FIJI PORTS ICT

INFORMATION SYSTEMS STRATEGIC PLAN

2019 - 2024

RAJNIEL LAL
FPCL

Contents

ABSTRACT

Fiji Ports Corporation Limited (FPCL) aims to be the maritime gateway in the Pacific region through facilitating waterborne transport, trade, and commerce. FPCL operates the major port facilities in Suva and Lautoka and the secondary port of Levuka and oversees the operations and International Port Facility Security requirements of Vuda, Malau, Rotuma and Wairiki.

The 5 Year Strategic Plan (2019-2023) is a cornerstone of the overall alignment of the Port to an increasingly dynamic and competitive business environment. Through the Strategic Plan, the Port will meet key challenges and leverage opportunities to achieve its goals. The Plan addresses the physical, operational, economic, environmental, and recreational requirements of the company. It forms the basis for strategic policy for effective resource utilization and efficient service delivery.

Numerous challenges were identified as well as significant opportunities for FPCL and its affiliates for the short and medium term, and that these required consideration of inputs which will provide guidance for the development of strategic initiatives and goals, as well as linked action plans and KPIs.

As part of the 5 year strategic plan, technology has been identified as an strategic goal which is mentioned as **Strategic Goal 6 – Safety, Security and Technology -** "Adopt Smart Port initiatives to achieve best practice in International Port Security and safe working environment". This goal identifies for the organisation to have an overall Information Systems Strategic Plan (ISSP), which would envision the path for achieving the strategic goal.

IMPORTANCE OF ISSP

Information systems have assumed an increasingly strategic role in organizations. It helps organizations to conduct their daily activities, functions properly (accurately and timely manner with the help of software) , and supports decision making. Information systems can be regarded as a strategic resource in an organization. The opportunities created can be classified in 4 areas:

- To gain competitive advantage.
- To improve productivity and performance.
- To enable new ways of managing and organizing.
- To develop new businesses.

This is not to say, however, that all strategic systems provide an organization with an advantage. As a system can be strategically important for different reasons – it can be a source of competitive advantage or it can be a strategic necessity. All strategic systems become strategic necessities as in an evolutionary theory of strategic development.

In an organization, ISSP can bring information systems users and information systems professionals together and establish a mutual understanding of the value of information systems and the problems associated with them. This can help organizations to develop priorities for information systems development by ranking such systems in terms of their efficiency, effectiveness, and strategic value.

Having a ISSP also ensures that whenever new systems are build they can communicate or interface properly with pre-existing systems. It ensures that the information systems infrastructure is consistent with the strategic vision of the organization. The success, and even survival, of an organization in today's markets is largely dependent upon the development and implementation of a coherent and innovative strategic information systems plan.

STRATERGIC PRIORITIES

The vision for ICT department is to be the business enabler for FPCL on the digital frontier. This would help FPCL achieve greater heights in the maritime industry.

FPCL ICT team has developed a set of strategic priorities and formulated these into 8 **Key Challenges**.

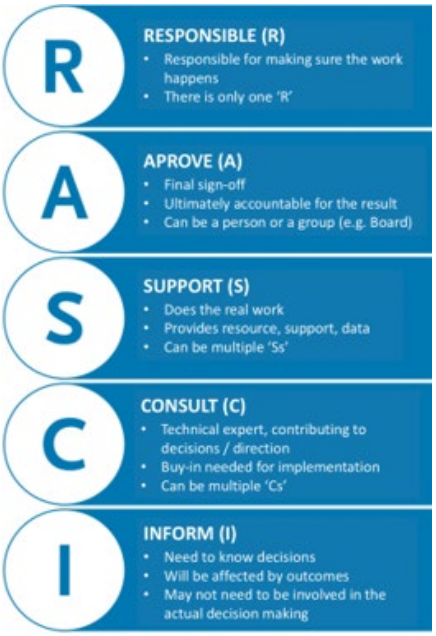
The ICT Manager with the guidance of the FPCL Project Management Office (PMO) will complete these through rolling action plans, starting Quarter 4 of 2019.

Throughout the duration of the Strategic Plan, FPCL ICT team will channel its efforts and attention on the following thematic areas:

1.	Enhanced IT Border Security Infrastructure. Monitoring and Response
2.	Incorporate Business Continuity of Information System with Organisational Continuity plan
3.	Organisational wide IT Policies and Procedures
4.	Unification of System
5.	Professional services automation systems and process
6.	Unification of Systems
7.	Learning/Knowledge Management
8.	International Best Practices Certification

To ensure clear reporting structures, the **RASCI matrix** is being utilized for defining the roles and to determine the tasks, responsibilities and authority of the development group members.

The letters R, A, S, C and I each constitute a combination of a name/role and result/process/task.



R (responsible) - those who do the work and are responsible for the result. They report directly to the person accountable

A (accountable) - the one ultimately responsible and authorised to hold accountable those responsible

S (supportive) - those who provide support and assistance to those responsible for the result.

C (consulted) - those whose opinions are sought before decisions or steps are taken to achieve the result (two-way communication).

I (informed) - those who are informed after decisions have been made or results have been achieved. They have no influence over the result.

The benefits of using RACSI are

- Determines ownership of a particular project or task
- Promotes teamwork by clarifying roles and responsibilities
- Improves communication by getting the right groups involved
- Increases efficiency by eliminating duplication of effort
- Reduces misunderstanding between and across employees and key stakeholder groups
- Improves decision-making by ensuring the correct people are involved

Throughout the delivery of the Challenges and at the Program level, Managers will ensure that transparent individual **S.M.A.R.T activities** are created that deliver on the promise. S.M.A.R.T. is an acronym that is used to guide the development of measurable goals. Each objective should be **S**pecific, **M**easurable, **A**chievable, **R**elevant and **T**ime-bound.

Specific	Details exactly what needs to be done and is clear and concise
Measurable	Quantifiable achievement or progress that can be measured with set values
Achievable	Objective is accepted by those responsible and must be attainable and realistic
Relevant	Objective is possible to attain and must be relevant to the overall purpose
Time-bound	Time period for achievements must be clearly stated

Outcomes	Desired Outputs	Measures	Related Activities	RASCI	Start	Finish	Potential Risks
1. Enhanced IT Border Security infrastructure, monitoring and response	• Reduce attack surface area • Security reporting • Strengthened Security at Internet gateway • Defence in Depth	• ICT Vulnerability Assessment • Penetration Testings • Reporting • Monitoring	1.1 Assess current border security 1.2 Identify Security Provider 1.3 Patch Management 1.4 Identify and implement current best industry security tools 1.5 Periodic reviews 1.6 Formulation of security & change management committee	*R: MICT* *A: CFO* *S: ICT Team* *C: External vendors* *I: CEO*	Q4 2019	Q3 2020	• Breach of system and data integrity • Cost of Security Upgrades • Lack of trained personnel internally • Unauthorized changes Indicative Budget: $105,000.00
2. Incorporate Business Continuity of Information System with Organisational Continuity plan	• Build resiliency of Information systems • Availability and accessibility of system during disasters • Minimizing Downtime service disruptions • Ensuring recovery and restoration • Increase Confidence in Systems	• High availability and fail over of critical infrastructure • Fail-over to DR site with minimum service outages • Data Restoration test • Identification of RPO &RTO for systems	2.1 Identify business critical infrastructure 2.2 Assess and implement High Availability for infrastructure 2.3 Network Upgrade 2.4 Restore backup on cloud infrastructure 2.5 Test accessibility of restored servers & services from user 2.6 Reverse restore to Data Centre and test for data integrity 2.7 Collaborate with business units and develop BCP and restoration test	*R: MICT* *A: CFO* *S: ICT Team* *C: External vendors* *I: CEO*	Q2 2020	Q2 2021	• Unavailability of system • Loss of business • Uncoordinated process for recovery Indicative Budget: $68,000.00
3. Organisation wide ICT policies and procedures	• Electronic versions of polices • Availability and accessibility of policies • Informed workforce • Addressing security and vulnerability issues	• HR and Executive management endorsement of policies • Policy Enforcement	3.1 Periodically updating ICT policies 3.2 Ensuring policies are available on relevant portals 3.3 Ensure policy covers all aspects of ICT controls 3.4 Enforce policy via system	*R: MICT* *A: CFO* *S: ICT Team* *C: External vendors* *I: CEO*	Q2 2020	Q1 2021	• Misinterpretation of policies • Staff compliance • System breaches Indicative Budget: $60,000.00

Outcomes	Desired Outputs	Measures	Related Activities	RASCI	Start	Finish	Potential Risks
4. Professional services automation systems and processes	• Better revenue capture • Better resources planning • Faster process delivery times • Visibility of data • Knowledge creation via transformation data into information and utilization of knowledge for decision making. • Improved accounting/ Financial management system • Digital approval process	• HR system and biometric system integration • Stock reporting with ease • Faster LR processing and PO issuance • Effective tracking of Vessels • Effective capturing of revenue and expenses	4.1 Identify requirements and develop/source relevant applications 4.2 Consult with Navision Vendor 4.3 Process review and realignment 4.4 Vessel Traffic Management implementation 4.5 Digitalization of applications for berthing and port management 4.6 Security Integration	*R: MICT* *A: CFO* *S: ICT Team* *C: External vendors* *I: CEO*	Q4 2019	Q4 2021	• System downtime • Inefficient utilization of resources • Information silos • Loss of business Indicative Budget: $100,000.00
5. Quality, Integrity and meaningful representation of data	• Clean data in the system • Reduce data anomalies • Dependable sources of data • Informed and accurate decisions • Dashboard reporting	• Error free reporting • On Demand reporting • Customized reporting • Increased turnaround time for reporting • Accurate representation of the business via data insights	5.1 Periodic internal audit of Data Sources 5.2 Data Cleansing 5.3 Implement Dashboard reporting	*R: MICT* *A: CFO* *S: ICT Team* *C: External vendors* *I: CEO*	Q2 2020	Q4 2020	• Audit risk assessment is incomplete or inaccurate • Inaccurate representation of the business Indicative Budget: $15,000.00

Outcomes	Desired Outputs	Measures	Related Activities	RASCI	Start	Finish	Potential Risks
6. Unification of Systems	• Full integration of applications • All FPCL offices to be interconnected • Anywhere anytime access to FPCL ICT services • API identification for systems	• Collaboration between HQ and other offices • Coordination of workforce whilst in transit	6.1 Connect HQ with all Offices 6.2 Identify relevant technology for unification of systems 6.3 Implement identified technology such as API's	*R: MICT* *A: CFO* *S: ICT Team* *C: External vendors* *I: CEO*	Q4 2019	Q2 2021	• Data theft due to lost or compromised machine • Systems breach Indicative Budget: $45,000.00
7. Learning/ Knowledge Management System	• Learning platform for staff • Continuous staff development	• Staff development trend during appraisals • Internal certifications	7.1 Identify requirements and develop/source relevant applications 7.2 Implementation of Learning Infrastructure 7.3 Develop Course Content 7.4 User training guides, manual and videos	*R: MICT* *A: CFO* *S: ICT Team* *C: External vendors* *I: CEO*	Q3 2020	Q4 2021	• Retention of knowledge • Lack of trained personnel internally Indicative Budget: $50,000.00
8. International Best Practice Certifications	• International standard compliant accreditation / certification • Streamlined processes • Industry recognition	• Certificate of compliance (staged) • Attaining business excellence awards • ISO 20000 – Service Management • ISO 27001 – Information Security Management • ISO 22301 – Business Continuity	8.1 Identification of standards and compliance testing authority 8.2 Review and documentation of internal processes. 8.3 Alignment of internal processes to identified standards 8.4 Compliance testing by authority	*R: MICT* *A: CFO* *S: ICT Team* *C: External vendors* *I: CEO*	Q1 2022	Q4 2023	• Failure to comply with industry standards Indicative Budget: $60,000.00

2019

Fourth Quarter

- ICT Vulnerability Assessment
- VTMS Project Initiation
- Remote Site Connectivity

2020

First Quarter

- Patch Management
- Periodic review of network and security policies
- VTMS Project
- Digital Berthing Application
- Remote Site Connectivity

Second Quarter

- Review of Office 365 access policies
- Implementation of monitoring and reporting for network and system issues
- VTMS Project
- Identify Business critical Infrastructure
- ICT Policy review
- Data Cleansing
- Audit of Data Sources
- Identify and implement relevant industry security tools

Third Quarter

- Formulation of security & change management committee
- Assess and implement High Availability for infrastructure
- Ensuring policies are available on relevant portals
- Identify requirements and develop/source relevant applications
- Dashboard and customized reporting
- Learning Management System – Requirements gathering

Forth Quarter

- Upgrade backup application and test restoration of backup on cloud infrastructure
- Consultation with Navision Vendor
- Ensuring policies are available on relevant portals
- Identify & implement relevant technology for unification of systems
- Dashboard and customized reporting
- API identification & integration
- Policy enforcement

2021

First Quarter	Second Quarter	Third Quarter	Forth Quarter
Network Backbone Upgrade	Test accessibility of restored servers & services from user	Test accessibility of restored servers & services from user	Upgrade backup application and test restoration of backup on cloud infrastructure
Policy enforcement	Policy enforcement	User training guides, manual and videos	User training guides, manual and videos
Smart Security	Process review and realignment	Process review and realignment	Process review and realignment
Implementation of Learning Infrastructure	Implementation of Learning Infrastructure		Scope ISO standards
	Develop course contents		Reverse restore to Data Centre and test for data integrity

2022

First Quarter	Second Quarter	Third Quarter	Forth Quarter
ISO 20000 – Service Management	ISO 20000 – Service Management	ISO 20000 – Service Management	ISO 20000 – Service Management
ISO 27001 – Information Security Management	ISO 27001 – Information Security Management	ISO 27001 – Information Security Management	ISO 27001 – Information Security Management
ISO 22301 – Business Continuity	ISO 22301 – Business Continuity	ISO 22301 – Business Continuity	ISO 22301 – Business Continuity
Collaborate with business units and develop BCP and restoration test	Collaborate with business units and develop BCP and restoration test		
	Penetration Testing		

PROGRESS REPORT

The following is the status update for the projects that had been embarked on

	Project Name	% Complete	July Status	Current Status
3.1	Office365 Migration	100	All user mailboxes (emails) have been moved from inhouse Exchange server (v2003) to Office365. With O365, FPCL has a more resilient communications platform. FPCL now has an increased Integrity and availability of emails.	Email flow has been stable since the migration. User awareness needs to be created for other additional features that can help in business communication.
	Project Name	% Complete	July Status	Current Status
3.2	Client End Security Application	100	Malwarebytes security appliance has been installed on all domain machines to protect against virus infections. ICT team has access to a dashboard that shows protected machines.	Protection is in place for malware and antiviruses.
	Project Name	% Complete	July Status	Current Status
3.3	Internet Bandwidth Upgrade	100	Bandwidth across all FPCL sites including HQ has been upgraded to cater for other projects like Office365 and video conferencing. Hardware required for upgrade of other FPCL sites have been procured and received by the ICT team. These installations will be happening in July 2019.	Currently no issues have been encountered in regards to the speed and accessibility of cloud services. Review of the same would be conducted by the end of the year.
	Project Name	% Complete	July Status	Current Status
3.4	ICT Helpdesk Solution	100	A comprehensive ICT helpdesk solution has been implemented which helps the ICT team to document and update tasks. Furthermore, this incident management platform also has features such as asset management, contracts management, problem and change management.	Tickets are being logged on the helpdesk system and will be useful to measure turnaround time for issues.

	Project Name	% Complete	July Status	Current Status
3.5	Firewall Replacement	100	FPCL firewall has been replaced. The new firewall is a next gen device with advanced application filtering. Other features include VPN, traffic shaping, and reporting. The new device is scalable and sufficient for the near future.	Further enhancements to the border security is being scoped to increase threat and user visibility across the network.
	Project Name	% Complete	July Status	Current Status
3.6	Offices, Meeting Rooms cable Tidy-up	80	Cabling at most of FPCL sites have been completed. The server room comms rack and security office network racks are left to be tidied up. This should be completed by mid-July.	This is on hold for server room as there is an upgrade that is scoped for the server room. Other sites to be tidied up by end of October.
	Project Name	% Complete	July Status	Current Status
3.7	Corporate Wi-Fi Blanket	55	A comprehensive solution has been designed for the complete wireless connectivity coverage for FPCL HQ and other sites. The access points for the corporate Wi-Fi blanket project has arrived. ICT team has configured a test device and is testing out the deployment. Once the configured device is finetuned, the settings will be cloned onto other devices and deployed across the organization. The FPCL domain upgrade project is a prerequisite to this project. The new domain would allow harnessing the complete functionality of the wireless controllers for confidentiality and availability on a wireless platform. ETA on this is end of July.	Equipment have been delivered and should be rolling out installation by OCT. Project was delayed due to the prerequisite not being completed which was the domain migration. Domain migration has been planned to be completed by end of OCT.

	Project Name	% Complete	July Status	Current Status
3.8	Domain Upgrade	40	A new domain controller has been commissioned and Office365 along with few other services are running on the new DC. The upgrade of Port Manager, Dynamics Nav, SharePoint and migration of file share will enable the final phase of domain migration. Upgrade and migration of these applications are in negotiation with the vendors of relevant applications.	This has been planned to competed by end of October.
	Project Name	% Complete	July Status	Current Status
3.9	Network Vulnerability Assessment	40	An assessment of the FPCL internal network has been completed by Datec Fiji Ltd. Report is pending and FPCL ICT team is discussing with Datec for the same. The exercise is the first part of a two-part exercise. The second part of the assessment will be a black box penetration testing of our network from outside. The vendor or consultant will not be provided with any information about the network but in agreement and in conjunction with FPCL ICT team, they will try to access to the network from external means. Once that report is finalised and submitted, FPCL ICT team will work on rectifying the identified issues. This will help us reduce our cyber threat footprint and further secure our network from structured threats.	Datec is yet to produce the report for the assessment. Penetration testing will be put on hold until the report is tabled and remedial actions are taken.

	Project Name	% Complete	July Status	Current Status
3.10	Access Control and Time attendance	40	The project has been significantly delayed due to the need of automation, however, FPCL ICT has managed to find a solution to the integration needs and also secured vendors to deliver this project. Other stakeholders within FPCL are reviewing the details of the project and will be out for procurement shortly after.	Work is in progress. Vendor has been identified and project is underway. Expected completion by end of October
	Project Name	% Complete	July Status	Current Status
3.11	ICT Office Space Restructure	100	The project is in its final stages. The renovation of the office structure has completed. Office is being tidied up and structured cabling is underway	This has been completed
	Project Name	% Complete	July Status	Current status
3.12	Hardware Refresh	0 (On Hold)	This project will need extensive planning and assessments to be conducted. Most of our ICT assets are near obsolete. A preliminary study will be conducted to establish the requirements and then mapped to available technology that will be cost effective, yet efficient. With the introduction of high- tech applications like the VTMS, we will need to plan for this project more comprehensively.	This will be carried out progressively with the plan of deploying 10 machines in a quarter over the year. This will ensure that replacements are done periodically and will not have a major expenditure in a single year.

STRATEGIC BREAKDOWN

The following provides the breakdown of each strategy mentioned in the above document.

Enhanced IT Border Security infrastructure, monitoring and response

The strategy focuses on improving the security posture for FPCL as a whole. The outcome through this strategy is to provide comfort and ensure that FPCL infrastructure both physical and logical are secured. This will help achieve the following:

- ***Reduce attack surface area***
- ***Security reporting***
- ***Strengthened Security at Internet gateway***
- ***Defense in depth***

With majority of the **services now being digital** and majority of daily tasks carried out via **computerized systems**, **measures and controls need** to be in place to ensure that **Confidentiality, Integrity and Availability of Data, Information and System is maintained**. This strategy also caters for incident response should there be breaches detected and co-ordinate action plan to minimize and contain the breach.

To achieve this strategic goal the following systems, processes and measures need to be implemented:

1. **ICT Vulnerability Assessment** – this would give a clear picture as to the controls that need to be in place. The scope for this will encompass network, systems and applications.
   Start – Q4, 2019; Finish – Q1, 2020

2. **Patch management** – this is to ensure that servers and user machines are patched with the latest security patches to avoid any vulnerabilities being exploited
   Start – Q1, 2020; Finish Q1, 2020

3. **Review O365 access polices** – Office 365 is a great tool for productivity, however, security policies need to be defined and implemented to ensure that corporate data is secure and only accessible via trusted sources.
   Start – Q2, 2020; Finish Q2, 2020

4. **Monitoring & Reporting** – this will provide respective shareholders an insight of the security posture. It would also provide actionable items to ensure that security is maintained.
   Start – Q2, 2020; Finish Q2, 2020

5. **Identify and implement current best industry security tools** – implementation of this will help the ICT team as well as the organization as a whole to have visibility of the network, security, system and application infrastructure.
   Start – Q2, 2020; Finish Q4, 2020

6. **Periodic reviews** – this will be done to ensure that industry best practices and polices are followed. Network and system security is ever evolving with change of technology and people. As such periodic review will ensure that FPCL is protected.
   Start – Q1, 2020; Finish Q4, 2020

7. **Penetration Testing** – this to be carried out at least annually. Carrying out this testing will provide comfort to the management and the stakeholders that the corporate system and network is secure and reliable.
   Start – Q2, 2021; Finish Q2, 2021

8. **Formulation of security & change management committee** – this is to ensure that changes made to network, security and system is communicated to senior management and are made aware of the impact of the same. This also ensures transparency and control on the changes made to infrastructure.
   Start – Q3, 2020; Finish Q3, 2020

To achieve this goal, an indicative budget of **$105,000.00** is requested which will cater for the hardware, tools and application required to fulfil the goal. The budget spread is over a period of 2 years with majority spend on

- ***ICT Vulnerability Assessment - $30,000, Year 1***
- ***Patch Management Software - $10,000, Year 1***
- ***Security, Incident and Event Management tool - $20,000, Year 1***
- ***Network Monitoring Tool - $15,000, Year 1***
- ***Penetration Testing - $30,000, Year 2***

Incorporate Business Continuity of Information System with Organisational Continuity plan

The strategy focuses on implementing and improving the **availability and continuity** of FPCL's Information and Communications systems. The continuity plan will be in-sync with the overall Business continuity of the organization. This will help achieve the following:

- ***Build resiliency of Information systems***
- ***Availability and accessibility of system during disasters***
- ***Minimizing Downtime service disruptions***
- ***Ensuring recovery and restoration***
- ***Increase Confidence in Systems***

At present FPCL utilizes majority of the IT infrastructure to carry out its day to day task. With such dependency placed on the Information system, FPCL should have a **comfort on the Confidentiality, Integrity and Availability of system and its information**. To achieve this strategic goal, the following activities need to be carried out:

1. **Identify business critical infrastructure** – this will help identify business dependent systems and process. More focus will be given to high priority infrastructure. This exercise will also help identify the response plan should the system go down. A measure which will be attached to this will be the Recovery Point and Recovery Time Objective (RPO & RTO).
   Start – Q1, 2020; Finish Q1, 2020

2. **Assess and implement High Availability for infrastructure** – currently systems and network has a single point failure which include the firewall, network switches and servers. The goal is to achieve resiliency and availability by implementing N+1 where by the system is able to function in an event of hardware or software failure.
   Start – Q3, 2020; Finish Q1, 2021

3. **Network backbone upgrade** – redesign and upgrade the current uplink from the different levels to Server room to handle more network traffic and to ensure resiliency by implementing multiple pair cables. Upgrade of remote site networks will also done to ensure coverage for all sites.
   Start – Q1, 2021; Finish Q1, 2021

4. **Upgrade backup application and test restoration of backup on cloud infrastructure** – currently all backups are stored off site on Vodafone's cloud infrastructure. Restoration are to be done to test and ensure integrity of the data is intact.
   Start – Q4, 2020; Finish Q4, 2020

5. **Test accessibility of restored servers & services from user** – this is to achieve the full restoration of services from the cloud service and ensure that end users and systems can access the restored services. This will ensure that the systems are available and will provide comfort for business continuity should there be a catastrophic failure of FPCL IT infrastructure.
   Start – Q2, 2021; Finish Q3, 2021

6. **Reverse restore to Data Centre and test for data integrity** – this is to ensure that once the systems have been restored with-in FPCL IT infrastructure, data can be accurately and successfully restored back.
   Start – Q4, 2021; Finish Q4, 2021

7. **Collaborate with business units and develop BCP and restoration test** – one of the most important step for having a successful continuity plan is to ensure that each department and individual are aware of the process and the role that they paly for a more coordinated recovery process.
   Start – Q1, 2022; Finish Q2, 2022

This strategic goal is to ensure that there is minimum business loss during disasters and that FPCL has a resilient infrastructure. To achieve this goal, an indicative budget of **$68,000.00** is requested which will cater for the hardware, tools and application required to fulfil the goal. The budget spread is over a period of 2 years with majority spend on

- ***High Availability for Server & Network devices at HQ - $40,000, Year 1***
- ***Network Backbone upgrade - $8,000, Year 2***
- ***Backup software upgrade - $20,000, Year 1***

Organisation wide ICT policies and procedures

The strategy focuses on **improving respective ICT policies and creating awareness** for the same. The outcome of this strategy is to review the current policy and align the same according to industry best practise. Awareness of policies and procedures are to be achieved to ensure that FPCL has informed staff work force and are in compliance to any mandatory regulations. The following will be the subsequent benefit:

- ***Electronic versions of polices***
- ***Availability and accessibility of policies***
- ***Informed workforce***
- ***Addressing security and vulnerability issues***
- ***System and network policy enforcement***

Any business to prosper and achieve maximum returns, needs to **evolve both functionally and technologically**. To cater for this, business processes and policies need to be reviewed and ICT is no exception.

Currently, awareness of policies and procedures is limited and revision of changes are not properly carried out. This creates an environment where awareness of policies and procedures are not communicated properly. With the turnover of staff and changes to the business processes, the following task need to be conducted:

1. **Periodically updating ICT policies** – this will ensure that policy reflects the changes in the Information and Technology arena captured. This would also ensure that controls and measures are periodically reviewed to ensure maximum effectiveness.
   Start – Q2, 2020; Finish Q3, 2020

2. **Ensuring policies are available on relevant portals** – this will ensure that relevant documents and information is readily available to staff for their consumption. This could also be used for refresher on the policies and procedure. Look at tools that can be implemented for ease of access to users. E.g. SharePoint in conjunction with LiveTiles
   Start – Q3, 2020; Finish Q4, 2020

3. **Ensure policy covers all aspects of ICT controls** – this is ensure that the ICT policies covers and enforces security and control for the day to day system operations. Policy should include but not limited to capturing Incident response, Change Management, Physical Security Access, Information Security and any other policies relevant to ICT.
   Start – Q2, 2020; Finish Q3, 2020

4. **Policy Enforcement** – Implement policy enforcement via tools such as application control system and mobile device management.
   Start – Q4, 2020; Finish Q2, 2021

The outcome of this strategic goal is to ensure that FPCL has relevant and current policies to ensure well informed work force, avoid system breaches and maintain relevant compliance. To achieve this goal, an indicative budget of **$60,000.00** is requested which will cater for the consultation, training and staffing required to fulfil the goal.

The budget spread is over a period of 2 years with majority spend on

- ***Policy portal (SharePoint integration with LiveTile) - $20,000, Year 1***
- ***Policy enforcement tool - $20,000, Year 2***
- ***Mobile Device Management - $20,000, Year 1***

Professional services automation systems and processes

The strategy focuses on the **automation of systems and processes via integration** of existing systems to **increase efficiency and value add to services**. This process of achieving automation via integration would ensure that data is collected accurately, reducing data anomalies and improving decision making based on information derived by the data with reducing information silos. Following will be the benefits of the strategy:

- ***Better revenue capture***
- ***Better resources planning***
- ***Faster process delivery times***
- ***Visibility of data***
- ***Knowledge creation via transformation data into information and utilization of knowledge for decision making.***
- ***Improved accounting/ Financial management system***
- ***Digital approval process***

At this stage, FPCL has **silos of information** which are not systematically linked and requires manual intervention for data transformation to produce relevant reports and information. This offcourse leads to anomalies in information and uncertainty of reports produced. The following systems and activities have been identified to achieve the strategic goal:

1. **Identify requirements and develop/source relevant applications** – outcome of this activity will produce a list of systems that FPCL currently utilizes and relevant expectation of system integration.
   Start – Q3, 2020; Finish Q3, 2020

2. **Consultation with Navision Vendor** – outcome is to understand the features and requirements for implementing additional modules of Navision to extensively use it to its full potential ERP system. This would also ensure data anomalies are reduced and data flow and visibility is increased. Since FPCL has invested time and resource, both personnel and financial, it would beneficial to explore feature and functionality instead of replacing the same.
   Start – Q4, 2020; Finish Q4, 2020

3. **Process review and realignment** – with system integration and gradual introduction of process automation, current processes will need to be reviewed and realigned to ensure effectiveness and process optimization.
   Start – Q2, 2021; Finish Q4, 2021

4. **Vessel Traffic Management** – system to be implemented for effective management of Vessel traffic within the port territory. Implementation of the system will ensure effective monitoring and tracking of vessel movement, identifying security breaches and risk and ensure vessels are charged effectively and correctly for the services rendered. Integration activity will include the relative systems to receive data for processing e.g. Navision for finance processing.
   Start – Q1, 2020; Finish Q4, 2020

5. **Digital Berthing Application** – this activity will be carried out to automate the process for generating, submitting and processing berthing application. The outcome would reduce the paper foot print associated with individual application, reduce revenue leakage due to manual processing and controls and increase efficiency of services provided.
   Start – Q4, 2019; Finish Q1, 2020

6. **Security Integration** – Integration of security devices such as CCTV, access controls and alarm systems within a centralized platform to create a holistic view of security for all Wharfs. This would also set the platform for smart security and monitoring system for ports and harbour. *Start – Q1, 2021; Finish Q2, 2021*

The holistic goal for the strategy to raise efficiency, reduce data anomalies, reduce manual intervention and increase data flow processing with data visibility. To achieve this goal, an indicative budget of **$100,000.00** is requested which will cater for the consultation, acquisition, development and training required to fulfil the goal.

The budget spread is over a period of 2 years with majority spend on

- ***Application Development - $30,000, Year 1***
- ***Navision consultation - $10,000, Year 1***
- ***Digital Berthing Application - $30,000***
- ***Smart Security - $30,000, Year 2***

Quality, Integrity and meaningful representation of data

The focus of this strategy is to gain **deeper insight and representation of data via analytics** to produce trends and other key information which would be beneficial to the business to make informed decisions.

It is widely known that data is a valuable asset for any organization and can be used for the benefit for the organization to prosper. To achieve this, data should be reliable and accurate. The following is benefits is associated with the above strategy:

- ***Clean data in the system***
- ***Reduce data anomalies***
- ***Dependable sources of data***
- ***Informed and accurate decisions***
- ***Accurate representation of the business via data insights***
- ***Dashboard reporting***

A challenge that FPCL faces currently is the lack of insight provided by data analysis. This is due to the multiple sources of data input and anomalies associated with various data inputs. To ensure that the data is dependable and accurate, the following activities are to be carried out:

1. **Data Cleansing** – a general cleansing of data to be carried out to ensure that data sources have accurate data stored which can be extracted to provide accurate information. This exercise would also identify any additional data to be captured for reporting purpose.
   Start – Q2, 2020; Finish Q2, 2020

2. **Audit of Data Sources** – audit would be carried out in regards to the controls and measures that are in place to ensure that data is kept confidential, integrity of data is maintained and is available to authorized personal. This would significantly reduce data anomalies and increase information accuracy.
   Start – Q2, 2020; Finish Q2, 2020

3. **Dashboard and customized reporting** – implementation of reporting systems to offer dashboard reporting which can provide both holistic and granular view of the information. This would also allow for reports to be customized as required by various department and can be generated on-demand increasing the turn-around time. A sub activity for the same will be to setup a data warehouse for reporting purpose.
   Start – Q3, 2020; Finish Q4, 2020

The holistic goal for this strategy is to ensure that data is realised as an valuable asset and is processed and analysed analytically to provide in-depth information and understanding of the business position. This strategy will ensure that FPCL has accurate representation of the business growth via dashboard reporting and further understand the variables that have effect on various business objective.

To achieve the this goal, an indicative budget of **$15,000.00** is requested which will cater for the consultation, acquisition, development and training required to fulfil the goal.

The budget spend will be mainly on

- ***Dashboard reporting and Report Customization - $15,000, Year 1***

Unification of Systems

This strategy is an **extension of the Automation strategy but encompasses the unification of physical infrastructure** located at various sites. The goal of this strategy is to link each of the sites to ensure that data and information is processed real-time and is free of any anomalies. The benefits with implementing the strategy is:

- ***Full integration of applications***
- ***All FPCL offices to be interconnected***
- ***Anywhere anytime access to FPCL ICT services***
- ***Collaboration between HQ and other offices***
- ***Coordination of workforce whilst in transit***

To achieve the above mentioned benefits, the following activities are to be carried out:

1. **Connect HQ with all sites** – this is to achieve access and data processing real time. It would also ensure that support and other services can be provided ad-hoc.
   Start – Q4, 2019; Finish Q1, 2020

2. **Identify & implement relevant technology for unification of systems** – the scope for the same includes seamless unification stand-alone systems used to deliver information and communication to achieve a centralized center to dissipate information.
   Start – Q4, 2020; Finish Q1, 2021

3. **API identification & integration** – Application Programmable Interfaces (API) are feature that allows for different systems to communicate and process data based on the access levels provided. Identifying API's would help FPCL to integrate systems not only internally but also with external parties.
   Start – Q4, 2020; Finish Q2, 2021

The holistic goal for the strategy is to achieve unification of ICT systems and allow ease of access to all FPCL sites. This would allow for collaboration with users from different sites on specific business needs.

To achieve the this goal, an indicative budget of **$45,000.00** is requested which will cater for the infrastructure, acquisition, development and training required to fulfil the goal.

The budget spread is over a period of 2 years with majority spend on

- ***Network devices for remote site connectivity - $25,000, Year 1***
- ***API integration for system unification - $20,000, Year 2***

Learning/ Knowledge Management System

The outcome of this strategy is to **implement a continuous learning program** where **staff upskill** and refresh their current knowledge of the various systems, processes and polices. This would also help in identifying staff development trends and have provisions for internal certification. The benefit of having a Learning Management System (LMS) are:

- ***Ease of conducting staff trainings***
- ***Running refresher trainings***
- ***Ability to asses employees on the understanding of systems and processes***
- ***Monitor staff development***
- ***Provide Internal Certification***

With the implementation of the LMS, **trainings can be conducted on the pace of individual employee** allowing for **better management of time allocation during working hours**. The following activities are attached to the strategic goal:

1. **Requirements gathering** – this is the most important activity for as this would set and define the expectation for the LMS. Consultation will be required with HR team and individual business units as to the expectation of the system.
   Start – Q3, 2020; Finish Q3, 2020

2. **Implementation of Learning Infrastructure** – infrastructure would be required to setup a smart classroom where trainings and interactions can be recorded and uploaded to the LMS for future use and references.
   Start – Q1, 2021; Finish Q2, 2021

3. **Develop course contents** – once the system is implemented, relevant course contents needs to be developed and published on the learning system. This would include both assessed and non-assessed courses.
   Start – Q2, 2021; Finish Q2, 2021

4. **User training guides, manual and videos** – to allow for staff to refresh their knowledge on processes associated to a task. These could be document or audio/visual based.
   Start – Q3, 2021; Finish Q4, 2021

With the implementation of the Learning Management System, FPCL would be setting a trend and showcasing the ability of retaining knowledge and having a well informed and trained work force. This would also help employees to access trainings on-demand to up skill themselves.

To achieve the this goal, an indicative budget of **$50,000.00** is requested which will cater for the infrastructure, acquisition, development and training required to fulfil the goal.

The budget spend will be mainly on

- ***Learning Management System and relevant infrastructure - $50,000, Year 2***

International Best Practice Certifications

The outcome of this strategy is to **achieve international recognition** with regards to **Service Management, Information Security Management** and **Business Continuity**. Achieving these certifications would allow process streamlining and gain industry recognition.

With the successful implementation of the above 7 strategies, planning out and implementing for ISO standards would be possible as majority of task and systems would have been implemented. With this in mind, the overall achievement timeline would be 2 years and may be redefined after consultation with ISO implementers

The following ISO standards are aimed for achieving:

- **ISO 20000 – Service Management** - ISO/IEC 20000-1:2011 is a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS. The requirements include the design, transition, delivery and improvement of services to fulfil agreed service requirements. The module that is relevant to IT is the ITIL and ITSM (IT Service Management) *Start – Q1, 2022; Finish Q4, 2023*

- **ISO 27001 – Information Security Management** - The ISO/IEC 27000 family of standards helps organizations keep information assets secure. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. *Start – Q1, 2022; Finish Q4, 2023*

- **ISO 22301 – Business Continuity** - ISO 22301 has been developed by ISO/TC 223, Societal security. This technical committee develops standards for the protection of society from, and in response to, incidents, emergencies and disasters caused by intentional and unintentional human acts, natural hazards and technical failures. Its all-hazards perspective covers adaptive, proactive and reactive strategies in all phases before, during and after a disruptive incident. *Start – Q1, 2022; Finish Q4, 2023*

The holistic goal of this strategy is to ensure that FPCL practices and is complaint to industry standards and sets the trend in the industry.

To achieve the this goal, an indicative budget of **$60,000.00** is requested which will cater for the consultation, acquisition, development and training required to fulfil the goal.

The budget spend will be mainly on

- ***ISO 20000 – Service Management - $20,000, Year 3***
- ***ISO 27001 – Information Security Management - $20,000, Year 3***
- ***ISO 22301 – Business Continuity - $20,000, Year 3***

CHALLENGES AND OPPORTUNITIES

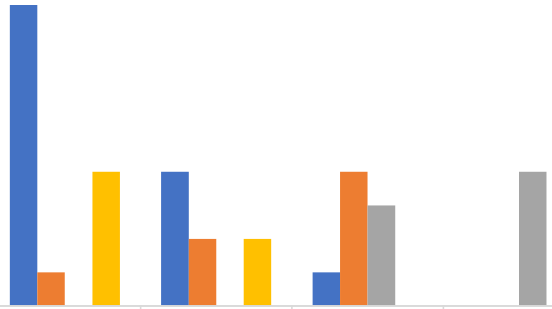
To fully achieve the above mentioned strategy, the following prerequisites needs to be in place to ensure a sound foundation is provided to implement the strategy. These are projects that need to be scoped and progressed with as soon as possible. These would also tie-in with the above strategic goals to provide more accurate results.

Project	Goal	Impact	Delivery
Health Check – user and business infrastructure	Gather accurate information on user and business infrastructure	Business disruption for system users.	November 2019
System Audit	Collate information on how systems are performing. Assess controls and measures in place to ensure system integrity	Business disruption due to unplanned outage	November 2019
Policy review	Review current IT Policy. Incorporate change management, security management, incident reporting and other critical arears.	Inadequate controls and lack of guidance	January 2020
Server Room Upgrade	Upgrade of current server room to industry standards. Installation of Fire suppressant, false flooring and environmental monitoring. UPS needs to be upgraded for the systems as well.	Business disruption due to potential hazards such as fire	March 2020
User infrastructure refresh	Periodical replacement of desktop and laptops. Replacement can be spread over each quarter.	Disruption due to outdated hardware	Jan 2020 – Dec 2020
Review staffing	Review current IT structure. Review JDD and contract terms	Staff retention	Nov 2019 – Nov 2020

INFORMATION SYSTEMS STRATERGIC PLAN (ISSP) DASHBOARD

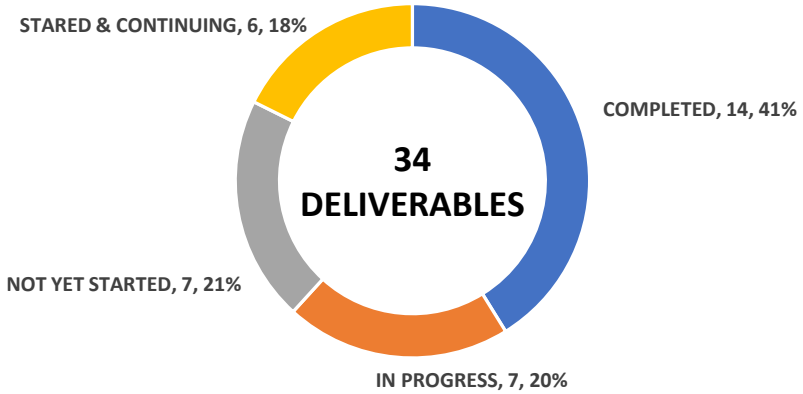
8	34	14	6	7	7
ISSP PILLARS	DELIVERABLES	COMPLETED	STARTED & CONTINUING	IN-PROGRESS	NOT YET STARTED

NO. OF DELIVERABLES DISTRIBUTED OVER THE YEAR

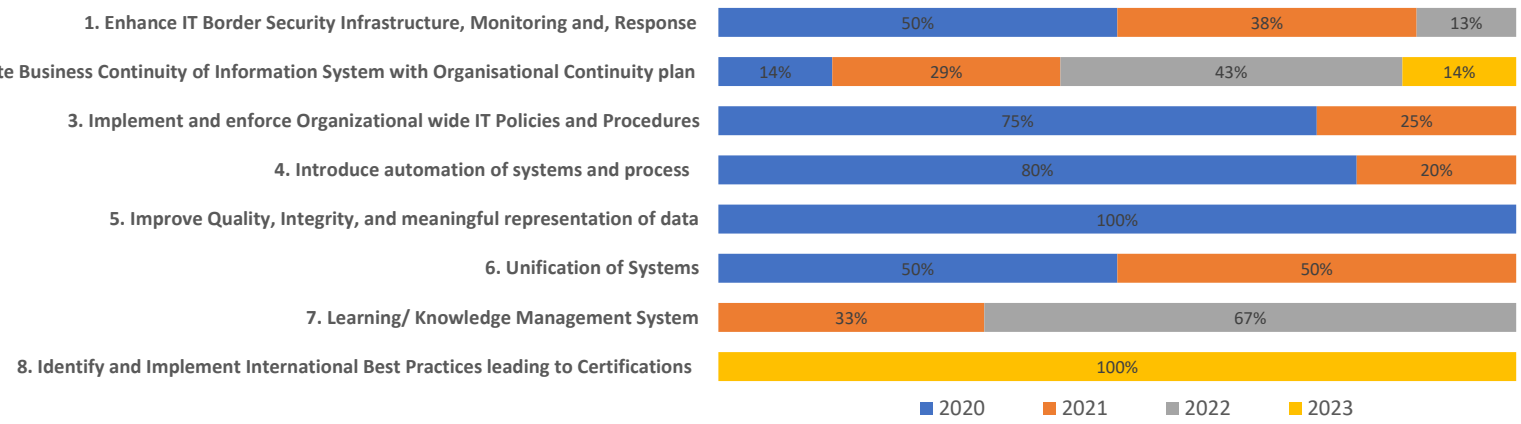


	2020	2021	2022	2023
COMPLETED	9	4	1	0
IN PROGRESS	1	2	4	0
NOT YET STARTED	0	0	3	4
STARED & CONTINUING	4	2	0	0

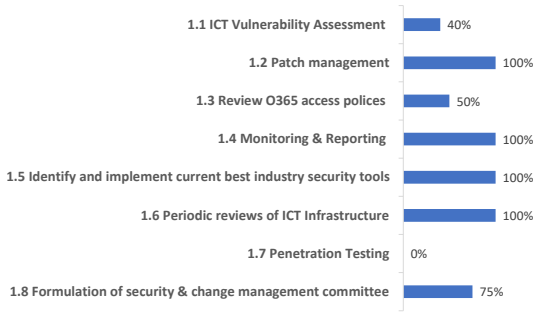
ISSP PROGRESS



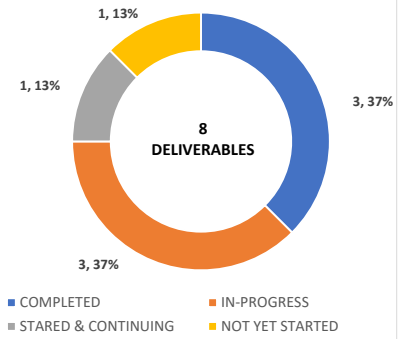
% OF DELIVERABLES PER ISSP PILLAR SPREAD OVER THE YEARS



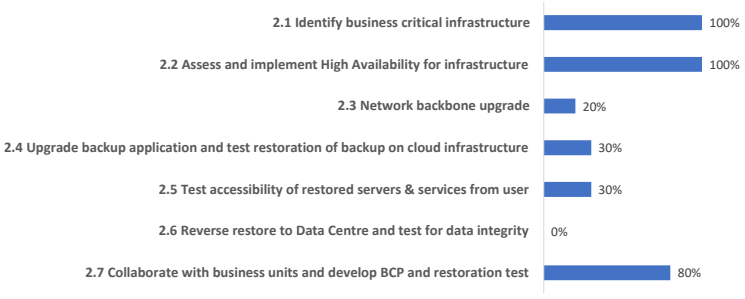
1. ENHANCE IT BORDER SECURITY INFRASTRUCTURE, MONITORING AND, RESPONSE



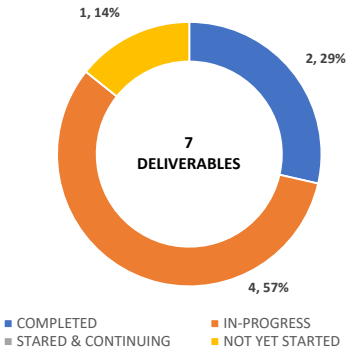
PROGRESS ON IMPLEMENTATION OF STRATEGIES (NO. & % COMPLETED)



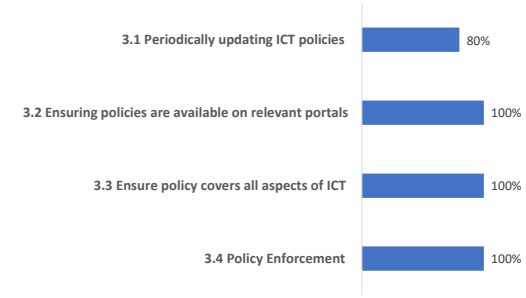
2. INCORPORATE BUSINESS CONTINUITY OF INFORMATION SYSTEM WITH ORGANISATIONAL CONTINUITY PLAN



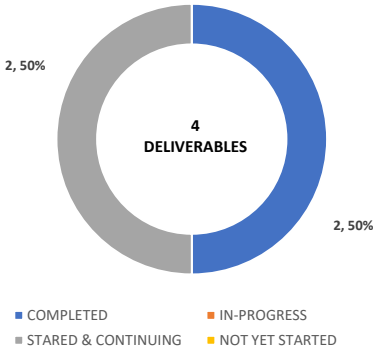
PROGRESS ON IMPLEMENTATION OF STRATEGIES (NO. & % COMPLETED)



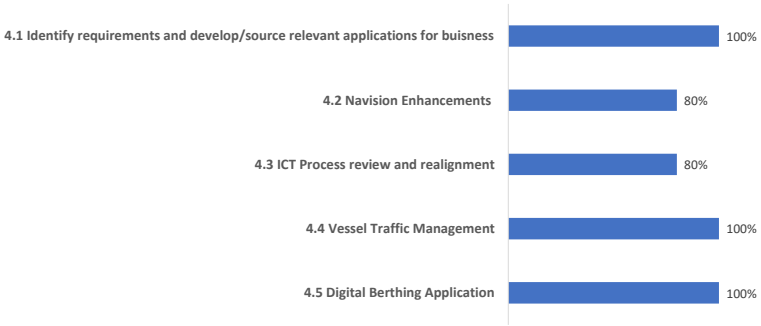
3. IMPLEMENT AND ENFORCE ORGANIZATIONAL WIDE IT POLICIES AND PROCEDURES



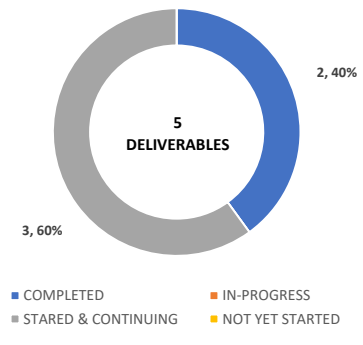
PROGRESS ON IMPLEMENTATION OF STRATEGIES (NO. & % COMPLETED)



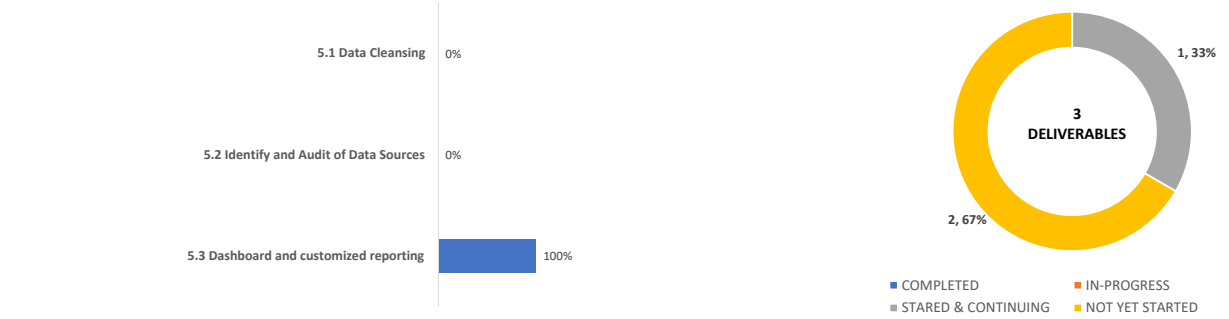
4. INTRODUCE AUTOMATION OF SYSTEMS AND PROCESS



PROGRESS ON IMPLEMENTATION OF STRATEGIES (NO. & % COMPLETED)

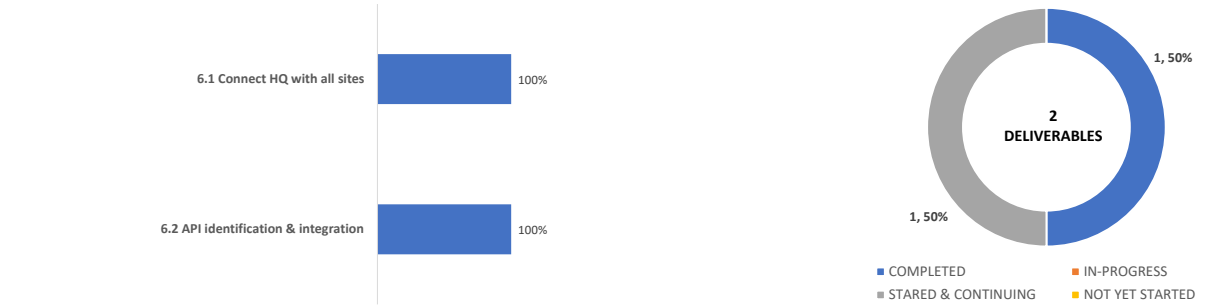


5. IMPROVE QUALITY, INTEGRITY, AND MEANINGFUL REPRESENTATION OF DATA



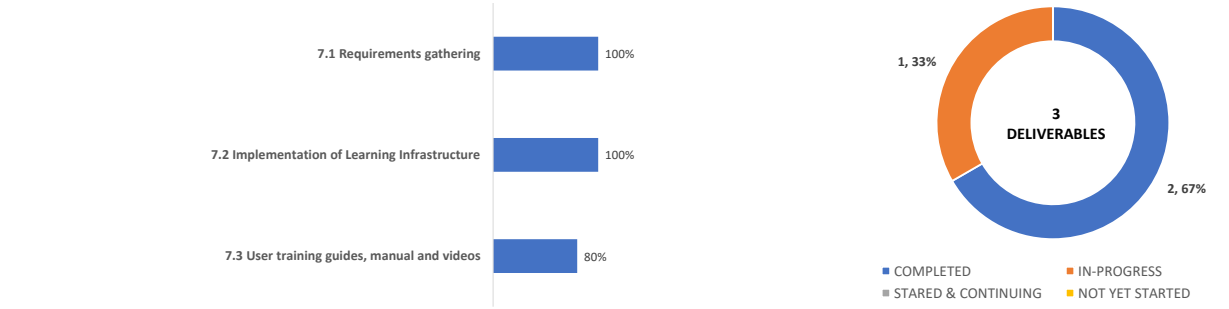
PROGRESS ON IMPLEMENTATION OF STRATEGIES (NO. & % COMPLETED)

6. UNIFICATION OF SYSTEMS



PROGRESS ON IMPLEMENTATION OF STRATEGIES (NO. & % COMPLETED)

7. LEARNING/ KNOWLEDGE MANAGEMENT SYSTEM



PROGRESS ON IMPLEMENTATION OF STRATEGIES (NO. & % COMPLETED)

8. IDENTIFY AND IMPLEMENT INTERNATIONAL BEST PRACTICES LEADING TO CERTIFICATIONS

PROGRESS ON IMPLEMENTATION OF STRATEGIES (NO. & % COMPLETED)