoring.	MH(3,4)	Train the internal team to use the monitoring tool; provision the budget for training and manpower for the non-standard tool	L(1,3)

Solution Risk Tool- Step 7 Populate SRB/PPSC deck

- Populate entries from the risk worksheet to the SRB/PPSC deck
- Table risks with your stakeholders, and track in the system risk register.

S/N	Risk Description	Gross Risk Rating (Likelihood, Consequence)#	Avoidance & Mitigation[2]	Residual Risk Rating (Likelihood, Consequence)#
Implementation Risk				
1	Use of under qualified or role-mismatched staff for critical roles such as UI designer/ System Architect may lead to widespread quality issues and rework.	(H4,4)	- Pre-qualified and certified staff will be hired as part of resource mobilisation. - Provision for training and certification for existing staff. - Engage external certified professionals to augment the team	M(2,4)
2	Highly serialised work structure and tight dependencies that may result in missed dependencies leading to project delays.	M(3,3)	-Tasks are broken down further to reduce hard dependencies, and dependencies are closely monitored.	M(2,3)
Security Risk				
1	Critical defects not addressed leading to system vulnerable to security compromises	H(4,4)	Upgrade to latest stable supported versions.	L(1,4)
2	Extended outage due to lack of support;	H(4,4)	Use well established, commercially supported equivalents.	L(1,4)
Technology Risk				
1	Extended outage due to lack of skilled internal resources	M(3,3)	Purchase premium support from product principal.	L(1,3)
2	Functional failure because data received at Smart DataHub is incomplete.	M(3,3)	Reconcile data when receive and implement monitoring and alerts during batch job completion	M(2,3)
3	Slower response to problems due to skills gaps in application level monitoring.	MH(3,4)	Train the internal team to use the monitoring tool; provision the budget for training and manpower for the non-standard tool	L(1,3)

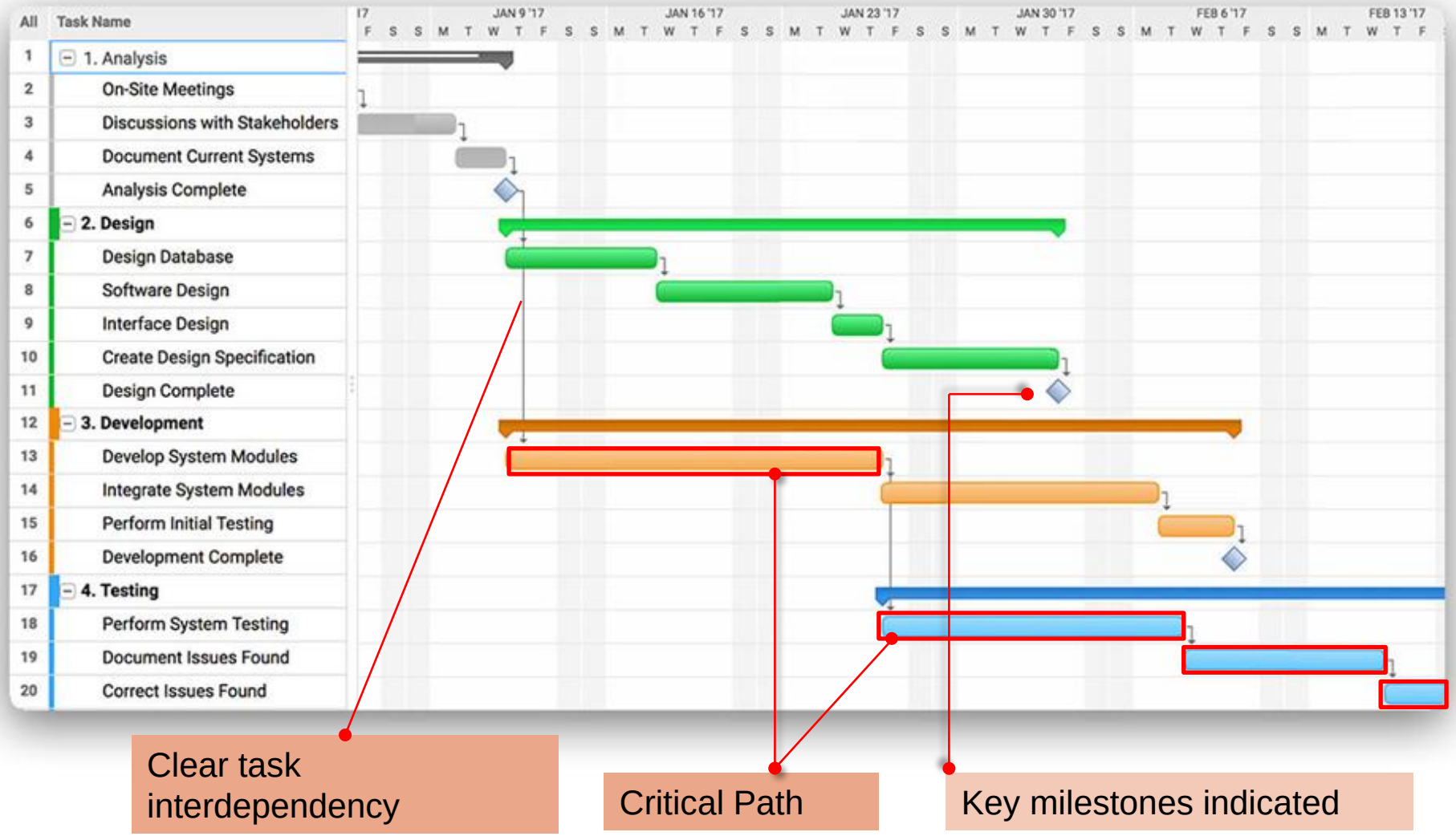
Project Planned Schedule

1. Insert the project schedule in the form of Gantt chart

2. The schedule should detail the project works with the expected time duration and any interdependency and critical path between the tasks.

3. Include key milestones, deliverables and critical path(s).

Project Planned Schedule- Sample



1 Improve Business Case Review

2) Benefits & KPIs:

Indicate 3 to 5 KPIs in the following categories project targets to achieve:

(1) Manpower Productivity
(2) Clinical / Care Effectiveness,
(3) Process / Operational Improvements
(4) Population Health / Preventive Health
(5) IT Security / Resiliency
(6) Adoption / Engagement
(7) Systems Decommissioning & Cost Savings

Outcome Categories	KPI Examples	Cost Savings / Effectiveness Examples
1) Manpower Productivity	Reduction in man-hours / staff numbers	Savings to manpower costs (e.g. Reduced 98% time or 100 FTE hours per month to track expired stocks * FTE salary rates)
2) Clinical / Care Effectiveness	a) Reduction in errors / re-works b) Lesser infections, decreased complications, reduced diseases rates c) Reduction in re-admissions / unnecessary tests / treatments / healthcare service utilisation / LOS	a) Cost savings on re-works (e.g. reducing reworks due to human errors by 5% per year = 5% x load x ave cost $10 per test b) Lower cost of care to achieve desired health outcomes (e.g. from reduced occurrences) c) Lower cost of care to treat / manage patients
3) Process / Operational Improvements	a) Shorter turnaround time to services / transit patients, reduction in waiting time b) Higher throughput, increased capacity / volume / transactions / load	Savings to equipment costs, manpower costs translated from time savings

1 Improve Business Case Review

Refer to PPSC Template on Framework for Articulating Benefits Outcomes / KPIs

Presentation

2) Benefits & KPIs:

Outcome Categories	KPI Examples	Cost Savings / Effectiveness Examples
4) Population / Preventive Health	a) Reduced disease rates with early detections b) Improve Disability-Adjusted Life Year (DALY), Quality-Adjusted Life-Year (QALY)	a) Reduced costs of managing patients with certain diseases/conditions (e.g. cost of managing CKD patients per year * % of reduced instances with early detection) b) Savings in life years, converted based on GDP/capita
5) IT Security / Resiliency	a) Reduced security threats / attacks / risks, reduced unauthorised access b) Reduced outages / failures / data loss, faster system recovery	Quantify potential penalties, financial losses when business can't operate, Cost avoidance to fix / remedy issues
6) Adoption / Engagement	a) Number of sites deployed, number of users / account sign up b) Number of transactions / services purchased / downloads	N. A.
7) Systems Decommissioning & Cost Savings	Decommissioning of the existing system(s) or application(s) that would be replaced once the project is implemented	Delta cost difference of the maintenance costs between legacy systems and new systems will be the cost savings/avoidances

2) Benefits & KPIs:

Guidelines to coming up with Project KPIs

- Consider **short term** and **long term outcomes** of the project – you may phase out the targets across the project implementation
- KPIs should be "**SMART**" –
  - **S**pecific (what is the metric to be measured e.g. reducing waiting time or manpower costs, increasing number of user transactions)
  - **M**easurable (quantify the target in % or actual numbers e.g. reducing 50% of waiting time)
  - **A**chievable, **R**ealistic (use existing information i.e. current baseline /current performance to establish the new target e.g. reducing 50% of waiting time from current performance of 10min per patient queue)
  - **T**ime-bound (within the period of the project e.g. By FY22 to achieve 50% reduction of waiting time)

1 Improve Business Case Review

2) Benefits & KPIs: Examples / Good Samples

Outcome Category	Desired Outcomes	Current Baseline (Please indicate how baseline measure is derived, as well as current cost for activity / process)	Proposed Targets (Please indicate how targets and the timeframe (i.e. year, quarter or month) to when the target would be achieved)	Financial Implications (i.e. potential / estimated cost savings / avoidance, to time bound the figures annually or across 'X' years)
Manpower Productivity	Reduction in time on tracking of inventory	a) 1000 hours (in total) for 5 inventory staff to perform stock counts and replenish stocks per month b) 50 hours to manually track stock expiry per month • Current Manpower cost for these activities per year = 1050 hours x $15 (per hr inventory staff rate) x 12 months = $189, 000	a) In first 2 years of implementation (by FY19 Q4), **to reduce 60% time or 600 hours (in total) per month** with RTLS stock tracing & bin top up concept. From 3rd year FY20 Q1 onwards, **to reduce 95% time or 950 hours (in total) per month** b) Upon implementation (FY18 Q4), to reduced 98% time or 49 hours per month to track expired stocks	Potential cost savings in manpower per annum = 999 hours x $15 (per hr inventory staff rate) x 12 mths = $179,820 Potential cost savings in manpower across first 3 years - $413,460 • Year 1 – 649 hours x $15 x 12 months = $116,820 • Year 2 – same as Year 1 • Year 3 – 999 hours x $15 x 12 mths = $179,820
P D				d more timely.

Good Sample where the KPI is

- **S**pecific on manpower time savings
- **M**easurable on 60% of reduction per month
- **A**chievable, **R**ealistic where it phase out the improvement targets from 60% to 95% across 3 years of implementation FY19 to FY20
- **T**imebound on clear timeframe FY19 to F20 to measure targets

1 Improve Business Case Review

2) Benefits & KPIs: Examples / Good Samples

Define or Estimate the 'monetary' values (e.g. ROI / cost savings) for all of the benefits/KPIs wherever possible, across the entire project lifecycle

Outcome Category	Desired Outcomes	Current Baseline (Please indicate how baseline measure is derived, as well as current cost for activity / process)	Proposed Targets (Please indicate how targets and the timeframe (i.e. year, quarter or month) to when the target would be achieved)	Financial Implications (i.e. potential / estimated cost savings / avoidance, to time bound the figures annually or across 'X' years)
Manpower Productivity	Reduction in time on tracking of inventory	a) 1000 hours (in total) for 5 inventory staff to perform stock counts and replenish stocks per month b) 50 h expi • Curre activi $15 (rate)	a) In first 2 years of implementation (by FY19 Q4), **to reduce 60% time or 600 hours (in total) per**	Potential cost savings in manpower per annum = 999 hours x $15 (per hr inventory staff rate) x 12 mths = $179,820 Potential cost savings in manpower across first 3 years - $413,460 • Year 1 – 649 hours x $15 x 12 months = $116,820 • Year 2 – same as Year 1 • Year 3 – 999 hours x $15 x 12 mths = $179,820

Define or Estimate the 'monetary' values (e.g. ROI / cost savings) for the KPI

- Annual Manpower Cost Savings = Reduced man-hours / FTE hours * FTE salary rates * 12 mths)

Prime/Direct Impact of Proposed Targets on Beneficiaries

Deliver a more seamless and hassle-free patient experience through IT automation. Patients are served more timely.

MINISTRY OF HEALTH
SINGAPORE

Thank You!