Town of
Port Hedland

Information & Communications Technology Strategy 2020-2025

Acknowledgement of Country

The Town of Port Hedland would like to acknowledge the Kariyarra, Ngarla and Nyamal people as the Traditional Custodians of the Port Hedland lands. We recognise their strength and pay our respects to their Elders past and present.

We extend that respect to all Aboriginal & Torres Strait Islander people of the local community and recognise their rich cultures and their continuing connection to land and waters.

Contents

Executive Summary

The Town of Port Hedland (the Town) has an extensive and diverse Information and Communication Technology (ICT) portfolio. This reflects the diversity of functions performedby the Town and the requirement for self-sufficiency caused by Port Hedland's isolation. The ICT strategy aims to deliver ICT services and assets that meets users' needs reliably and in a cost effective manner.

The ICT strategy has identified a significant program of work that is required over its term toimplement generational change to key business systems and applications, catch-up onhardware renewal and to improve network communications, disaster recovery capability andsecurity strength. The program is highly interdependent and the implications of each part onthe other needs to be clearly understood. At the end of the program the Town will be relianton Software as a Service (SaaS) arrangements that will reduce the on-premise hardware footprint but also increase dependency on the internet.

Initiatives that will have the greatest direct impact on users are:

- The core system replacement project to replace SynergySoft
- Migration to Microsoft 365
- Clean-up of corporate data

To successfully achieve these initiatives the organisation needs to adequately resource themand sustain the appetite to pursue process improvement.

As each initiative is delivered transactional interaction with the Town will be simplified for the community and vendors, internal business processes will flow more smoothly and staff will have a better suite of tools to perform their roles. The ability to resist and recover from business interruptions and cyber malevolence will increase and become simpler.

Governance

Strategic Community Plan and Corporate Business Plan

ICT has a direct and indirect linkage to the Strategic Community Plan (SCP).

The direct linkage arises by specific actions for ICT to deliver in the Corporate Business Plan (CBP) as strategic responses identified in the SCP, summarised in Table 1: ICT Responses to the SCP.

ICT has an indirect link to the SCP through the provision of the business systems and applications and infrastructure needed by the various functions of the Town to deliver the services and programs contained in the SCP.

Table 1: ICT Responses to the SCP

Strategic Theme	SCP Outcome	Strategic Response	Action
Our Community	An inclusive and involved community	*1.b.1* Newcomers to Port Hedland are provided with inductions, information and opportunities to engage and get involved	*1.b.1.2* Provide free public Wi-Fi at identified Town locations
Our Economy	An enabling, attractive business environment	*2.b.4* Business approval processes are transparent and pathways streamlined	*2.b.4.1* Develop, implement and review an ICT and IS strategy *2.b.4.2* Develop, implement and review new technology and system improvements

Vision

The vision for the ICT strategy is to provide a reliable and cost effective ICT solution that meets users' needs.

Reliable

- Stable business systems and network communications
- Appropriate redundancy to sustain critical functionality
- Secure against cyberattack

Cost Effective

- Fit for purpose business systems, equipment and infrastructure
- Planned migration to proven technologies in accordance with the ICT strategy
- Adherence to the asset management plan

Meeting User Needs

- Simplified ICT experience for all users
- Community provided with the facilities it is willing to pay for
- Transactional ease for community and vendors
- Staff provided with the technology tools they need to effectively and efficiently serve the community.

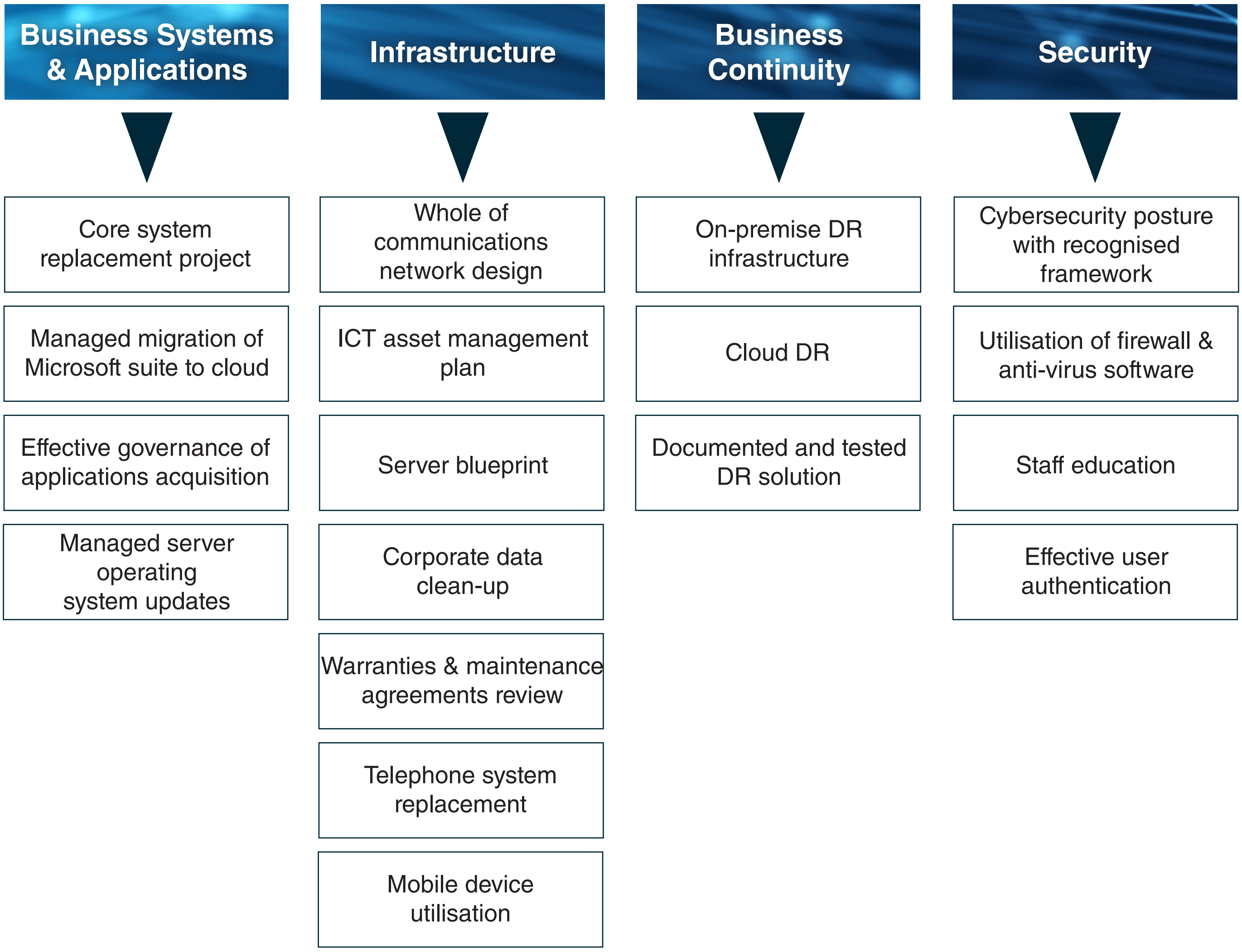
The strategy to achieve the vision is structured around Business Systems and Applications, Infrastructure, Business Continuity and Security. The roadmap from the current state to the desired state is detailed in Appendix 1: ICT Strategic Roadmap.

Reliable

Cost Effective

Meeting User Needs

ICT Strategic Roadmap



Business Systems & Applications	Infrastructure	Business Continuity	Security
Core system replacement project	Whole of communications network design	On-premise DR infrastructure	Cybersecurity posture with recognised framework
Managed migration of Microsoft suite to cloud	ICT asset management plan	Cloud DR	Utilisation of firewall & anti-virus software
Effective governance of applications acquisition	Server blueprint	Documented and tested DR solution	Staff education
Managed server operating system updates	Corporate data clean-up		Effective user authentication
	Warranties & maintenance agreements review		
	Telephone system replacement		
	Mobile device utilisation		

Risk Management

The risks associated with ICT changes as the delivery of ICT services evolves. A risk assessmentof the major ICT risks has been performed and reassessed to measure the impact successful implementation of the ICT strategy would have, summarised in Table 1: ICT Risk Profile Summary. The risk profile is assigned according to the likelihood of an event occurring and the severity of the consequence of the risk occurring. The risk matrix used to determine the risk profile is contained in Appendix 3: Risk Matrix.

Strategic responses to the major risks are summarised in Table 2: ICT Risk Mitigation. For risksrating that remain unchanged, in most instances the ICT strategy reduces the likelihood of anevent occurring but does not reduce the impact. For example, the consequence of data theftremains the same once it is stolen. The ICT strategy is not expected to have a singularly measurable impact on the likelihood of staff leaving the organisation.

Table 1: ICT Risk Profile Summary

Risk	Current Risk Rating	Residual Risk Rating
1. Cyberattack – loss of service	High	Moderate
2. Prolonged loss of local network communications	Moderate	Low
3. Prolonged server outage	Moderate	Moderate
4. Prolonged loss of internet communications	Moderate	Moderate
5. Obsolete business system or application	High	Low
6. Under investment in ICT	High	Moderate
7. Over investment in ICT	Low	Low
8. Data theft	Moderate	Moderate
9. Prolonged telephone system outage	Moderate	Moderate
10. Staff turnover	High	High

Table 2: ICT Risk Mitigation

Risk	Likelihood	Consequence	Strategic Response
1. Cyberattack – loss of service	Possible	Major	• Develop cybersecurity posture with recognised framework • Effective utilisation of firewall and anti-virus software • Staff education • Effective user authentication
2. Prolonged loss of local network communications	Unlikely	Major	• Whole of communications network design
3. Prolonged server outage	Unlikely	Major	• Documented and tested DR solution
4. Prolonged loss of internet communications	Unlikely	Moderate / major	• Core system replacement project • Managed migration of Microsoft suite to cloud • Whole of communications network design • Server blueprint • On-premise DR infrastructure • Cloud DR
5. Obsolete business system or application	Likely	Moderate	• Core system replacement project • Managed migration to newer versions of Microsoft products • Effective governance of applications acquisition
6. Under investment in ICT	Likely	Moderate	ICT strategic roadmap

Table 2: ICT Risk Mitigation

Risk	Likelihood	Consequence	Strategic Response
7. Over investment in ICT	Unlikely	Minor	• ICT strategic roadmap
8. Data theft	Possible	Moderate	• Cybersecurity posture with recognised framework • Utilisation of firewall and anti-virus software • Staff education • Effective user authentication
9. Prolonged telephone system outage	Possible	Moderate	• Telephone system replacement
10. Staff turnover	Likely	Moderate	• Core system replacement project • Managed migration of Microsoft suite to cloud • Effective governance of applications acquisition- Corporate data clean-up

The detailed risk assessment outlining business impact and mitigations is contained in Appendix 2: ICT Risk Assessment.

The most significant change to the ICT risk profile will be driven by the continued adoption of Software as a Service (SaaS). As major systems are moved to SaaS the on-premise server footprint will decrease. Cybersecurity, including protection from data theft, and disaster recovery will be provided by the system providers who are better resourced to address these challenges. Disaster recovery for the residual systems and data, primarily the corporate drive, will also be in the cloud. This trend does however increase exposure to the risk of disruption to internet services. The mitigations for this will be the retention of on-premise back-up capability and duplicated internet connections on separate trunk routes.

A distinction is made between short-term and prolonged service outages for local network communications, servers, internet and phone system. Increasing the probability of uninterrupted services is achieved by increasing the investment in redundancy with automatic fail-over capability. In some instances this may be achievable but the cost would need to be justified against the benefits.

The Town has not maintained a sufficient level of investment in its business systems and applications, specifically its core business system. The current system, SynergySoft, is at end of life and implementation of a replacement system will require significant investment in business process capability.

Policies & Internal Operating Procedures

The governance framework for ICT is provided by polices, Internal Operating Procedures (IOP) and agreements.

Polices that directly impact ICT are:

- 15/003 CCTV Operations
- 9/010 Asset Management

Staff usage of ICT is guided by:

- HR007 Mobile Phone Usage
- HR012 Equal Employment Opportunity, Bullying, Harassment and Grievance Handling
- Conditions of Computer / Communication Use Agreement signed by employees

The strategy identifies a need for IOPs for:

- Acquisition and maintenance of applications software
- ICT asset management
- Working from home

To further support the strategy, IOPs should be developed for:

- Business continuity and disaster recovery
- Cybersecurity

An ICT asset management IOP should include guidance for the disposal of retired equipment.

Human Resources

ICT human resources are a hybrid of Town staff, contractors and support agreements. Town staff currently consists of support officers and a part-time manager. Support officers provide front-line user support and co-ordinate minor projects. Two key contractual arrangements are in place, one to provide technical ICT leadership and support and one to monitor and maintain the CCTV network. Support agreements are in place with software and hardware vendors to provide helpdesk support for specific products.

Consultant support will be required for various projects including the core system replacement project, Microsoft 365 migration, telephone system replacement, network communications review and server blueprint.

Stakeholders

The ICT strategy aims to best meet the ICT needs of relevant stakeholders in a reliable and sustainable manner within the constraints of available resources.
The community, Town staff, vendors and regulatory agencies are identified as key stakeholders and their identified needs are detailed here.

The ICT strategy aims to ensure that the Town has the business systems and applications and ICT infrastructure in place, supported by adequate business continuity capability and protected by impenetrable security to meet these expectations in an operationally and financially sustainable manner.

Community

Access to technology based resources

- Physical assets including computers and printers
- Internet access including public Wi-Fi
- Library resources including e-library resources

Technology for doing business with the Town

- On-line payments including rates, fees and fines
- Obtaining permits and approvals

Respect for privacy

- Opportunity to understand CCTV deployment, capabilities and data retention
- Transactions and approval data retention, access and security

Dependable

- The Town is able to continue to deliver services and provide leadership and assurance
- People are provided with important information during significant community incidents

The Town utilises technology to:

- Operate efficiently and reduce costs
- Promote sustainably in its operations

Staff

Provided with the right tools to do their job

- User devices including computers and mobile devices and office devices
- Business systems and applications
- Access to on-line resources
- Support for the way they work including collaboration tools and remote working

User support

- Training and support for specific business systems and applications
- Generic technical support for hardware and connectivity issues

Reliability

- Access to business systems and applications and data always available
- ICT hardware always working

Supported through change

- Assistance and support to adopt to ICT enabled changes to business processes

Vendors

Supported engagement

- Communications from tender to completion through technology enabled channels
- Simple invoice submission and payment

Technology based service delivery

- Core deliverable is a technology rather than a service or a good
- Communications and data access necessary to fulfil deliverables

Regulatory Agencies

Compliance

- Compliance with statutorily imposed compliance obligations
- Compliance with industry imposed compliance obligations

Security

- Data is properly secured
- System and data access is appropriately controlled

Business Systems & Applications

Business systems and applications includes the core business system, currently SynergySoft, the Microsoft (MS) Office suite, ad hoc applications and server operating systems. This aspect of ICT is due for generational change that will impact the way people work and how ICT is delivered to the organisation. This change is dependent on organisational buy-in for process change and the availability of sufficient and reliable internet capacity.

Core Business System

SynergySoft supports business processes, primarily support services and some core services. The vendor has discontinued system development and are seeking to introduce a new product. Work has commenced by the Town to select and implement a replacement system.

Support services processes include: accounts payable and receivable, cash receipts, fixed asset register, general ledger, inventory, procurement, rating and rates notices, records management and trust and reserve administration. Core services processes include: cemetery administration, customer relationship management, desktop mapping, property administration and ranger services including dog registration and infringements.

Payroll is currently being outsourced and the Town does not have an asset management or maintenance management system.

The Town intends to engage a consultancy to project manage implementation over the anticipated two to three year implementation timeframe. This approach is intended to provide access to the appropriate resources and continuity of knowledge having regard to the difficulty the Town has recruiting and retaining staff. Key challenges are anticipated to be data migration and change management.

The preferred solution will be selected following a tender process. The Town currently does not have a position on whether the preferred solution is a best of breed, that is, multiple products, or an integrated solution, that is, most functions performed by a single system.

It is anticipated that the new core system will be SaaS. This will require adequate internet capacity and business continuity planning will need to address disruptions of internet service.

Microsoft Office Suite

The Town is currently working on MS Windows 10 operating system, MS Office 2016 Professional Plus and Internet Explorer. Migration to newer versions of Windows occurs periodically and once a version has been widely proven. Internet Explorer is used alongside Google Chrome and to a lesser extent, Firefox. Internet Explorer is anticipated to be phased out by Microsoft and replaced by Edge during the life of the strategic plan.

Microsoft Office has undergone generational change. The new generation is SaaS and has significant implications for users who adopt it. MS 365 integrates with corporate data storage, communications, security and disaster recovery. The implementation pathway will consume significant effort to properly understand the product and the implication for contiguous software.

A graduated implementation will be adopted. MS 365 will be piloted with a group of users before a whole of organisation roll-out. It will also operate in parallel with the existing on-premise solution. The objective will be to have fully migrated by the expiry of the on-premise MS Office licence. There is no immediate need to implement the change, particularly given the young age of the servers, however the Town should not dismiss the opportunity to avoid operating with redundant software in the future.

Ad Hoc Applications

The Town has a significant portfolio of applications, many of which are SaaS. The acquisition of these is usually user driven. It is not the role of ICT to adjudicate on a user's need for a particular application however duplication of solutions and mistakes of the past should be avoided, ICT does not have the capacity or expertise to provide user support and network communication constraints need to be considered. Appropriate governance is required for acquisition decisions.

Some applications may have been adopted because the functionality was not available in SynergySoft. The new core business system may offer previously unavailable functionality that should be assessed first. Existing applications may also be made redundant by the new system.

There have been instances of technology purchases that have not been able to be utilised because of network communication constraints. Some applications have become disused after a key advocate for their acquisition has left the organisation.

Each application needs to have an independent support arrangement with the vendor. ICT needs to be consulted prior to any purchases to assess the ICT infrastructure and security implications.

An IOP is required for the acquisition and management of applications that as a minimum addresses regulatory considerations, approval process, agreement management and retirement. ICT will maintain a database of application agreements.

Server Operating Software

The operating system for the servers has recently been updated to Windows 2016. Veeam is used to provide the virtual server environment and to back-up data. The server operating system will be updated periodically. Implementation planning for any alternative data back-up systems will need to accommodate statutory data retention requirements for the existing tape library.

Infrastructure

The Town has geographically dispersed infrastructure consisting of network communications, ICT hardware and telephony.

Network Communications Infrastructure

Network communications have developed organically in response to limited or uneconomical access to public telecommunications. The network currently utilises an enterprise grade 100Mb and 4G internet connections, point-to-point (PtP) radio links between sites and a SIP enabled telephone connection. The network has been expanded to address immediate user needs and a more considered approach is now possible.

A network communications infrastructure plan is required. The plan will assess existing infrastructure, forecast future demand and design a network to meet that demand and provide a sufficient level of redundancy. The assessment of existing infrastructure will include availability and reliability of internet communications that will be critical to business systems and applications and disaster recovery.

ICT Hardware

The Town has lagged in ICT hardware renewal and this is addressed in the 2020/21 budget. Equipment is replaced according to age however there is no formal documentation of ICT asset management. An ICT asset management IOP will guide both hardware and software investment and renewal and the asset management plan needs to include the CCTV network.

The main server and storage is located at the Civic Centre. Other locations have task specific servers and a DR environment has been created at the Depot. The main server was renewed in 2019 and server requirements are expected to change significantly with the continued uptake of SaaS, including DR storage. It is intended to relocate the main server to the Depot. Accordingly a server blueprint is required to understand the implication of these considerations.

There is a pressing need to clean-up the corporate drive which will be a major undertaking and data retention requirements must be complied with. The Town incurs considerable expenditure on equipment warranties and maintenance agreements and the cost effectiveness of these will be reviewed.

Telephony

The telephone system is overdue for replacement and the Town makes extensive use of mobile devices. A new system is likely to be cloud hosted and integrate with Microsoft 365 in the future. Existing telecommunications are internet dependent and a DR solution will need to be independent of the internet.

Mobile devices are currently well utilised to assist staff in the field. Future considerations include: equipping users with the most appropriate device for their role, accommodating the desire for bring-your-own devices in a sustainable manner and pushing messages to staff and the community with mobile devices.

The Town has established a DR solution at the Depot that replicates critical data a number of times per day. This solution is still maturing and requires documenting. Two further stages of development of the Town's DR capacity will be pursued: documenting scenario responses beyond the DR site and a cloud solution.

Business Continuity

The Town has established a DR solution at the Depot that replicates critical data a number of times per day. This solution is still maturing and requires documenting. Two further stages of development of the Town's DR capacity will be pursued: documenting scenario responses beyond the DR site and a cloud solution.

The ICT response to COVID-19 proved that the Town has the capability to rapidly respond to significant workplace interruption. The lessons from this response need to be captured and the response further refined. Documented responses to various scenarios and periodic testing of the DR site will ensure the Town is best placed to continue to serve the community in the event of disruptive events.

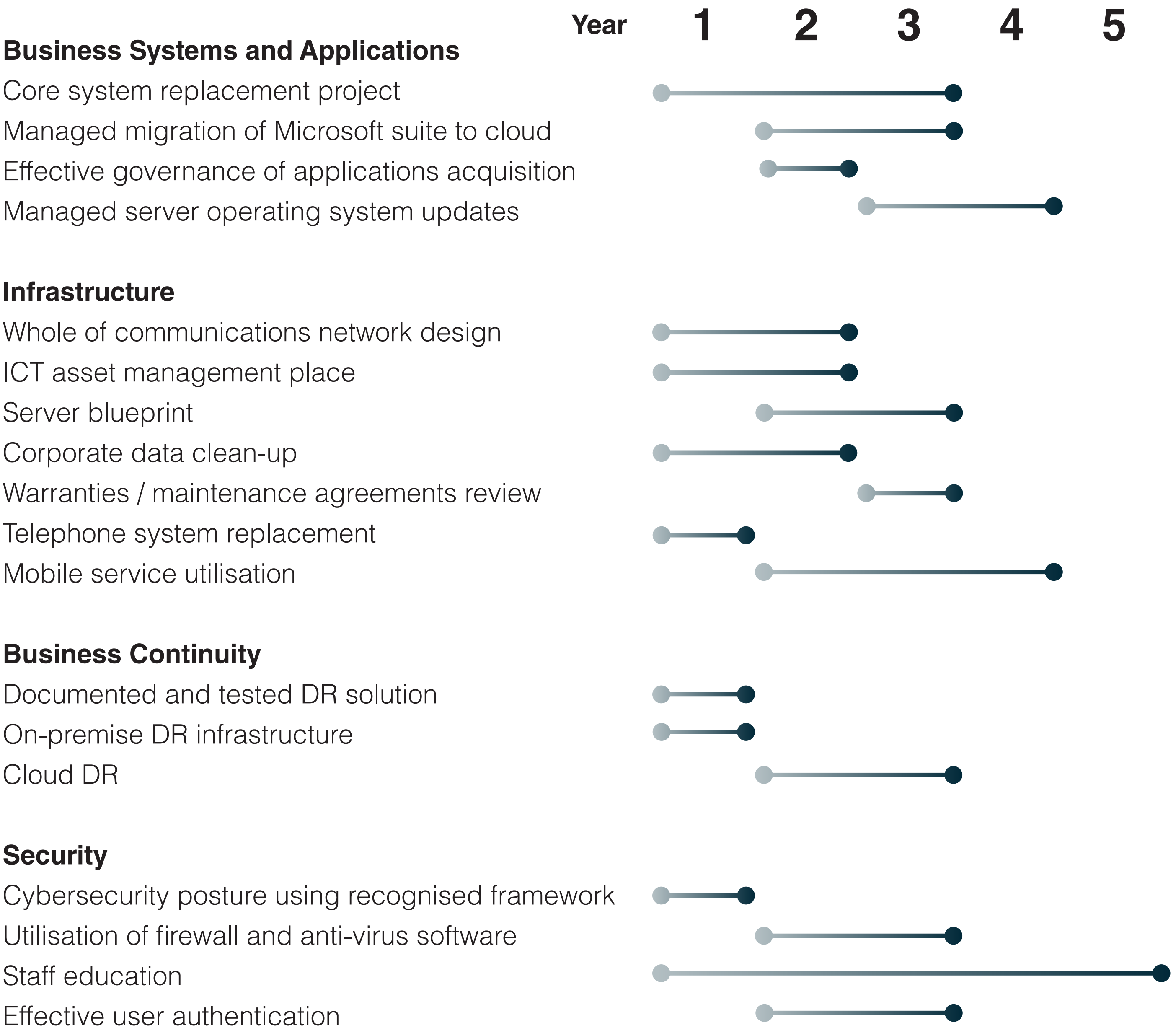
Numerous vendors offer cloud DR solutions that can be utilised in the event of physical disruption or a cyberattack. The Town had initially identified a preferred cloud DR solution however this was considered in isolation of the DR solution available with SaaS business systems and applications. The DR solution will evolve with the core business system replacement project and MS 365 transition. In the interim, the Town will continue to rely on the Depot DR site and weekly back-up tapes.

Security

The Town currently does not have a formal cybersecurity plan and relies primarily on its firewall and anti-virus software. Information to help staff stay safe on-line is shared periodically across the organisation. A formal cybersecurity risk assessment and plan will be developed using a recognised framework followed by periodic penetration testing. The opportunity to utilise multi-factor user authentication will be investigated.

ICT Strategy Delivery

The strategy will be delivered over five years as outlined in the implementation project plan. The implementation plan seeks to achieve generational change in the first three years. The final two years of the plan will be dedicated to bedding down the change. More significant projects will be formally project managed, including the core business system replacement project, MS 365 migration and corporate drive data clean-up. A project manager will be engaged to lead the core business system replacement project.



Business Systems and Applications

Core system replacement project
Managed migration of Microsoft suite to cloud
Effective governance of applications acquisition
Managed server operating system updates

Infrastructure

Whole of communications network design
ICT asset management place
Server blueprint
Corporate data clean-up
Warranties / maintenance agreements review
Telephone system replacement
Mobile service utilisation

Business Continuity

Documented and tested DR solution
On-premise DR infrastructure
Cloud DR

Security

Cybersecurity posture using recognised framework
Utilisation of firewall and anti-virus software
Staff education
Effective user authentication

APPENDIX 1: ICT STRATEGIC ROADMAP

Business Systems and Applications

As-Is	To-Be	Bridging the Gap	Actions	Timeframe (Year)
Core Business System				
SynergySoft ▪ At end of life ▪ Utilisation has not been fully developed by Town ▪ Some fundamental underlying business processes under-developed	New generation of business system successfully implemented Efficient underlying business processes capable and in control	Core system replacement project	Core system replacement project: ▪ Appoint project manager ▪ Procure new system ▪ Development implementation plan ▪ Acquire additional human resources as needed ▪ Prepare business and data for change ▪ Implement new solution ▪ Post-implementation support	1-3
Microsoft Office Suite				
▪ Microsoft Windows 10 OS	Optimally timed migration to next version	Managed migration of Microsoft suite to cloud	MS Windows version control: ▪ Monitor MS Windows maturity and industry trend to identify optimal migration point ▪ Manage migration	2-3
▪ Microsoft Office 2016 Professional Plus suit of desktop applications	Comprehensive utilisation of Microsoft cloud		MS 365 migration: ▪ Assess capacity and reliability of internet connection	2-3

▪ Entering three year licence renewal			▪ Assess reliability of MS365 ▪ Understand production functionality and implication for storage, servers, DR, security, etc ▪ Develop implantation plan ▪ Amend licencing agreement as required ▪ Manage implementation	

As-Is	To-Be	Bridging the Gap	Actions	Timeframe (Year)
Ad hoc Applications				
Substantial portfolio of ad hoc applications that are mostly user initiated and web based Missing licencing agreement documentation Acquisition requires ELT approval Ad hoc applications include: ▪ Active Carrot ▪ Armando ▪ Big Red Sky ▪ Carpool ▪ Copernic ▪ Danthonia ▪ Deepfreeze ▪ Elmo ▪ Fixie ▪ Hootsuite ▪ Industrial Automation Smartpack ▪ InfoCouncil ▪ Intramaps GIS ▪ iSentia ▪ LG HUB ▪ Linked-in ▪ Links Modular Solution ▪ Mailchimp ▪ Mandalay ▪ Milestone	Users have access to required applications Central register of applications Adequate stewardship of application agreements Agreement term and price structure matches business needs Efficient process to control acquisition Clarity on the role of the ICT function in managing applications	Effective governance of applications acquisition	Collate database of all application licencing agreements Rationalise applications based on usage Develop IOP for acquisition and control of applications including minimum standards for agreements, business case, support provision and budget and management sign-off	2 2 2

▪ Mozaic ▪ Open Insight ▪ PaperCut ▪ Power BI ▪ Rapid Plan ▪ Secure Pay ▪ Signage Live ▪ SLIP ▪ Smart Sheet ▪ Smarty Grants ▪ Spydus ▪ Survey Monkey ▪ Trapeze Plan Manager ▪ TreeSize Professional ▪ Typeform ▪ Vendorpanel ▪ When-I-Work ▪ Wondershare Filmora ▪ Smartfill				
Server Operating Software				
Servers utilise Microsoft Server 2016	▪ Up to date with patches ▪ Optimally timed migration to next version	Managed server operating system updates	▪ Monitor Microsoft Server maturity and industry trend to identify optimal migration point ▪ Manage migration	3-4
Veeam backup & recovery: Protects virtual machine workloads in the form of: ▪ Backup to disk ▪ Backup to tape (stored offsite)	▪ Documented recovery objectives aligned with business continuity plan, including downtime and data loss	Documented and tested DR solution	▪ Define Line of Business (LoB) applications including the planned deployment models for the next 5 years (on-prem, IaaS, SaaS)	1-3

No defined recovery objectives Undefined risks relating to downtime or data loss	▪ Backup solution that meets defined recovery objectives in a supportable and cost-effective manner. ▪ Back-ups potentially to the cloud		▪ Consult stakeholders on impact of downtime and loss of data per LoB application ▪ Prepare, distribute and ratify the BC Plan ▪ Determine solution for existing tape library to enable statutory data retention compliance ▪ Identify and implement back-up solution	
▪ Cisco enterprise solution: ▪ Working well for the business ▪ Maintain platform with normal lifecycle turnover	▪ Up to date firmware ▪ Replacement plan developed	Server blueprint	▪ Review existing equipment and plan for replacement ▪ Manage migration of equipment	1-2

Infrastructure

As-Is	To-Be	Bridging the Gap	Actions	Timeframe (Year)
Network Communications Infrastructure				
Organic communications infrastructure: ▪ Enterprise grade 100Mb internet connection ▪ 4G internet connections ▪ Internet enable link between some sites ▪ ACMA licensed link Depot – Civic ▪ PtP link Stadium to Depot ▪ Installing PtP link JD Hardie - Depot – Civic ▪ SIP enabled telephone connection Capacity and reliability of available internet connections unknown	Planned communications infrastructure that: ▪ Accommodates changing data capacity requirements internally and via internet ▪ Provides appropriate redundancy ▪ Cost effective Monitoring performance and utilisation Planned renewal	Whole of communications network design	Engage communications consultant to: Review existing network Assess Port Hedland internet infrastructure Forecast capacity demand for alternative SaaS scenarios - Phone system - Core business system - MS Office suite - Disaster recovery Identify cost effective redundancy opportunities Produce network design	1
			Implement communications infrastructure plan	1-2
			Develop asset management plan	1-2
ICT Hardware				
Some parts of asset renewal are lagging:	▪Equipment replacements based on pre-defined lifespans	ICT asset management plan	Develop ICT asset management IOP	1-2
			Monitor equipment development trends	1-5

As-Is	To-Be	Bridging the Gap	Actions	Timeframe (Year)
▪ Substantial renewal of user devices identified in 2021 budget ▪ Substantial UPS renewal identified in 2021 budget ▪ Status of switches unknown Telephone system replacement critical ▪ CCTV infrastructure mostly standardised	▪ Limited range of user devices that best meet user needs ▪ New telephone infrastructure		Assess user needs and scan products available	1-5
			Issue RFT for replacement telephone system	1
			Collate CCTV equipment age profile	2
On-premise main server critical to core systems: ▪ Refreshed in 2019 ▪ Unsure of ability to shut-down and re-start Storage not entirely in control: ▪ Corporate drive is a mess driving storage demand ▪ Unlimited e-mail storage for users ▪ No forecast of future storage demand	Server right-sized to evolving requirement. Ability to forecast and manage storage requirements	Server blueprint	Engage consultant to model processing and storage requirements with alternative SaaS adoption scenarios	2-3
	Server room relocated to Depot		Determine Depot accommodation requirement	1
			Develop server relocation plan	2
	Safe server shut-down and re-start ability: ▪ Manually ▪ Automatically during power outage		Implement APC Powerchute	1
			Documented and tested shut-down and re-start procedure	1
	Clean and controlled storage	Corporate data clean-up	Develop IOP for corporate drive data retention and disposal	1-2
			Corporate drive data clean-up	1-2

As-Is	To-Be	Bridging the Gap	Actions	Timeframe (Year)
Significant expenditure on hardware warranties / maintenance agreements	Optimal use of warranties / maintenance agreements	Warranties / maintenance agreements review	Develop ICT warranties / maintenance agreement position paper: ▪ Identify warranties currently in place and review agreements ▪ Review relevant consumer legislation ▪ Canvass views from other organisations	3
Telephony				
Telephone system and desktop handsets urgently need replacing	New phone system and handsets: ▪ System is compatible with future office technologies that may be adopted ▪ Adequate redundancy to provide internal calling capability in event of internet outage	Telephone system replacement	Procure replacement phone system and handsets	1
Telephone communications is internet based				
Passive messaging to community via social media	▪ Targeted push messaging via text messaging	Mobile device utilisation	Assess community (and staff) appetite for receiving text notifications and nature of message	3-4
Town owns a collection of mobile phones of different	Cost effective provision of mobile phones that meets user needs		Investigate implication and feasibility of bring your own option	2-3

As-Is	To-Be	Bridging the Gap	Actions	Timeframe (Year)
models and ages, some of which are unused			Formalise mobile phone eligibility criteria	1-2

Business Continuity

As-Is	To-Be	Bridging the Gap	Actions	Timeframe (Year)
Disaster Recovery (DR) back-up site at Depot ▪ Creates additional system administration effort ▪ Covers critical systems only ▪ Currently relies on 7 day back-up tape ▪ Evolving to twice daily replication ▪ Untested	Documented and tested DR solution	Documented and tested DR solution	Complete documentation and test Depot DR solution Continued adoption of SaaS	1
	Simplified on-premise DR infrastructure	On-premise DR infrastructure	Continued migration to SaaS for various applications	3-4
	Minimum ICT capacity in event of internet outage		Determine business systems and applications that can be made available from on-premise server during internet outage Ensure required on-premise server and storage capacity in place	2-4 1
	Mainstream cloud based DR solution	Cloud DR	Investigate cloud DR solution in context of software system and application renewals and replacement	1-3
Proven capacity for staff to work off-site and communicate effectively	Current remote working plan and instructions	Documented and tested DR solution	Develop IOP for working remotely	1-2

Security

As-Is	To-Be	Bridging the Gap	Actions	Timeframe (Year)
No formal cybersecurity plan	Formal cybersecurity plan	Cybersecurity posture using recognised framework	Engage cybersecurity consultant	1
			Conduct cybersecurity audit	1
			Develop and implement cyber security plan	1
			Install software security updates as they become available	1-5
Limited understanding of cybersecurity	Annual penetration testing		Conduct annual penetration tests	1-5
Firewall security (SonicWall)	Reporting on security breach attempts	Utilisation of firewall and anti-virus software	Implement firewall reporting functionality	1
Regularly updated anit-virus software (ESET)	Up to date security software		Ensure timely installation of security updates	1-5
	Cost effective security software		Review firewall and anti-virus solutions	2-3
Regular staff awareness via Friday Facts	Informed and vigilant staff	Staff education	Continue Friday Facts information sharing	1-5
			Include information in on-line induction	2-3
Automated password renewal	Enforced minimum password standards	Effective user authentication	Purchase password software	1
	Two factor authentication		Investigate two factor authentication	2-3

APPENDIX 2: ICT DETAILED RISK ASSESSMENT

Risk	1. Cyberattack – loss of service
Likelihood	Possible
Consequence	Major
Impact	Mitigation
▪ Denial of server based services, all systems become unavailable	▪ Up to date firewall and anti-virus protection ▪ Monitor incursion attempts at firewall ▪ DR site to reinstate critical processes if not impacted ▪ Tape back-up to restore data from ▪ Increase use of SaaS provides access to vendor's protection and DR

Risk	2. Prolonged loss of local network communications
Likelihood	Unlikely
Consequence	Major
Impact	Mitigation
▪ Server based business systems and applications and data not available from Civic servers ▪ Loss of e-mail between sites ▪ Loss of internet access for most sites ▪ Loss of CCTV service	▪ Redundant communication links between critical sites ▪ Depot operate from DR servers ▪ Internet access point at Depot (future state) ▪ CCTV has three servers and independent communications links that operate independently. Footage loss limited to failed link

Risk	3. Prolonged server outage
Likelihood	Unlikely
Consequence	Major
Impact	Mitigation
▪ Server based business systems and applications and data not available from Civic servers ▪ Loss of e-mail between sites ▪ Loss of internet access for most sites ▪ Loss of CCTV service	▪ Replicated DR server at Depot for critical systems ▪ Ability to physically rearrange servers between sites and reconfigure virtual servers ▪ Tape back-up of critical data every 7 days and entire system every 30 days ▪ Libraries, Stadium, JD Hardie and Landfill customer systems SaaS ▪ CCTV system has three parts, each hosted on a separate server

Risk	4. Prolonged loss of internet communications
Likelihood	Rare / Unlikely
Consequence	Moderate / Major
Impact	Mitigation
▪ Unable to make external phone calls ▪ Loss of SaaS business systems and applications ▪ Loss of access to other internet based resources	▪ Enterprise grade internet connection ▪ Internet access point at Depot (future state)

Risk	5. Obsolete business system or application
Likelihood	Likely
Consequence	Moderate
Impact	Mitigation
▪ Unavailability of system support to pursue enhancements or remediate issues ▪ Missed opportunities for process improvement and efficiency gains ▪ Staff frustration from working with an inadequate system	▪ ICT strategy and asset management plan to holistically guide ICT investment and renewals ▪ Maintain awareness of business systems and applications development

Risk	6. Under investment in ICT
Likelihood	Likely
Consequence	Moderate
Impact	Mitigation
▪ Increased risk of equipment failure as it ages ▪ Increased difficulty maintaining equipment as it ages ▪ Reduced reliability of lower quality equipment ▪ Growing bow wave of catch-up investment required ▪ Legacy hardware has higher on-going cost compared to newer hardware ▪ Systems software and business systems and applications become unsupported ▪ Missed opportunities for business process improvements that are enabled by new devices or systems and applications ▪ Missed opportunities for improved delivery of community services ▪ Staff disenfranchised by below-par ICT tools	▪ Implement ICT strategy and asset management plan ▪ Select equipment of suitable quality to match pre-defined lifespan ▪ Understand current software suite and remain abreast of developments in those areas

Risk	7. Over investment in ICT
Likelihood	Unlikely
Consequence	Minor

Impact	Mitigation
▪ Higher acquisition cost of over-specified hardware ▪ Higher on-going maintenance costs ▪ Higher on-going training costs ▪ Increased likelihood of underutilisation of ICT assets ▪ Inefficient use of Town funds	▪ Implement ICT strategy and asset management plan ▪ Select equipment of suitable quality to match pre-defined lifespan ▪ Review change management implications for new business systems and application acquisitions ▪ Wait for technologies to be proven ▪ Centrally co-ordinate ICT investment

Risk	8. Data theft
Likelihood	Possible
Consequence	Moderate
Impact	Mitigation
▪ Confidential data may be used for harmful purposes ▪ Non-compliance with various obligations ▪ Damage to Town's reputation	▪ Password protection ▪ Up to date firewall and anti-virus protection ▪ Monitor incursion attempts at firewall

Risk	9. Prolonged telephone system outage
Likelihood	Possible
Consequence	Moderate
Impact	Mitigation
▪ Loss of telephony internally and externally ▪ System is obsolete increasing likelihood of delayed return to service	▪ Maintenance support arrangement in place for telephone system ▪ Some spare handsets held ▪ Replace system ▪ Utilise existing after hours call centre to manage incoming calls ▪ Utilise mobile phones

Risk	10. Staff turnover
Likelihood	Almost certain
Consequence	Moderate
Impact	Mitigation
▪ ICT support staff: ▪ Loss of system and network knowledge ▪ Loss of key contractor and vendor relationships ▪ Staff: ▪ Loss of business system and applications use knowledge ▪ Advocate for software applications they are familiar with ▪ Loss of knowledge regarding data storage ▪ Derails ICT project implementations	▪ Utilisation of external contractors who also maintain intimate system and network knowledge ▪ Documentation of ICT processes ▪ Utilise business systems and applications that are common in local government ▪ Retain vanilla software configurations ▪ IOP for applications software acquisition and management ▪ Disciplined approach to data management ▪ Utilise external consultants on ICT implementations

APPENDIX 3: RISK MATRIX

Measures of Likelihood

Level	Likelihood	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances	More than once per year
4	Likely	The event will probably occur in most circumstances	At least once per year
3	Possible	The event should occur at some time	At least once in 3 years
2	Unlikely	The event could occur at some time	At least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	Less than once in 15 years

Risk Matrix

Consequence Likelihood		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost Certain	5	5	10	15	20	25
Likely	4	4	8	12	16	20
Possible	3	3	6	9	12	15
Unlikely	2	2	4	6	8	10
Rare	1	1	2	3	4	5

1-4	Low	5-9	Moderate	10-16	High	17-25	Extreme

Town of
Port Hedland

13 McGregor Street
Port Hedland 6721

08 9158 9300
council@porthedland.wa.gov.au
www.porthedland.wa.gov.au