OPERATIONS REVIEW

IT GOVERNANCE

This assessment followed industry best practices including IT governance frameworks such as COBIT v5 (Control Objectives for Information and related Technologies).

IT Governance is the processes and structures which inform, direct, manage, and monitor how the organization makes the best and most effective use of technology.

An IT governance framework is designed to ensure that the right people are making the right decisions, at the right time and for the right reasons. It is also important that everyone in the organization understands how technology decisions are made, priorities set so that they can add their ideas into the mix in the right way.

In some cases, IT decision making means collective decision on corporate priorities, in other areas it will involve technical decision making on the best data storage technology or networking protocol – thus different groups, with different skill sets need to be involved.

Organizations often view decisions about technology as complicated, technical and "best left to the experts in IT". However, in a surprising number of cases, decisions about technology have ramifications, well beyond the technology itself:

- How do we want to use technology in our business?
- What technology do we want our people to use, and how do we want them to use it?
- How much should we spend on technology?
- Which of our business processes should we direct our IT dollars towards?
- What do we need to tackle first?
- Should we do this now, or later?
- How secure do we want to be?
- What should be available first in the event of a data centre outage or a disaster event?

These are not decisions that technologists alone should be making, they are important business decisions that the leaders of the organization must address. There are of course purely technical decisions to be made, and the right IT staff (with the appropriate skillsets) need to be involved – but in most cases IT experts should be advising business leaders.

Perhaps more important is the cultural and business change and learning that is necessary to take full advantage of technology. It is important that business leaders learn what's possible, and learn from other projects what it takes to be successful. Governance models allow this type of learning to be internalized.

What is an IT Governance Model?

IT governance models should facilitate collaborative working, bringing together staff from various departments and disciplines. IT governance is a combination of:

- Decision making groups and individuals (e.g. membership, inter-relationships)
- Policies & standards (e.g. architecture, software procurement policy)
- Processes & methods (e.g. prioritization, project execution)
- Measurement and monitoring (e.g. KPI reporting)

Our assessment discovered that there is no formal IT framework in place at SPi for the governance and management of enterprise IT. There are job descriptions that define roles and responsibilities and signing delegation of authorities; the Director of IT appears to make most technology decisions without input from the business.

IT Policies

Policies and standards should establish the parameters within which SPi uses technology, creating clear expectations for those that use and manage technology. In keeping with the commentary throughout this section, many of the decisions related to technology are business or management decisions. These are not decisions to be made by IT on behalf of the corporation. For example:

- Which employees get smartphones
- Who is authorized to register a web domain for the organization
- Which websites staff can access, and whether that activity should be tracked
- What content is saved when an employee exits the company
- How much space does an employee have in email

For each of these decisions several factors need to be weighed, including business impacts, employee impacts and importantly, cost impacts. A standard IT policy framework typically addresses the following areas:

- Acceptable use
- IT Security
- Backup, recovery, BC and DR
- Asset lifecycle management
- Hosted and cloud solutions
- Data management (lifecycle, privacy)
- IT procurement processes
- Email & voicemail standards (including archiving)

SPi has a major gap in this area. IT Management, with the input of staff, stakeholders and an ITSC should review, revise and augment a corporate IT policy framework in the context of this strategy, to ensure that it accurately reflects how the organization wishes to use and manage technology. A leadership team (**the Board**) needs to be responsible for reviewing and approving policies recommended by IT Management/ITSC.

IT Architecture

IT Architecture is one of the most important standards. At a high level the Architecture represents core concepts that underpin this strategy that SPi will pursue. The IT Architecture represents a macro level blueprint, the Official Plan if you will, for how the IT environment is to be developed and built.

More detailed current and to-be architectures (the equivalent of secondary and community master plans, to carry on the analogy) have been, or will be, developed by the SPi IT team for the Infrastructure, Application, Integration, Data and Business Process layers of the architecture. These plans, through the work of the **Architecture Review Board** will ensure that new solutions can be designed and implemented in a way that appropriately integrates with existing solutions.

In addition to the IT Architecture the [1]IT Management team will lead the development of guidelines and playbooks to simplify and delegate IT decision making to project teams and staff. Examples include:

- IT service catalog
- Device guidelines, and associated requests / approval processes
- Cloud playbook
- Security assessment process
- Project initiation playbook
- Change management playbook
- Business process design playbook

Internal to IT, documentation of IT technical standards and SOP's (Standard Operating Procedures), are important internal documents and tools to help the IT team deliver its mandate and comply with policy directives. IT documentation, though currently adequate where it exists, should be improved by the IT Team. The team should determine where the knowledgebase will be managed. At a minimum, SOP's for the following areas should be in place:

- Incident management
- Change control process management
- Backup and recovery,
- Problem management
- Security management,
- Configuration management of critical systems

Table 1.0 summarizes the assessment of an IT Governance framework with a score based on a 1-5 rating as outlined in **Figure 1.0**:

Table 1.0: IT Governance Review

IT GOVERNANCE		
CRITERIA		**ASSESSMENT**
LEVEL OF ACCEPTANCE Discipline is accepted by the organization		IT Governance Framework – does not exist IT Policies – there are no formal SPi policies in place and the organization relies on its MSP for standard backup practices SOPs – operating procedures do not appear to be in place for most IT processes
BUSINESS ALIGNMENT Discipline aligns with business objectives		The business does not have a formal IT Steering Committee or working group to help determine requirements – The IT Manager appears to make all decisions.
OBSOLESCENCE Component is up to date and fully supported		Processes do not exist
COST/EFFORT Includes direct costs (HW/SW) and indirect costs (downtime/operations)		By not having these processes in place, SPi has experienced unnecessary outages and performance degradation within the infrastructure. Business units work in silos creating technology issues and inefficiencies.

Figure 1.0: Rating Legend – IT Governance

[1] Organizations quite often leverage outside advisors in order to enhance the process

BUSINESS CONTINUITY MANAGEMENT (BCM)

IT SERVICE CONTINUITY MANAGEMENT (ITSCM)

As a subset of the Business Continuity Plan, IT Service Continuity Management (ITSCM) proactively assures IT services can be recovered and provisioned based upon the established business continuity management timeframes. Basically, once you rate your critical applications, assuring the critical are up first within the agreed upon timeframe. This helps to have a pre-defined process in place to help the organization recover to normal operating procedures after a disaster. On the reactive side of the equation, once the disaster has occurred. IT service continuity management is the process responsible for assessing the impact of the disruption on IT services.

Backup and Recovery

ITSCM considers application backup and recovery one of the risk mitigating factors in assuring service continuity.

Currently SPi does not have a formal Backup & Recovery strategy per se, although they do have backups being performed by the MSP as defined by their (MSP) schedule. The solution does not address data management which will most likely result in "stale" inactive data residing on production storage at a high cost to the business.

Business Continuity (Disaster Recovery & IT Enterprise Risk Management)

For organizations such as SPi, service disruptions, delays in responding to customer requests, inability to process transactions in a timely manner or being unable to resume business in the face of a disaster can all have significant impacts on the effective operation of the business.

[2]Currently the MSP (Fujitsu) guarantees a system uptime of 99.5% (3.6 hours of allotted downtime per 30-days). This is well below industry standards of 99.999% (26 seconds of allotted downtime per 30-days).

There are no Disaster Recovery provisions in place for any systems currently in place within the Fujitsu facility.

> ***SLA Note:*** *This Agreement does not include an off-site disaster recovery plan. Such a service is available from Fujitsu, and has been the subject of a preliminary proposal, but has not been accepted by the Client. If SPi wishes to add this service in the future, a new proposal can be made taking into account the specific needs of the customer*

Cyber-Insurance

Currently SPi does not hold a Cyber-insurance policy to protect against a data security breach. Generally speaking, any individual or business entity that collects any type of electronic data about people should seriously consider buying Cyber-insurance — it is likely one of the biggest gaps in insurance coverage today. There are common elements in today's policies such as:

- Crisis management, which may include the expense of investigating an incident and remediating networks;

[2] The Uptime SLA details the percentage of time SPi systems are guaranteed to be up and available, rather than offline for any number of reasons. Without an Uptime SLA that matches SPi needs, systems could go offline resulting in a loss of business - damaging operations.

- Notification, which would cover the cost of notifying all individuals potentially impacted by the loss of data or;
- Business loss such as theft or fines and penalties assessed.

In addition to this, many insurance companies will not provide cyber-insurance coverage without a formal Business Continuity Plan. If the coverage is in fact available, the premiums will typically be substantially more than a standard policy for an organization with a formal BCP strategy.

Table 2.0 summarizes the assessment of a Business Continuity strategy with a score based on a 1-5 rating as outlined in **Figure 2.0**:

Figure 2.0: Rating Legend - BCM

Table 2.0: BCM Assessment

BUSINESS CONTINUITY MANAGEMENT (BCM)		
IT SERVICE CONTINUITY MANAGEMENT (ITSCM) – DESIGNED TO SUPPORT THE OVERARCHING BCM PROGRAM		
CRITERIA		ASSESSMENT
LEVEL OF ACCEPTANCE Discipline is accepted by the organization		Backup & Recovery – There are formal procedures in place with the MSP Disaster Recovery – There are no formally documented procedures in place however the MSP has included this service as part of the SLA IT Enterprise Risk Management – There is no formal program in place to address Risk within ITS
BUSINESS ALIGNMENT Discipline aligns with business objectives		Backup & Recovery – The overall strategy is somewhat aligned with the business Disaster Recovery – No work has been completed and aligned with the business objectives IT Enterprise Risk Management – Nothing has been formalized
OBSOLESCENCE Component is up to date and fully supported		Backup & Recovery – The technology used is adequate Disaster Recovery - This process has never been tested IT Enterprise Risk Management – Nothing formal is in place
COST/EFFORT Includes direct costs (HW/SW) and indirect costs downtime/operations)		Backup & Recovery – the solution currently used has a high cost of ownership (high operating costs) Disaster Recovery –Costs and effort is unknown at this time, however the MSP contract has a significant operating cost to the business IT Enterprise Risk Management – Nothing formal is in place

IT Service Management (ITSM)

The service desk was an evolution of the helpdesk, born out of the ITSM best practice framework ITIL, and based on the underlying concept of "managing IT as a service." The terms are often used interchangeably, but it's important to note that Helpdesk is now considered a *sub-set* of a Service Desk; The process concerned with resolving issues using the break/fix concept.

A Service Desk is more strategic term - it's not just about "fixing stuff", but also about adding new services and maintaining the existing ones.

Within the IT Service Operation part of the ITIL Service Lifecycle, the Service Desk function is the core, acting as a **single point of contact** for all end users. The Service Desk usually logs and manages all incidents and service requests, and provides an interface for all other Service Operation processes and activities. The Service Desk is the key to the implementation of the Request Fulfillment and Incident Management processes. It's important to understand that Incident Management is a cross-IT organization process, not a Service Desk-only process.

Within SPi IT Service Management has some structure but lacks a formal single channel for issues. Issues can be logged through SPi support or Fujitsu ("MSP")

The following key items were discovered during the assessment:

1. Service Desk (Helpdesk)
    a. Both SPi and the MSP have independent service desk systems
    b. Incidents can flow through the SPi or Fujitsu with no centralized tracking or reporting
    c. There appears to be inconsistencies with incident resolution times and details in the systems
2. Incident Management
    a. The use of two service desk platforms, lack of a formal incident management process, along with multiple vendor support for systems has made the incident management lifecycle inefficient
    b. Incidents can appear as multiple tickets in each system, skewing reporting.
3. Proper definitions of [3]"incidents" vs "problems" do not appear to be followed
4. Asset Management – This appears to be an ad hoc process
    a. There is some tracking of assets through spreadsheets but this is an informal process
5. Reporting and Trend Analysis
    a. There are no defined key performance indicator (KPI) metrics
    b. Reports are available but neither SPi or the MSP publish and review incidents on a predefined schedule
6. Change Status Tracking and Reporting
    a. There is no change management process in place or any reporting to senior management
7. Monitoring and Reporting Against SLAs
    a. There is nothing in place to report against service level agreements (SLA)

[3] According to ITIL, an **incident** is an unplanned interruption to a service or a degradation in the quality of a service. What often determines the classification of something as an incident is whether or not the service level agreement (SLA) was breached. However, ITIL allows for raising an incident even before an SLA has been breached in order to limit or prevent impact. A **problem** is defined as the root cause of one or more incidents. Problems can be raised in response to one or more incidents, or they can be raised without the existence of a corresponding incident.

Table 3.0 summarizes the assessment of IT Service Management (ITSM) with a score based on a 1-5 rating as outlined in **Figure 3.0**:

Table 3.0: IT Service Management

IT SERVICE MANAGEMENT (ITSM)		
CRITERIA		**ASSESSMENT**
LEVEL OF ACCEPTANCE Discipline is accepted by the organization		Although the has been a certain level of acceptance over the duration of the MSP contract, processes need to be re-evaluated and streamlined
BUSINESS ALIGNMENT Discipline aligns with business objectives		The processes are somewhat aligned but required re-evaluation with greater input from senior management
OBSOLESCENCE Component is up to date and fully supported		The ITSM systems are adequate with respect to functionality and capabilities but need to be better utilized and in line with ITIL best practices
COST/EFFORT Includes direct costs (HW/SW) and indirect costs (downtime/operations)		The inefficiencies with the overarching ITSM processes have created redundancies and gaps that are costing the business unnecessary operating expenditures and a potential loss of revenue during the incident management lifecycle.

Figure 3.0: Rating Legend – IT Service Management

RECOMMENDATIONS

OPERATIONS

IT GOVERNANCE

Several opportunities to improve the governance of technology could be implemented, including:

- Roles and responsibilities of each group could be more clearly defined
- Corporate IT policies must be updated
- An **IT Architecture Review Board** and standing **Steering Committees Group** should implemented
- Comprehensive portfolio information on operational / technical infrastructure projects should be shared with an IT Steering Committee (ITSC).

IT POLICIES

There is a major gap in this area that needs to be addressed. IT Management, with the input of staff, stakeholders and ITSC should review, revise and augment the corporate IT policy framework in the context of this strategy, to ensure that it accurately reflects how the organization wishes to use and manage technology. A leadership team needs to be responsible for reviewing and approving policies recommended by IT Management/ITSC.

IT ARCHITECTURE

Add an Architecture Review Board

The Architecture Review Board is responsible for coordinating the development of architectural standards. The Board also reviews all technology and business initiatives to monitor compliance with the standardized architecture, and makes recommendations to project teams, sponsors, the IT Management Team, and ITSC.

These plans, through the work of the **Architecture Review Board** will ensure that new solutions can be designed and implemented in a way that appropriately integrates with existing solutions.

Solutions, Network and Technology Architect roles will be established within the IT department and will have the delegated authority from the IT Management team to review solutions for architectural fit.

IT STANDARDS, GUIDELINES AND PLAYBOOKS

In addition to the IT Architecture the IT Management team will lead the development of guidelines and playbooks to simplify and delegate IT decision making to project teams and staff. Examples include:

- IT service catalog
- Device guidelines, and associated requests / approval processes
- Cloud playbook
- Security assessment process
- Project initiation playbook
- Change management playbook
- Business process design playbook

Internal to IT, documentation of IT technical standards and SOP's (Standard Operating Procedures), are important internal documents and tools to help the IT team deliver its mandate and comply with policy directives. IT documentation, though currently adequate where it exists, should be improved by the IT Team. The team should determine where the knowledgebase will be managed. At a minimum, SOP's for the following areas should be in place:

- Incident management

- Change control process management
- Backup and recovery,
- Problem management
- Security management,
- Configuration management of critical systems

Branch Office Certification Program

There are currently no formal standards in place for the branches, that would allow the organization to configure remote sites to adhere to controlled specifications.

The implementation of a Branch Certification Program would include a formally documented infrastructure for such items as:

- Connectivity (type, configuration, installation, provider)
- Cabling (type, configuration, installation)
- IP Address Management (IPAM)
- Hardware/Software

This program would enhance the support process and could be extended to include an onboarding process for new corporate acquisitions.

BUSINESS CONTINUITY MANAGEMENT (BCM)

IT SERVICE CONTINUITY MANAGEMENT (ITSCM)

Backup and Recovery

The backup and recovery process needs to be formally documented and linked to the data archiving process as outlined in Data Lifecycle Management section of this report.

Business Continuity (Disaster Recovery & IT Enterprise Risk Management)

Currently the MSP (Fujitsu) guarantees a system uptime of 99.5% (3.6 hours of allotted downtime per 30-days). This is well below industry standards of 99.999% (26 seconds of allotted downtime per 30-days). In addition to this, there are no formal Disaster Recovery (DR) requirements identified by SPi.

To mitigate the effects of disruption, it is essential SPi prepare and manage a business continuity strategy. A Business Continuity Management (BCM) program will enable SPi to update, control and deploy these plans and align them with their strategic and operational objectives.

The 5 levels of disaster

Consider the five levels of disaster recovery when preparing the business continuity plan:

1) Email or File lost
2) Server down or damaged
3) Physical office inaccessible (evacuation)
4) Office obliterated; server room lost (fire)
5) The entire city where your office is located is struck by disaster

For each disaster scenario, determine the:

- RPO (Recovery Point Objective) or how much data you could afford to lose in minutes, hours, or days
- RTO (Recovery Time Objective) or how long it should take to get you back up and running

Then, verify that what the MSP will do in each disaster scenario is acceptable to SPi—and meets your various RPO and RTO requirements.

As the industry leader in BCM, our processes follow the Disaster Recovery Institute (International) framework and best practices guidelines:

Program Initiation

Corporate communication within the Business Continuity Management (BCM) program is the first step to success:

1. Is the SPi BCM strategy clearly aligned with corporate business goals?
2. Have key roles been defined?
3. Framework development

Gaining executive/senior management support & commitment is critical to the success of a Business Continuity Program. Once SPi develops a mission statement/charter for the BCM process, the next step is to define objectives that support the organizations mission. One of the key activities in this stage will be the initiation of a BCM Steering Committee[6]. This group will provide guidance, oversight, resources, input, and approval throughout the program.

The three main elements of the BCM Program are:

1. Scope – Document what the plan will recover and what it will not – consider the "whole" organizations
2. Objectives – Document what will be delivered at the end of the project & the benefit to the organizations
3. Assumptions – Document all assumptions such as funding & management commitment.

IT Enterprise Risk Management

It all starts with a Risk Assessment and Business Impact Analysis (BIA):

1. Identify organizational risks/threats and vulnerabilities & initiate the BIA
2. Define process Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
3. Automated reporting eliminates the need for cumbersome tools such as spreadsheets.

Risk Evaluation/Control coupled with a Business Impact Analysis will identify threats & vulnerabilities and the likelihood that they will occur – followed by the identification of potential impacts to the business. The result if the analysis is a clear definition of time sensitive processes and the requirements to recover them in a timeframe that's acceptable to the organizations.

The BCM program must identify the criteria to quantify and qualify impacts such as:

- Customer impact
- Financial Impact
- Regulatory impact
- Reputational impact
- Operational impact
- Human impact

Strategy and Development

Build a robust business continuity and disaster recovery plan aligned with key industry standards and frameworks:

1. Define operations/technology continuity & recovery strategies
2. Emergency response, Pandemic Preparedness
3. Single, centralized framework

The data collected during the Risk Evaluation and BIA phases can now be used to identify available continuity and recovery strategies for the businesses operations and technology. Recommended strategies must meet RTO and RPO objectives identified in the BIA. A cost benefit analysis is then

[6] SPi could consider leveraging IT Steering Committee as a starting point for an overarching BCM program

performed on the recommended strategies to align the cost of implementing the strategy against the assets at risk.

This element also defines Emergency Preparedness and Response requirements to develop and implement the organizations plan for response to emergency situations that may impact safety of employees, visitors, and other assets. Incident Management is introduced which helps you define escalation procedures that help determine criteria for disaster declaration.

Plan Implementation and Documentation

Manage BC/DR & Risk programs and efforts from one, centralized platform:

1. Development of continuity/recovery processes & procedures
2. Crisis/Incident Management fully integrated with dashboards & reports
3. Customized templates

The Business Continuity Plan is a set of documented processes and procedures which will enable the business to continue or recover time sensitive processes to the minimum acceptable level within the timeframe acceptable to the organization. The BCM teams design, develop, and implement the continuity strategies approved by the business and document the recovery plans to be used in response to an incident or event. Our recommended cloud-based system allows you to manage all relevant plans from an easy to access centralized location.

Some of the plans developed during this phase include:

- Disaster Recovery Plans
- Emergency Plan
- Incident Management Plan
- Business Continuity Plan

Plan Implementation and Documentation

Includes a virtual sandbox to test recovery scenarios & perform exercises:

1. Simplify audits and control reviews
2. Crisis communication, awareness & training
3. Plan testing exercises

A program should also be developed and implemented to establish and maintain awareness about the BCM Program and to train staff so they're prepared to respond during an event.

A BCM system allows organizations to perform regular testing from a dedicated recovery sandbox. In order to be effective a BCM Program must implement a regular exercise schedule to establish confidence in the business. As part of the change management program, the tracking and documentation of these activities provides an evaluation of the on-going state of readiness and allows for continuous improvement to recovery capabilities and ensure that plans are complete and accurate.

By following the guidelines outlined in this section of the report SPi could expect to complete a major portion of this work with 60 – 90 days of effort. Key activities will be:

1. Initiate the DR Steering Committee and establish revised guidelines and principles as required
2. Identify organizational Risks, Threats and Vulnerabilities
3. Initiate a Business Impact Analysis' "as required" in order to establish RTO and RPO's
4. Build DR procedures as required
5. Determine if the MSP satisfies the requirements

IT Service Management (ITSM)

It is recommended that SPi centralize and clarify the role of the **Service Desk** – ensure that it follows ITSM best practices framework.

As illustrated in **Figure 6.0**, the recommendation is that SPi refine its support model to ensure adherence to ITIL best practices pertaining to ITSM. The primary objective should be to centralize all support calls through the SPi helpdesk. From there, Tier-1 support will escalate to the MSP as necessary.

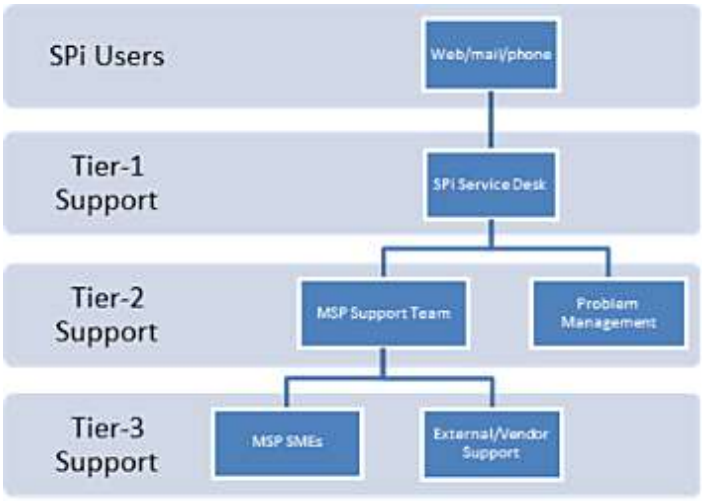

Figure 6.0: Example of role separation within IT for the Incident Management process. While Problem Management does not support SPi users directly, it is responsible for finding and eliminating the root cause of an incident.

Tier-1 Support / Service Desk

As illustrated, SPi Service Desk is involved in the Incident Management process, in the role of **Tier-1 Support**. Once end users contact the Service Desk as the central point of contact, SPi Service Desk attempts to collect as much information and diagnostics about the incident as possible, and even resolves the issue on the spot, if possible. This will reduce resolution time for all minor incidents (q: my computer doesn't work – a: did you try to turn it on?), and first-contact resolutions consequently increase end user satisfaction.

In general, Tier-1 support staff within ITIL Incident Management will be managed by a **Service Desk Supervisor (or equivalent)**, who will also serve as the escalation point, if needed. If Tier-1 Support is not able to resolve the incident right away, it will escalate the incident to **Tier-2 Support** (MSP).

Tier-2 Support / Service Desk

Tier-2 Support of Incident Management is a role generally composed of the resources with greater technical skills than those of Tier-1. In the case of SPi this role will be delegated to the outsourced MSP. The MSP will keep SPi support aware of the progress of the incident via ticket updates.

Tier-3 Support / Service Desk

The **Tier-3 Support role** is typically reserved for external suppliers and vendors; The MSP will escalate as necessary, keeping SPi support aware of the progress of the incident via ticket updates.