Town of
Port Hedland

ATTACHMENTS

Under Separate Cover

Audit, Risk and Compliance Committee
Meeting
Tuesday, 8 March 2022

Table of Contents

William Buck
CHARTERED ACCOUNTANTS & ADVISORS

INTERNAL AUDIT REVIEW OF RECORDS MANAGEMENT

NOVEMBER 2021

This report, including management actions and implementation timeframes, were agreed with and accepted by:

Name:	Karren MacClure
Title:	Director Corporate Services, Town of Port Hedland
Date:	15-12-2021.
Signature:	

Name:	Carl Askew
Title:	Chief Executive Officer, Town of Port Hedland
Date:	15.12.2021
Signature:	

TABLE OF CONTENTS

Executive Summary

Introduction

As part of the internal audit programme William Buck Consulting (WA) Pty Ltd was asked to conduct a review of controls implemented in respect of the effectiveness of the record management processes in place at the Town of Port Hedland ("Town").

Scope

The review focussed on the controls in place on a high level, relating to the following business objectives:

- Record Keeping Plan is aligned with the *State Records Act 2000* (SRA) and has been reviewed and approved by the State Records Office;
- Record keeping processes and documents are in place to ensure compliance at a high level with the SRA including Record Keeping Plan, Metadata Management Policy, Thesaurus and Retention, managing digital information and Disposal Plan and key requirements are complied with;
- Staff are aware and adhering to record keeping responsibilities under the SRA and Record Management practices at the Town and sufficient, appropriate, and fit for purpose procedures exist to guide the process;
- Consistent approach to record keeping requirements across the organisation;
- Appropriate quality control processes are implemented in respect of Records Management;
- Access to records is appropriately controlled either through a system or hard copy records;
- Record audits are performed by the Records Officer e.g., frequency, results, and follow-up;
- Disposal/destruction of both electronic and paper-based records are aligned to the General Disposal Authority for Local Government Records (GDA), by either staff or records;
- Appropriate controls are implemented to mitigate any key findings, which also might be applicable to the Town, set out in the Office of the Auditor-General's performance reports issued on Records Management which includes lack of policies and procedures, currency and approval of Record Keeping Plan, poor implementation of Record Keeping Plan, inadequate trainings on record keeping, limited monitoring of staff records management practices, records management, storage of records, inadequate protection of records, disaster recovery planning etc.;
- Effectiveness of controls for a centralised process for all incoming and outgoing records (e.g., mail); and
- Record Keeping Systems are compliant with the SRA and Record Management practices at the Town.

We selected the following operational areas to perform our testing:

- Accounting;
- Governance;
- Human Resources;
- Projects; and
- Information Technology.

We also noted that the Town was in the process of evaluating a new Enterprise Resource Planning (ERP) Software which will also include the record management system.

Overall comment & findings

Overall, based on the work we have performed, we have identified 5 high and 5 medium rated findings in relation to the basic design and operation of processes in respect to records management which include the following:

- Data and records stored outside the Records Management System and hard copies of records require transfer to the Town's Record Keeping System (Synergy).
- Record Management System has several inactive files for different departments and review and reconciliation procedures needed for inactive files still needs to be documented.
- Improvement opportunities identified around the disposal of records.
- The Record Keeping Plan requires alignment to the current organisational structure.
- Various computer applications were not integrated to the Records Management System. Specific guidelines which are aligned with record keeping requirements for the different departments were not in place. A new computer application system acquired without considering the integration plan.
- Systematic approach to Record Management System (Synergy) implementation, change management, data security controls and business continuity testing was not evidenced.

- Mail handling procedures and file movement procedures require improvement.
- Consistent and programmed approach to the records audit and quality assurance was not followed.
- Consistent and programmed approach for the records audit was not evidenced.
- Records Management Procedures are not timely reviewed.

Distribution and rating of observation with regards to operational areas is tabulated below. Risk Rating is based on risk rating approach stated on pages 19-20 of this report.

Area	Extreme	High	Medium	Total
Policies and Procedures	-	1	1	2
Record Keeping Plan.	-	-	1	1
Approach to Record Keeping.	-	-	1	1
Disposal of Records.	-	-	1	1
Record Keeping System.	-	2	-	2
Mail Handling and File Movement.	-	1	-	1
Handling Vital Record.	-	1	-	1
Records Audit and Quality Assurance.	-	-	1	1
Total	-	5	5	10

Detailed findings can be found within the following section.

Detailed Findings

1. Records stored outside the Records Management System and other hard copies require transfer to the formal record keeping system:

Rating Calculation
Consequence = Major
Likelihood = Likely

Overall Risk Rating		
Extreme	High	Medium

Observations

It was noted that a large amount of data and physical records were maintained outside the Town's Record Keeping System (Synergy). Our findings for each of the operational area we tested are noted below:

a) **Accounting and payroll data:** In response to our inquiry the finance team confirmed that the following data is currently still stored outside the record keeping system:

i. Working papers and spread sheets for the budget template, other similar worksheets, and sundry items.
ii. The Town outsourced payroll processing for 3 months and then reverted to internal payroll processing. Payroll information for three months of outsourced processing is stored in hardcopy form with the records management department.
iii. Timesheets for the payroll stored in boxes at the records department. These time sheets are digitally scanned and also stored on a computer drive.

The Finance team confirmed that the files are currently stored on computer hard drives outside the record management system have necessary access controls and are backed up regularly. It was however, noted that list of files stored on computer drives outside the record keeping system was not available to ensure the completeness of the data.

b) **Human Resources:** A meeting was held with the Human Resources Manager, and we noted the following:

i. The present Human Resources Manager took charge in April 2020 and a formal handover did not take place on the assumption of duties, hence the completeness of records not ensured.
ii. A large amount of data was stored on outside the records management system which included employment contracts, termination, disciplinary actions, and other relevant records. The Human Resources Department expressed their concerns over security in relation to the Records Management System (Synergy); however, no incident of compromise was notified to us.
iii. Human Resources only record some basic documents in the records management system. A sample of 5 employees records were tested and these were yet to be recorded in the records management system.
iv. Complete list of the files stored outside the Records Management System were not in place to confirm the completeness.
v. Although recruitment and training are managed through independent systems data is currently saved on outside the record keeping system.
vi. Some physical records were also stored at the Town's civic centre, however a list of such records was not maintained to ensure completeness and safeguarding of important records.

c) **Human Resources-Work Health and Safety (WHS):** Testing in Human Resources also covered WHS. The following observations were noted:

i. Several claim files were kept in a steel cabinet. In some files the record was not retained in an organised manner. Scanned copies of these files were also digitally saved outside the Record Management System, however, were not part of the Record Management System (Synergy).
ii. Some claim files were old. The following samples were noted as evidence of files not made part of the record management system:

Claim Number	Date
0000028073	22 January 2019
00000028930	28 February 2020

The Human Resources team confirmed that the data and documents stored outside the Records Management System are safeguarded by appropriate access controls which include access controls over outside the Records Management System and periodical data back-ups.

d) **Projects and Infrastructure services**: Two meetings were held with the Manager Infrastructure Project and Assets. The following observations were noted:

i. Asset registers and projects data was saved outside the Records Management System. Data was not part of the Record Management System (Synergy).
ii. Existence of the following controls around data outside the Records Management System was not confirmed:

a. Physical and access controls.
b. Data back-up.
c. List of data to ensure completion and safeguarding.

Reasons for not transferring this data to the Record Keeping System and the existence of documented plans for making this data part of the record keeping system was not provided.

Recommendations

It is recommended that all the data and the hardcopy records should be made part of the records keeping system. A documented plan should be prepared and approved for each of the department carrying data outside the Record Keeping System (Synergy).

a) **Accounting and payroll data:**

i. A formal strategy should be prepared and implemented to ensure that all the computer data and physical files are made part of the record keeping system.
ii. List of files and data outside the records keeping system, should be prepared. A periodical review and reconciliation procedures for such data and files should be implemented, until the time these records become part of the Town's formal record keeping system.

b) **Human Resources**

i. A formal strategy should be prepared and implemented to ensure that all the computer data and physical files are made part of the record keeping system.
ii. List of files and data outside the records keeping system, should be prepared. A periodical review and reconciliation procedures for such data and files should be implemented, until the time these records become part of the Town's formal record keeping system.

c) **Human Resources- Work Health and Safety (WHS):**

i. A formal strategy should be prepared and implemented to ensure that all the computer data and physical files are made part of the record keeping system.
ii. List of files and data outside the records keeping system, should be prepared. A periodical review and reconciliation procedures for such data and files should be implemented, until the time these records become part of the Town's formal record keeping system.

d) **Projects and Infrastructure services:**

i. A formal strategy should be prepared and implemented to ensure that all the computer data and physical files are made part of the record keeping system.
ii. List of files and data outside the records keeping system, should be prepared. A periodical review and reconciliation procedures for such data and files should be implemented, until the time these records become part of the Town's formal record keeping system.

Management Comment, Timeframe & Responsibility

a) **Accounting and payroll data:**

Action agreed by management	i. Management agrees with the audit observation. A formal strategy will be implemented by June 2023. ii. Management agrees with the audit observation. A list of files and data will be created by June 2023. A periodical review and reconciliation process will be defined by the targeted date.
Action Owner	Manager Financial Services
Target Date	30 June 2023

b) Human Resources:

Action agreed by management	i. Management agrees with the audit observation. A formal strategy will be implemented by June 2023. ii. Management agrees with the audit observation. A list of files and data will be created by June 2023. A periodical review and reconciliation process will be defined by the targeted date.
Action Owner	Manager Human Resources
Target Date	30 June 2023

c) Human Resources-Work Health and Safety (WHS):

Action agreed by management	i. Management agrees with the audit observation. A formal strategy will be implemented by June 2023. ii. Management agrees with the audit observation. A list of files and data will be created by June 2023. A periodical review and reconciliation process will be defined by the targeted date.
Action Owner	Manager Human Resources Senior Records Officer
Target Date	30 June 2023

d) Projects and Infrastructure services:

Action agreed by management	i. Management agrees with the audit observation. A formal strategy will be implemented by June 2023. ii. The Town will review and formalise its current processes. A periodical review and reconciliation process will be defined by the target date.
Action Owner	Manager Infrastructure Projects and Assets
Target Date	30 June 2023

2. Review and Reconciliation procedures needed for inactive files in the Record Keeping System

Rating Calculation
Consequence = Moderate
Likelihood = Possible

Overall Risk Rating		
Extreme	High	Medium

Observation

Files are opened in the record management system for saving the documents digitally. The files act as a container to the documents of similar nature. These files are opened by the Records Management Team on the request raised by the respective departments. Different level of access rights can be defined for such files. We obtained a sample of 100 files for each of the operational areas we tested for this control and noted that several files were inactive. The test summary is noted below:

S.No	Operational Area	Number of Inactive Files out of 100	Operational Area Manager Comments
1	**Finance**	**45**	**Files are inactive as they are no longer used. Reasons for inactivity may include old/project completed.** **Majority of these files cover all day-to-day records requirements. New ones established on a need basis only.** **This status was assessed by the current Manager Financial Services, and these meet the current Record Keeping Plan requirements.**
2	Governance	60	The Governance team has not been made aware of this list or responsibilities with respect to managing files at the time of review.

S.No	Operational Area	Number of Inactive Files out of 100	Operational Area Manager Comments
3	Projects and Infrastructure Services	54	Response not received.

The file opening form require checks for existence of a duplicate file, however, we noted that periodical review controls were not in place to ensure that:

- the existing files are correctly utilised, and
- the new files are opened only when a legitimate need arise i.e., for new projects or key new operational aspect etc.

As part of our review, we noted that the record department identified instances of use of incorrect files for saving the documents. Using the incorrect files also impact the document search capability and security of files on the system.

Recommendations

It is recommended that procedures should be improved to ensure periodical review and follow up mechanism is implemented. This should cover ensuring that:

i. Current folders are being utilised correctly.
ii. Inactive folders are reviewed for disposal in line with the Record Keeping Plan and the statutory plan.
iii. Inactive files not to be used in future are timely identified, to prevent the possibility of incorrect record keeping.
iv. Closure or reallocation of inactive files no longer needed by a certain department.

Management Comment, Timeframe & Responsibility

Action agreed by management	Management agrees with the audit observation. A full review of the current Standard Operating Procedure (SOP) '*Closing Synergy Files*' will be performed to include adequate procedures for periodical review and follow-up processes, by the targeted date.
Action Owner	Senior Records Officer
Target Date	31 December 2022

3. Improvements required around Retention and Disposal

Rating Calculation
Consequence = Moderate
Likelihood = Possible

Overall Risk Rating		
Extreme	High	Medium

Observation

a) **Procedures require close alignment to General Disposal Authority for Local Government Record:** State Record Commission of Western Australia (SRC) Standard 2, defines the term disposal as follows:

"Disposal refers to the removal of records from the organisation once they have reached the inactive phase, and their subsequent destruction, or permanent retention at State archives".

SRC Standard 2, principle 5 – Retention and Disposal refers the Local Governments to use the General Disposal Authority for Local Governments (GDALG) for compliance of disposal requirements. GDALG specify in detail the records disposal requirements relevant to each of key operational areas within the local governments.

As part of our testing, different operational areas were requested to identify and confirm the processes in place to ensure the compliance of the GDALG. Each of the departments, was requested to respond on a few of the items selected from the General Disposal Authority. The following is the summary of responses received:

S.No	Operational Area	Operational Area Manager Comments
1	Finance	This is a large body of work with many items identified. Under current resourcing this cannot be responded to. General comment would be that most records are setup at records with destruction dates and the only items requested to be destroyed are payroll documents after 7 years of storage.
2	Governance	All files requiring disposal are provided to Records for that purpose.
3	Projects and Infrastructure Services	Response not received.

It was noted that the Town has several internal procedures addressing the disposal of records, however these require linkage to the specific department's requirements stated in the General Disposal Authority for Local Government Records.

b) **Improvements required in procedures for continuous assessment of the record keeping requirements on disposal:** Section 5 of the Town's Record Keeping Plan deals with the retention and disposal of records. The following status was included in the Record Keeping Plan at the time of submission for approval. We noted that after the initial approval, processes the periodical assessment of these requirements were not available as evidence that the processes were actively improved and the status of the requirements were regularly reviewed:

Requirement	Status at the time of submission
Restricted Access Archives	The Town of Port Hedland does not have any state archives to which it intends to restrict access when they are transferred to the SRO.
Transfer of Archives	An Archives Transfer Request form has not been submitted to the SRO. The Town of Port Hedland will transfer State archives to the State Archives Collection for permanent preservation when requested by the SRO.
Non-Transfer of Archives	SRC Standard 7: State Archives retained by Government Organisations provides for organisations to retain State archives older than 25 years. The Town of Port Hedland has not identified any State archives that will not be transferred to the SRO for permanent preservation.

Recommendation

a) **Procedures require close alignment to General Disposal Authority for Local Government Record:** The procedure document should be updated to align these with the specific requirement of the General Disposal Authority for Local Government Records. Procedures should be linked to the specific departments' requirements covered in the General Disposal Authority for Local Government Record.

b) **Improvements required in procedures for continuous assessment of the Record Keeping Requirements on Disposal:** Procedures should be updated to ensure the continuous assessment of the requirements of the record keeping requirements.

Management Comment, Timeframe & Responsibility

a) **Procedures require close alignment to General Disposal Authority for Local Government Record:**

Action agreed by management	Management agrees with the audit observation. An Internal Operating Procedure (IOP) for '*Retention and Disposal of Records*' will be developed, approved and implemented by December 2022. The audit recommendation will be taken into consideration.
Action Owner	Senior Records Officer
Target Date	31 December 2022

b) **Improvements required in procedures for continuous assessment of the Record Keeping Requirements on Disposal:**

Action agreed by management	Management agrees with the audit observation. An Internal Operating Procedure (IOP) for '*Retention and Disposal of Records*' will be developed, approved and implemented by December 2022. The audit recommendation will be taken into consideration.
Action Owner	Senior Records Officer
Target Date	31 December 2022

4. Record Keeping Plan require alignment to the current organisational structure:

Rating Calculation
Consequence =Moderate
Likelihood = Possible

Overall Risk Rating		
Extreme	High	🟨 Medium

Observation

Section 2 of the Record Keeping Plan specifies that "The creation and management of records is coordinated by the Town of Port Hedland's ICT Unit, which consists of two Departments, the Information Technology Department and the Records Department.

We noted that the organisational status specified in the Record Keeping Plan is not aligned to current set up. Section 28 (2) of the State Records Act 2000 requires that "A government organization must review its Record Keeping Plan whenever there is any significant change to the organization's functions". Evidence of assessment to revise the Record Keeping Plan was not witnessed. Furthermore, specific reasons for not updating the Record Keeping Plan were not provided in response to our inquiries.

We also noted, a formal documented service level agreement between the Records Keeping Department and the Information Technology Department was not in place to define the relevant roles and responsibilities and improving the coordination. In response to our inquiry the Information Technology team confirmed that no service level agreement existed between the two departments.

Recommendations

It is recommended that:

i. In view of organisational changes, assessment of the condition of review of Record Keeping Plan should be performed as mandated under the Records Keeping Act 2000.
ii. A documented service level agreement between the Records and Information Technology departments should be approved and implemented.

Management Comment, Timeframe & Responsibility

Action agreed by management	i. Management agrees with the observation and will undertake a full review of the current document '*Recordkeeping Plan*', taking into account the audit recommendation. ii. Management does not agree with implementing a Service Level Agreement (SLA). .
Action Owner	Senior Records Officer
Target Date	31 December 2022

5. Procedures require improvements to include specific guidance on computer applications not integrated with the Records Management System.

Rating Calculation
Consequence = Moderate
Likelihood = Likely

Overall Risk Rating		
Extreme	High	Medium

Observation

We noted that section 2.1.2 of the records keeping plan provides information on the "Business Information Systems" in use by the Town. Most of these systems were not integrated with the Record Keeping System "Synergy". We reviewed this information and obtained further clarifications on the integration status of these applications. Inquiries we made in relation to the following aspects:

- Information on status of the plans, if any, developed for integrating these systems with the Synergy.
- Any applications that have been discontinued for which the Record Keeping Plan require updating.
- New applications procured by the Town after the approval of the Record Keeping Plan which require integration to Synergy. We already identified two such applications i.e., Vendor Panel (Application for Procurement) and ACONEX (Application for Project Records).
- Existence of documented procedures to ensure that all the new systems/applications procured and implemented are assessed for the compliance of record keeping requirements and are included in the list of Business Information Systems as part of the Record Keeping Plan.

The following is the summary of applications and response received form management:

S. No	System *(Function)*	Response by Management
1	Autodesk *(CAD Drawings)*	No Further Comments.
2	Altus *(Online leave portal)*	The capability will be absorbed into the new ERP system and hence integrated with the new EDRMS.
3	AMLIB *(Library Management Software)-(being phasedout)*	No Longer in use.
4	Spydus *(Library ManagementSoftware)-(being introduced)*	No Further Comments.
5	Links Modular Solutions *(Leisure center management software)*	No Further Comments.
6	MOZAIC *Local history software (being phased out, Spydushas this capability)*	No Further Comments.
7	MAGIQ Performance Software Suite *(Budgeting and reporting)*	No Longer in use.
8	Trapeze Plan Manager *(Planning and scheduling software)*	No Further Comments.
9	Smart Sheet *(Spreadsheet database)*	No Further Comments.
10	ELMO *(Recruitment, on boarding,LMS and E-Learning course library*	The capability will be absorbed into the new ERP system and hence integrated with the new EDRMS.
11	Big Red Sky *(Recruitment portal)*	The capability will be absorbed into the new ERP system and hence integrated with the new EDRMS.

S. No	System *(Function)*	Response by Management
12	HUB *(Council dashboard)*	No Further Comments.
13	WALGA E Quotes *(Creation of briefs for purchasing and locatingpreferred suppliers)*	Vendor Panel. No further comments.

We noted that:

i. Business systems for 3 and 7 were discontinued. Processes were not witnessed to ensure that records and data in relation to these systems were made part of the Record Keeping System (Synergy) before discontinuance.

ii. Formal documented plans to integrate the existing business systems were not produced. Furthermore, formal plans guiding compliance with the record keeping requirements specific to each business system were not produced. It was explained that the Town was in the process of evaluating a new ERP solution. We noted that only the business systems at serial numbers 2, 10 and 11 above are confirmed to be absorbed in the new ERP system. Planning for integration for remaining systems was not confirmed.

iii. Documented processes ensuring that new business system procured are assessed for meeting the record keeping requirements, were not available. One such system procured by the projects team was a software namely "ACONEX". This was explained as a major project management tool which also preserve the records for projects. We noted that integration of this system with the record management system was not considered. Furthermore, operational plan to transfer the existing data of the projects, saved on the local computer and network drives to the ACONEX and the record keeping system was not in place.

Recommendation

It is recommended that:

i. Procedures should be developed to ensure that data and records for the discontinued systems becomes part of the record management system.

ii. Procedures specific to each of the business systems which are not integrated should be developed to ensure that data from these systems becomes part of the formal record management system. Periodical review and reconciliation processes should also be developed to ensure that data on systems, not integrated, becomes part of the record keeping system and to ensure the timely updating of records and ensuring completeness and security of the data at all times.

iii. Procedures should be developed to ensure that procurement of new business systems also incorporate recordkeeping plans and strategies to ensure integration with the record management system and/or compliance with the record keeping requirements.

Management Comment, Timeframe & Responsibility

Action agreed by management	i. An Internal Operating Procedure (IOP) for '*Retention and Disposal of Records*' will be developed, approved and implemented by December 2022. The audit recommendation will be taken into consideration. ii. Management disagrees with the audit observation as an overall process should be followed for implementation, not individual. iii. Same as point i above.
Action Owner	Senior Records Officer
Target Date	31 December 2022

6. Systematic approach to the record management system implementation, change management and data security controls not applied.

Rating Calculation
Consequence = Moderate
Likelihood = Likely

Overall Risk Rating		
Extreme	High	Medium

Observations

A formal change management approach to Synergy System was not applied: A formal change management process for the record management system was not in place. In the absence of a formal change management process, there is a risk that the changes and developments to the system, post implementation are not made in a structured and controlled manner. This could be one of the root causes of the current system Synergy not performing at the optimum level. Change management systems generally include the following processes:

i. Continuous evaluation of the system to identify the emerging needs to meet the business and regulatory requirements.
ii. Documented administrative procedures for:
    - Recording the change requests.
    - Independent assessment and approval of the changes.
    - Engaging the vendor changes.
    - Implementing changes and in the system.
    - User Acceptance Testing.
    - Rolling out the changes to live environment.
    - Retention of the change log for all the changes.

Adequate data security controls around the Synergy System were not in place: A high-level review was conducted to identify the data security controls around the Synergy System. The following is the

a) comparative summary of key controls and the information technology team responses.

Key Control	Information Technology Team Response
Monitoring user behaviour and activity and identification of threats	Users are not monitored.
Assessment of the environment for vulnerabilities and risks.	The environment is not regularly assessed.
Suspicious user activity is timely identified and uncovered.	There is no process in place to identify such activities.
Threats are timely responded.	There is no formal threat response process.

The above status demonstrates weak data security controls around the Synergy System.

b) **Synergy System not tested for Business Continuity and Disaster Recovery:** It was also noted that the Synergy System was not tested for Disaster Recovery and Business Continuity Planning.

Recommendations

Management informed us that the Town was in the process of evaluating a new ERP which will include a records management system as well. The following are our recommendations in this regard:

a) **A formal change management approach to Synergy System was not applied:** A formal change management process for the records management system should be implemented. A Log of all the changes to the record management system should be retained. This process should also be implemented for the new ERP system.

b) **Adequate data security controls around the Synergy System were not in place:** A formal data security risk assessment should be carried out and appropriate data security controls should be implemented for the existing as well as new ERP.

c) **Synergy System not tested for Business Continuity and Disaster Recovery:** Synergy system should be tested as part of the implementation of business continuity and disaster recovery planning. Implementation of the new ERP should also ensure the business continuity and disaster recovery testing.

Management Comment, Timeframe & Responsibility

a) A formal change management approach to Synergy System was not applied:

Action agreed by management	Management agrees with the audit observation. The Town will implement a Change Management process based on the principals of the ITIL framework by the end of financial year 2022/2023.
Action Owner	Manager of IT and Program Delivery
Target Date	30 June 2023

b) Adequate data security controls around the Synergy System were not in place:

Action agreed by management	Management agrees with the audit observation. The Town will undertake an IT Security Review by the end of the financial year 2022/2023.
Action Owner	Manager of IT and Program Delivery
Target Date	30 June 2023

c) Synergy System not tested for business continuity and disaster recovery:

Action agreed by management	Management agrees with the audit observation. The Town will develop a BCDR framework and processes for its IT systems. The framework will be developed by end of the financial year 2022/2023.
Action Owner	Manager of IT and Program Delivery
Target Date	30 June 2023

7. Mail handling and files movement procedures require improvements:

Rating Calculation
Consequence = Major
Likelihood = Likely

Overall Risk Rating		
Extreme	High	Medium

Observation

The Town has "opening Hard Copy Mail" Standard Operating Procedures in place as approved on 21 January 2019. We noted the following weaknesses in the procedures:

i. Customer services officers maintains a register to obtain acknowledgement of the mail handed over to concerned officers after scanning. Section 3 of the procedures specify the types of mail not to be opened by staff and such mail is to be handed over to the staff member responsible for the correspondence. We noted that mail received in the name of individuals is also not opened and scanned by the reception and delivered directly to the person without acknowledgement of receipt in the register. This is prone to risk as mail addressed to an individual may contain sensitive documents.

We also noted that procedure is not detailed on actions to be undertaken by the recipients of the mail which is not opened at the customer services desk and delivered directly to the persons.

ii. Section 7 of the procedures prescribe scanning of corporate documents and sending the scanned copies through email to the records team. Hard copies are required to be retained in the Source Record Box. The records are kept in the Source Record Box until it is full and then sent to the records team. The procedure does not prescribe:

- The Source Records Box is to be kept under a lock and key.
- Covering list of the documents placed in the Source Record Box is maintained, updated, and reviewed before and at the time of delivery of documents to the records team.
- Treatment of vital records.

In the absence of defined guidelines, there is a security risk to the documents.

iii. We also noted that duplicate title deed for Lot no 9008 on Deposited Plan 404824/Volume 2874 Folio 673 was lost. It was explained that the title deeds were provided to the Town's solicitor, who returned the title to the Town on 2 December 2020. The Towns legal advisor received the documents and after which it did not reach the records department. We noted that section 4.1.7 of the Record Keeping Plan specifies that when hardcopy files are requested the records team digitise the records and make them available through the corporate EDRMS. If the hardcopy original is required, it is loaned out to staff through the EDRMS and tracked via this module. We noted that a formal follow-up and tracking mechanism for loaned files was not in place.

Procedure document titled "Loans and Returns" was provided to us. This document specifies the procedure for loan of hard copies. Furthermore, section 8 of the document states the return procedure, however, procedure for periodical follow up of the loaned documents was not in place.

An Internal operating procedure on records management also exist which was last approved on 9 January 2019. Section 5 of this document provides guidance on borrowing of files. This guidance, however, does not include specific instructions of issuance of borrowed files to outsiders and follow up thereof and this could be the root cause for loss of title deeds.

Recommendation:

Procedures should be improved:

i. To ensure that all types of mail delivery should be acknowledged from the recipients on the mail distribution register. Procedures should include guidance and detailed responsibilities of the persons receiving the mail which is not opened at the customer services desk.

ii. To include guidance to:
   a. Keep the Source Records Box under lock and key.
   b. Covering sheet/list of the documents placed in the Source Records Box should be maintained for review and reconciliation at the time of delivery.
   c. Ensure immediate delivery of vital records to the records management team.

iii. To include follow-up and tracking mechanism. Furthermore, explicit guidance for the treatment of providing and receiving back the loan documents to the third parties should be included in the procedures. This may include approval of delivery of vital records to third parties and maintaining a register for follow up. Internal operating procedures "Records Management" should also be updated to include the guidance for follow up of loaned documents to outsiders.

Management Comment, Timeframe & Responsibility

Action agreed by management	i. Management agrees with the audit observation and will undertake a full review of the current Standard Operating Procedure (SOP) '*Opening Hard Copy Mail*', taking into account the audit recommendation. ii. Same as point i above. iii. Same as point i above.
Action Owner	Senior Records Officer
Target Date	31 December 2022

8. Adequate measures not implemented for the vital records:

Rating Calculation
Consequence = Major
Likelihood = Likely

Overall Risk Rating		
Extreme	High	Medium

Observation

Section 4.3.1 of the records keeping plan, lays down the requirements for the vital records wherein title deeds are also listed as a vital record. At the time of field visit it was noted that property documents were stored in an area at the civic centre of the Town. This storage space was not protected from fire and other risks to the records. On our inquiry it was informed by the records officer that these records were originally stored at the airport premises for which the lease was expired. It is noteworthy that section 4.4 of the Record Keeping Plan clearly specifies that lease for the airport was expiring in March 2019 and Town was reviewing the alternate storage requirements. Despite the fact this was a known fact requiring attention, timely actions were not undertaken, and the vital records were exposed to risks.

Recommendation

It is recommended that property files should be transferred to a location meeting the record keeping requirements.

Management Comment, Timeframe & Responsibility

Action agreed by management	Management confirms that all property files were transferred to the new centralised records facility at the Depot on 13 October 2021, a location meeting the record keeping requirements.
Action Owner	Senior Records Officer
Target Date	Completed 13 October 2021

9. Consistent and programmed approach of the records audit and quality assurance not evidenced.

Rating Calculation
Consequence = Moderate
Likelihood = Possible

Overall Risk Rating		
Extreme	High	Medium

Observation

Quarterly record audits for the vital records are specified under section 4.3.1 of the Record Keeping Plan. In response to our inquiry the records officer informed that the last records audit was performed by the Senior Records Officer in 2020, which remained incomplete.

We noted that a programmed approach to the records audit was not evidenced. Furthermore, a process for recording, escalating, and actioning the deviations was not in place.

Recommendation

It is recommended that records audit process should be implemented with documented guidelines to record, escalate, and actioning the exceptions.

Management Comment, Timeframe & Responsibility

Action agreed by management	Management agrees with the audit observation. A Standard Operating Procedure (SOP) will be developed, approved and implemented to formalise a process for auditing records, by the targeted date.
Action Owner	Senior Records Officer
Target Date	31 December 2022

10. Procedures are not timely reviewed.

Rating Calculation
Consequence = Moderate
Likelihood = Possible

Overall Risk Rating		
Extreme	High	Medium

Observation

We noted that following procedures were not timely reviewed:

Procedure	Review Frequency	Last Review Date
IOP- Records Management (For Employees)	Annually	9 January 2019
IOP- Records Management (For Elected Members)	Annually	10 January 2019
SOP-Bank Guarantees	Annually	22 January 2019
SOP-Opening Hard Copy Mail	Annually	21 January 2019
IOP-Destruction Request	Annually	24 June 2019
IOP-Process for Destroying Records	Annually	1 May 2020
IOP-Sentencing Records for Disposal	Annually	24 June 2019
SOP- Preparing Sentencing Sheets	Annually	24 May 2019

Recommendation

It is recommended that all the procedures should be timely reviewed and aligned to the current processes and regulatory requirements.

Management Comment, Timeframe & Responsibility

Action agreed by management	Management agrees with the audit observation. A full review on the following procedures will be undertaken by the targeted date: • IOP - Records Management (For Elected Members) • SOP - Bank Guarantees • SOP - Opening Hard Copy Mail • IOP - Destruction Request • IOP - Process for Destroying Records • IOP - Sentencing Records for Disposal • SOP - Preparing Sentencing Sheets
Action Owner	Senior Records Officer
Target Date	30 June 2023

Rating Criteria

Recommendations made in this report have been rated as Extreme, High, or Medium based on an assessment of underlying issues. The assessment was made by Internal Audit using predetermined criteria as outlined below. An issue may display one, all or a combination of the example attributes listed against the relevant rating.

LEVEL	RATING	FORESEEABLE	DESCRIPTION
E	Excellent	Doing more than what is reasonable under the circumstances	Existing controls exceed current legislated, regulatory and compliance requirements, and surpass relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation
A	Adequate	Doing what is reasonable under the circumstances	Existing controls are in accordance with current legislated, regulatory and compliance requirements, and are aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation
I	Inadequate	Not doing some or all things reasonable under the circumstances	Existing controls do not provide confidence that they meet current legislated, regulatory and compliance requirements, and may not be aligned with relevant and current standards, codes of practice, guidelines and industry benchmarks expected of this organisation

MEASURES OF CONSEQUENCE

LEVEL	1	2	3	4	5
RATING	Insignificant	Minor	Moderate	Major	Catastrophic
HEALTH	Negligible injuries	First aid injuries	Medical type injuries or Lost time injury < 5 days	Lost time injury > 5 days	Fatality, permanent disability
FINANCIAL IMPACT	Less than $3,000	$3,000 - $30,000	$30,001 - $300,000	$300,001 - $3M	More than $3M
SERVICE INTERRUPTION	No material service interruption	Temporary interruption to an activity – backlog cleared with existing resources	Interruption to Service Unit/(s) deliverables – backlog cleared by additional resources	Prolonged interruption of critical core service deliverables – additional resources; performance affected	Indeterminate prolonged interruption of critical core service deliverables – non-performance
COMPLIANCE	Occasional noticeable temporary non-compliances	Regular noticeable temporary non-compliances	Non-compliance with significant regulatory requirements imposed	Non-compliance results in termination of services or imposed penalties	Non-compliance results in criminal charges or significant damages or penalties
REPUTATION	Unsubstantiated, localised low impact on key stakeholder trust, low profile or no media item	Substantiated, localised impact on key stakeholder trust or low media item	Substantiated, public embarrassment, moderate impact on key stakeholder trust or moderate media profile	Substantiated, public embarrassment, widespread high impact on key stakeholder trust, high media profile, third party actions	Substantiated, public embarrassment, widespread loss of key stakeholder trust, high widespread multiple media profile, third party actions
ENVIRONMENT	Contained, reversible impact managed by on site response	Contained, reversible impact managed by internal response	Contained, reversible impact managed by external agencies	Uncontained, reversible impact managed by a coordinated response from external agencies	Uncontained, irreversible impact

MEASURES OF LIKELIHOOD

LEVEL	RATING	DESCRIPTION	FREQUENCY	PROBABILITY
5	Almost Certain	The event is expected to occur in most circumstances	More than once per year	Greater than 90% chance of occurrence
4	Likely	The event will probably occur in most circumstances	At least once per year	60% - 90% chance of occurrence
3	Possible	The event should occur at some time	At least once in 3 years	40% - 60% chance of occurrence
2	Unlikely	The event could occur at some time	At least once in 10 years	10% - 40% chance of occurrence
1	Rare	The event may only occur in exceptional circumstances	Less than once in 15 years	Less than 10% chance of occurrence

RISK MATRIX

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

RISK ACCEPTANCE CRITERIA

RISK RANK	LEVEL OF RISK	DESCRIPTION	CRITERIA FOR RISK ACCEPTANCE	RESPONSIBILITY
EXTREME	17 - 25	Urgent Attention Required	Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	CEO / Council
HIGH	10 – 16	Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Director / CEO
MEDIUM	5 – 9	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Operational Manager
LOW	1 – 4	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Operational Manager

Department of
Local Government, Sport
and Cultural Industries
GOVERNMENT OF
WESTERN AUSTRALIA

Port Hedland - Compliance Audit Return 2021

Certified Copy of Return

Please submit a signed copy to the Director General of the Department of Local Government, Sport and Cultural Industries together with a copy of the relevant minutes.

Commercial Enterprises by Local Governments

No	Reference	Question	Response	Comments	Respondent
1	s3.59(2)(a) F&G Regs 7,9,10	Has the local government prepared a business plan for each major trading undertaking that was not exempt in 2021?	N/A	The Town of Port Hedland has not entered into any major trading as defined in reg 9 LG (Functions & General) Regulations 1996 for the 2021 financial year.	Finance
2	s3.59(2)(b) F&G Regs 7,8A, 8, 10	Has the local government prepared a business plan for each major land transaction that was not exempt in 2021?	N/A	No major land transactions entered into in 2021.	Finance
3	s3.59(2)(c) F&G Regs 7,8A, 8,10	Has the local government prepared a business plan before entering into each land transaction that was preparatory to entry into a major land transaction in 2021?	N/A	No major land transactions entered into in 2021.	Finance
4	s3.59(4)	Has the local government complied with public notice and publishing requirements for each proposal to commence a major trading undertaking or enter into a major land transaction or a land transaction that is preparatory to a major land transaction for 2021?	N/A	No major land transactions entered into in 2021.	Finance
5	s3.59(5)	During 2021, did the council resolve to proceed with each major land transaction or trading undertaking by absolute majority?	N/A	The Town has not entered into any major trading for the 2021 financial year. Only properties sold were under the threshold.	Corporate Affairs

Delegation of Power/Duty

No	Reference	Question	Response	Comments	Respondent
1	s5.16	Were all delegations to committees resolved by absolute majority?	Yes		Governance
2	s5.16	Were all delegations to committees in writing?	Yes		Governance
3	s5.17	Were all delegations to committees within the limits specified in section 5.17?	Yes		Governance
4	s5.18	Were all delegations to committees recorded in a register of delegations?	Yes		Governance
5	s5.18	Has council reviewed delegations to its committees in the 2020/2021 financial year?	Yes		Governance
6	s5.42(1) & s5.43 Admin Reg 18G	Did the powers and duties delegated to the CEO exclude those listed in section 5.43 of the Act?	Yes		Governance
7	s5.42(1)	Were all delegations to the CEO resolved by an absolute majority?	Yes		Governance
8	s5.42(2)	Were all delegations to the CEO in writing?	Yes		Governance
9	s5.44(2)	Were all delegations by the CEO to any employee in writing?	Yes		Governance
10	s5.16(3)(b) & s5.45(1)(b)	Were all decisions by the council to amend or revoke a delegation made by absolute majority?	Yes		Governance
11	s5.46(1)	Has the CEO kept a register of all delegations made under Division 4 of the Act to the CEO and to employees?	Yes		Governance
12	s5.46(2)	Were all delegations made under Division 4 of the Act reviewed by the delegator at least once during the 2020/2021 financial year?	Yes		Governance
13	s5.46(3) Admin Reg 19	Did all persons exercising a delegated power or duty under the Act keep, on all occasions, a written record in accordance with Admin Reg 19?	Yes		Governance

Disclosure of Interest

No	Reference	Question	Response	Comments	Respondent
1	s5.67	Where a council member disclosed an interest in a matter and did not have participation approval under sections 5.68 or 5.69, did the council member ensure that they did not remain present to participate in discussion or decision making relating to the matter?	Yes		Governance

No	Reference	Question	Response	Comments	Respondent
2	s5.68(2) & s5.69 (5) Admin Reg 21A	Were all decisions regarding participation approval, including the extent of participation allowed and, where relevant, the information required by Admin Reg 21A, recorded in the minutes of the relevant council or committee meeting?	Yes		Governance
3	s5.73	Were disclosures under section sections 5.65, 5.70 or 5.71A(3) recorded in the minutes of the meeting at which the disclosures were made?	Yes		Governance
4	s5.75 Admin Reg 22, Form 2	Was a primary return in the prescribed form lodged by all relevant persons within three months of their start day?	Yes		Governance
5	s5.76 Admin Reg 23, Form 3	Was an annual return in the prescribed form lodged by all relevant persons by 31 August 2021?	Yes		Governance
6	s5.77	On receipt of a primary or annual return, did the CEO, or the mayor/president, give written acknowledgment of having received the return?	Yes		Governance
7	s5.88(1) & (2)(a)	Did the CEO keep a register of financial interests which contained the returns lodged under sections 5.75 and 5.76?	Yes		Governance
8	s5.88(1) & (2)(b) Admin Reg 28	Did the CEO keep a register of financial interests which contained a record of disclosures made under sections 5.65, 5.70, 5.71 and 5.71A, in the form prescribed in Admin Reg 28?	Yes		Governance
9	s5.88(3)	When a person ceased to be a person required to lodge a return under sections 5.75 and 5.76, did the CEO remove from the register all returns relating to that person?	Yes		Governance
10	s5.88(4)	Have all returns removed from the register in accordance with section 5.88(3) been kept for a period of at least five years after the person who lodged the return(s) ceased to be a person required to lodge a return?	Yes		Governance
11	s5.89A(1), (2) & (3) Admin Reg 28A	Did the CEO keep a register of gifts which contained a record of disclosures made under sections 5.87A and 5.87B, in the form prescribed in Admin Reg 28A?	Yes		Governance
12	s5.89A(5) & (5A)	Did the CEO publish an up-to-date version of the gift register on the local government’s website?	Yes		Governance
13	s5.89A(6)	When a person ceases to be a person who is required to make a disclosure under section 5.87A or 5.87B, did the CEO remove from the register all records relating to that person?	Yes		Governance

No	Reference	Question	Response	Comments	Respondent
14	s5.89A(7)	Have copies of all records removed from the register under section 5.89A (6) been kept for a period of at least five years after the person ceases to be a person required to make a disclosure?	Yes		Governance
15	Rules of Conduct Reg 11(1), (2) & (4)	Where a council member had an interest that could, or could reasonably be perceived to, adversely affect the impartiality of the person, did they disclose the interest in accordance with Rules of Conduct Reg 11(2)?* *Question not applicable after 2 Feb 2021	N/A		N/A
16	Rules of Conduct Reg 11(6)	Where a council member disclosed an interest under Rules of Conduct Reg 11(2) was the nature of the interest recorded in the minutes?* *Question not applicable after 2 Feb 2021	N/A		N/A
17	s5.70(2) & (3)	Where an employee had an interest in any matter in respect of which the employee provided advice or a report directly to council or a committee, did that person disclose the nature and extent of that interest when giving the advice or report?	N/A	Nil employees had an interest to declare in respect to a report they provided advice on.	Governance
18	s5.71A & s5.71B (5)	Where council applied to the Minister to allow the CEO to provide advice or a report to which a disclosure under s5.71A(1) relates, did the application include details of the nature of the interest disclosed and any other information required by the Minister for the purposes of the application?	N/A	N/A	Governance
19	s5.71B(6) & s5.71B(7)	Was any decision made by the Minister under subsection 5.71B(6) recorded in the minutes of the council meeting at which the decision was considered?	N/A	N/A	Governance
20	s5.103 Admin Regs 34B & 34C	Has the local government adopted a code of conduct in accordance with Admin Regs 34B and 34C to be observed by council members, committee members and employees?* *Question not applicable after 2 Feb 2021	N/A		N/A
21	Admin Reg 34B(5)	Has the CEO kept a register of notifiable gifts in accordance with Admin Reg 34B(5)?* *Question not applicable after 2 Feb 2021	N/A		N/A

No	Reference	Question	Response	Comments	Respondent
22	s5.104(1)	Did the local government prepare and adopt, by absolute majority, a code of conduct to be observed by council members, committee members and candidates within 3 months of the prescribed model code of conduct coming into operation (3 February 2021)?	Yes		Governance
23	s5.104(3) & (4)	Did the local government adopt additional requirements in addition to the model code of conduct? If yes, does it comply with section 5.104(3) and (4)?	Yes		Governance
24	s5.104(7)	Did the CEO publish an up-to-date version of the adopted code of conduct on the local government's website?	Yes		Governance
25	s5.51A(1) & (3)	Did the CEO prepare, and implement and publish an up-to-date version on the local government's website, a code of conduct to be observed by employees of the local government?	No	A revised Town of Port Hedland Code of Conduct for employees has been drafted and is awaiting publication.	Governance

Disposal of Property

No	Reference	Question	Response	Comments	Respondent
1	s3.58(3)	Where the local government disposed of property other than by public auction or tender, did it dispose of the property in accordance with section 3.58(3) (unless section 3.58(5) applies)?	Yes		Finance Corporate Affairs
2	s3.58(4)	Where the local government disposed of property under section 3.58(3), did it provide details, as prescribed by section 3.58(4), in the required local public notice for each disposal of property?	Yes		Finance Corporate Affairs

Elections

No	Reference	Question	Response	Comments	Respondent
1	Elect Regs 30G(1) & (2)	Did the CEO establish and maintain an electoral gift register and ensure that all disclosure of gifts forms completed by candidates and donors and received by the CEO were placed on the electoral gift register at the time of receipt by the CEO and in a manner that clearly identifies and distinguishes the forms relating to each candidate?	Yes		Governance
2	Elect Regs 30G(3) & (4)	Did the CEO remove any disclosure of gifts forms relating to an unsuccessful candidate, or a successful candidate that completed their term of office, from the electoral gift register, and retain those forms separately for a period of at least two years?	Yes		Governance
3	Elect Regs 30G(5) & (6)	Did the CEO publish an up-to-date version of the electoral gift register on the local government's official website in accordance with Elect Reg 30G(6)?	No	An up to date register of electoral gifts was displayed on the Town of Port Hedland's website. The register was not compliant with reg 30G (6) as the full address of the individual was published, not solely the suburb/town as per reg 30G(6). The register has been updated to align with reg 30G(6).	Governance

Finance

No	Reference	Question	Response	Comments	Respondent
1	s7.1A	Has the local government established an audit committee and appointed members by absolute majority in accordance with section 7.1A of the Act?	Yes		Governance
2	s7.1B	Where the council delegated to its audit committee any powers or duties under Part 7 of the Act, did it do so by absolute majority?	Yes		Governance
3	s7.9(1)	Was the auditor’s report for the financial year ended 30 June 2021 received by the local government by 31 December 2021?	Yes		Finance
4	s7.12A(3)	Where the local government determined that matters raised in the auditor’s report prepared under s7.9 (1) of the Act required action to be taken, did the local government ensure that appropriate action was undertaken in respect of those matters?	Yes		Finance
5	s7.12A(4)(a) & (4)(b)	Where matters identified as significant were reported in the auditor’s report, did the local government prepare a report that stated what action the local government had taken or intended to take with respect to each of those matters? Was a copy of the report given to the Minister within three months of the audit report being received by the local government?	Yes		Finance
6	s7.12A(5)	Within 14 days after the local government gave a report to the Minister under s7.12A(4)(b), did the CEO publish a copy of the report on the local government’s official website?	Yes		Finance
7	Audit Reg 10(1)	Was the auditor’s report for the financial year ending 30 June received by the local government within 30 days of completion of the audit?	Yes		Finance

Integrated Planning and Reporting

No	Reference	Question	Response	Comments	Respondent
1	Admin Reg 19C	Has the local government adopted by absolute majority a strategic community plan? If Yes, please provide the adoption date or the date of the most recent review in the Comments section?	Yes	The Council adopted the Strategic Community Plan 2018 - 2028 by absolute majority on 23/05/2018 (Decision #OCM201718/205).	Governance
2	Admin Reg 19DA (1) & (4)	Has the local government adopted by absolute majority a corporate business plan? If Yes, please provide the adoption date or the date of the most recent review in the Comments section?	Yes	The Council adopted the Corporate Business Plan 2018 - 2022 by absolute majority on 24/10/2018 (Decision #OCM201819/067).	Governance
3	Admin Reg 19DA (2) & (3)	Does the corporate business plan comply with the requirements of Admin Reg 19DA(2) & (3)?	Yes		Governance

Local Government Employees

No	Reference	Question	Response	Comments	Respondent
1	Admin Reg 18C	Did the local government approve a process to be used for the selection and appointment of the CEO before the position of CEO was advertised?	N/A	The CEO was appointed in 2019.	Human Resources
2	s5.36(4) & s5.37 (3) Admin Reg 18A	Were all CEO and/or senior employee vacancies advertised in accordance with Admin Reg 18A?	N/A	No CEO or senior employee vacancies were advertised during 2021. All positions were filled from 2020 or prior.	Human Resources
3	Admin Reg 18E	Was all information provided in applications for the position of CEO true and accurate?	N/A	The CEO was appointed in December 2019 and commenced in February 2020.	Human Resources
4	Admin Reg 18F	Was the remuneration and other benefits paid to a CEO on appointment the same remuneration and benefits advertised for the position under section 5.36(4)?	N/A	The CEO was appointed in 2019.	Human Resources
5	s5.37(2)	Did the CEO inform council of each proposal to employ or dismiss senior employee?	N/A	N/A	Human Resources
6	s5.37(2)	Where council rejected a CEO's recommendation to employ or dismiss a senior employee, did it inform the CEO of the reasons for doing so?	N/A	N/A	Human Resources

Official Conduct

No	Reference	Question	Response	Comments	Respondent
1	s5.120	Has the local government designated a senior employee as defined by section 5.37 to be its complaints officer?	Yes		Governance
2	s5.121(1) & (2)	Has the complaints officer for the local government maintained a register of complaints which records all complaints that resulted in a finding under section 5.110(2)(a)? Does the complaints register include all information required by section 5.121 (2)?	Yes		Governance
3	s5.121(3)	Has the CEO published an up-to-date version of the register of the complaints on the local government's official website?	Yes		Governance

Optional Questions

No	Reference	Question	Response	Comments	Respondent
1	Financial Management Reg 5 (2)(c)	Did the CEO review the appropriateness and effectiveness of the local government's financial management systems and procedures in accordance with Financial Management Reg 5(2)(c) within the three years prior to 31 December 2021? If yes, please provide the date of council's resolution to accept the report.	Yes	The Interim Audit and Financial Management Review was received by Council on 26/06/2019 (Decision #OCM201819/237).	Finance
2	Audit Reg 17	Did the CEO review the appropriateness and effectiveness of the local government's systems and procedures in relation to risk management, internal control and legislative compliance in accordance with Audit Reg 17 within the three years prior to 31 December 2021? If yes, please provide date of council's resolution to accept the report.	Yes	The report was received and endorsed by Council on 25/08/2021 (Decision #OCM202122/041).	Risk and Insurance
3	s5.87C	Where a disclosure was made under sections 5.87A or 5.87B, was the disclosure made within 10 days after receipt of the gift? Did the disclosure include the information required by section 5.87C?	Yes		Governance
4	s5.90A(2) & (5)	Did the local government prepare, adopt by absolute majority and publish an up-to-date version on the local government's website, a policy dealing with the attendance of council members and the CEO at events ?	Yes		Governance

No	Reference	Question	Response	Comments	Respondent
5	s5.96A(1), (2), (3) & (4)	Did the CEO publish information on the local government's website in accordance with sections 5.96A(1), (2), (3), and (4)?	No	The information published on the Town of Port Hedland's website was as legislated, with the exception of 5.96A (1)(a). The Town did not have a map of the district on the public website. A map of the district has now been uploaded to the Town's website under the "Our Council" tab.	Governance
6	s5.128(1)	Did the local government prepare and adopt (by absolute majority) a policy in relation to the continuing professional development of council members?	Yes		Governance
7	s5.127	Did the local government prepare a report on the training completed by council members in the 2020/2021 financial year and publish it on the local government's official website by 31 July 2021?	Yes		Governance
8	s6.4(3)	By 30 September 2021, did the local government submit to its auditor the balanced accounts and annual financial report for the year ending 30 June 2021?	Yes		Finance
9	s.6.2(3)	When adopting the annual budget, did the local government take into account all it's expenditure, revenue and income?	Yes		Finance

Tenders for Providing Goods and Services

No	Reference	Question	Response	Comments	Respondent
1	F&G Reg 11A(1) & (3)	Did the local government comply with its current purchasing policy [adopted under F&G Reg 11A(1) & (3)] in relation to the supply of goods or services where the consideration under the contract was, or was expected to be, $250,000 or less or worth $250,000 or less?	No	The Town engaged a contractor directly, following a safety incident. The value of services accrued over the period exceeded the minimum quote requirement.	Procurement
2	s3.57 F&G Reg 11	Subject to F&G Reg 11(2), did the local government invite tenders for all contracts for the supply of goods or services where the consideration under the contract was, or was expected to be, worth more than the consideration stated in F&G Reg 11(1)?	No	Two did not go to public tender: One project was initially underestimated and the other was completed through Panel Contract with Construction Contract used as an amendment to the Panel Contract executed.	Procurement
3	F&G Regs 11(1), 12(2), 13, & 14(1), (3), and (4)	When regulations 11(1), 12(2) or 13 required tenders to be publicly invited, did the local government invite tenders via Statewide public notice in accordance with F&G Reg 14(3) and (4)?	Yes		Procurement

No	Reference	Question	Response	Comments	Respondent
4	F&G Reg 12	Did the local government comply with F&G Reg 12 when deciding to enter into multiple contracts rather than a single contract?	Yes		Procurement
5	F&G Reg 14(5)	If the local government sought to vary the information supplied to tenderers, was every reasonable step taken to give each person who sought copies of the tender documents or each acceptable tenderer notice of the variation?	Yes		Procurement
6	F&G Regs 15 & 16	Did the local government's procedure for receiving and opening tenders comply with the requirements of F&G Regs 15 and 16?	Yes		Procurement
7	F&G Reg 17	Did the information recorded in the local government's tender register comply with the requirements of F&G Reg 17 and did the CEO make the tenders register available for public inspection and publish it on the local government’s official website?	Yes		Procurement
8	F&G Reg 18(1)	Did the local government reject any tenders that were not submitted at the place, and within the time, specified in the invitation to tender?	Yes		Procurement
9	F&G Reg 18(4)	Were all tenders that were not rejected assessed by the local government via a written evaluation of the extent to which each tender satisfies the criteria for deciding which tender to accept?	Yes		Procurement
10	F&G Reg 19	Did the CEO give each tenderer written notice containing particulars of the successful tender or advising that no tender was accepted?	Yes		Procurement
11	F&G Regs 21 & 22	Did the local government’s advertising and expression of interest processes comply with the requirements of F&G Regs 21 and 22?	N/A	No expression of interests were released during this period.	Procurement
12	F&G Reg 23(1) & (2)	Did the local government reject any expressions of interest that were not submitted at the place, and within the time, specified in the notice or that failed to comply with any other requirement specified in the notice?	N/A	No expression of interests were released during this period.	Procurement
13	F&G Reg 23(3) & (4)	Were all expressions of interest that were not rejected under F&G Reg 23 (1) & (2) assessed by the local government? Did the CEO list each person as an acceptable tenderer?	N/A	No expression of interests were released during this period.	Procurement
14	F&G Reg 24	Did the CEO give each person who submitted an expression of interest a notice in writing of the outcome in accordance with F&G Reg 24?	N/A	No expression of interests were released during this period.	Procurement
15	F&G Regs 24AD(2) & (4) and 24AE	Did the local government invite applicants for a panel of pre-qualified suppliers via Statewide public notice in accordance with F&G Reg 24AD(4) and 24AE?	Yes		Procurement

No	Reference	Question	Response	Comments	Respondent
16	F&G Reg 24AD(6)	If the local government sought to vary the information supplied to the panel, was every reasonable step taken to give each person who sought detailed information about the proposed panel or each person who submitted an application notice of the variation?	Yes		Procurement
17	F&G Reg 24AF	Did the local government's procedure for receiving and opening applications to join a panel of pre-qualified suppliers comply with the requirements of F&G Reg 16, as if the reference in that regulation to a tender were a reference to a pre-qualified supplier panel application?	Yes		Procurement
18	F&G Reg 24AG	Did the information recorded in the local government's tender register about panels of pre-qualified suppliers comply with the requirements of F&G Reg 24AG?	Yes		Procurement
19	F&G Reg 24AH(1)	Did the local government reject any applications to join a panel of pre-qualified suppliers that were not submitted at the place, and within the time, specified in the invitation for applications?	N/A	No late submissions were noted.	Procurement
20	F&G Reg 24AH(3)	Were all applications that were not rejected assessed by the local government via a written evaluation of the extent to which each application satisfies the criteria for deciding which application to accept?	Yes		Procurement
21	F&G Reg 24AI	Did the CEO send each applicant written notice advising them of the outcome of their application?	Yes		Procurement
22	F&G Regs 24E & 24F	Where the local government gave regional price preference, did the local government comply with the requirements of F&G Regs 24E and 24F?	Yes		Procurement

I certify this Compliance Audit Return has been adopted by council at its meeting on ____________________

Signed Mayor/President, Port Hedland

Signed CEO, Port Hedland

MOORE

RISK MANAGEMENT GAP ANALYSIS

Town of Port Hedland

24 January 2022

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

1.1. Introduction

The Town of Port Hedland ("**Town**") requires a review of the existing risk management documentation so that it can implement a Risk Management Framework that reflects better practice principles, is fit for purpose, compliant with the *Local Government Act 1995* and supporting regulations.

Whilst the Town has basic risk management tools in place, it does not have an appropriate strategic Risk Management Framework.

A risk management improvement program had been previously developed but was put on hold due to other priorities. The risk improvement program refers to the overarching actions/initiatives taken by the Town to improve the overall risk management function.

The Risk Management Gap Analysis ("**Gap Analysis**") assessment represents the first phase of a body of work that subsequently includes development of the Risk Management Framework; and recommendation of a training methodology to embed an integrated risk management culture.

1.2. Objective and Scope

- Best practice where fit for purpose
- What policies and procedures does the Town currently have in place?
- Review of existing policies and procedures and benchmark against fit for purpose type policies and procedures; and
- Review of existing internal control reviews and benchmark against fit for purpose control reviews.

The scope does not include the analysis on training and technology as these aspects are anticipated to be implemented by the Town subsequently.

1.3. Approach

Our approach for performing the Gap Analysis included the following:

- Review the Town's risk management practices against AS/NZS 31000:2018 Risk Management.
- Interview with key stakeholders to inquire existing practices, training, state of internal controls, roles and responsibilities in relation to risk management.
- Obtain the current suite of risk management policies and procedures, including risk register and relevant reports.
- Review current practices and associated documents against organisational requirements to ensure fit for purpose.
- Identify draft observations.
- Confirmation of draft observations with the Town.
- Provision of draft report identifying:
  - The gaps in the Risk Management Framework compared to better practice principles which is fit for purpose, and compliance requirements. (Risk Management Framework refers to the overall elements within a risk management function which includes, policies, procedures, processes, and plans.)
  - The appropriateness of the governance arrangements for the Town's Risk Management Framework.

The purpose of the engagement was to identify "gaps", and not to identify and report the extent of risk management currently in place at the Town, nor the operating effectiveness of the current risk management practices.

1.4. Acknowledgement

We would like to thank the Town's personnel for their assistance during this analysis. Key personnel contacted for this engagement are outlined in Appendix 1.

1. EXECUTIVE SUMMARY (CONTINUED)

1.5. Positive Observations

Our review identified that the Town intends to integrate and align risk thinking and behaviours in the planning, reporting and operational practices performed by all staff to ultimately drive effective decision making in line with the Town's strategic objectives and Risk Appetite (currently not documented). Senior Management which we interviewed were cognisant of the key risks in their areas of responsibility and developed their own approach to treat and monitor (i.e., manage) those risks.

Whilst improvement opportunities have been identified to establish a common, consistent organisation wide approach for managing risks, there is no formal documentation of a unified process for managing risks at the Town.

Generally, based on our inquiries, Senior Management are risks averse and functions in a risk conscious manner, adopt processes that minimise the occurrence of risks and/or reduce the impact of risk on the Council. Interviews with stakeholders revealed a re-focus on risk management practices within the Town to embed a risk culture across the organisation. Senior leaders demonstrated a commitment to sound risk mitigation practices, which promote continuous improvement and ethical behaviours. This commitment is illustrated with the assignment of a specific resource to support business units with understanding risk concepts and processes. Additionally, we observed a dedicated business unit assigned to focus on risk, audit and insurance matters.

In operational areas that typically embody health, safety, regulatory and financial risks such as Human Resources and Infrastructure Services, through interviews and discussions, we observed Management had developed appropriate internal operating procedures with regular reporting and oversight. Analysis of the information indicated there are granular details to provide Officers with guidance on how to plan, assess, and act in response to hazards and threats.

Initiatives such as “Take 5”, “Safe Work Method Statements” and “Hazard Reporting” confirm a culture that has a strong emphasis on workplace safety minimising the occurrence of personal injury.

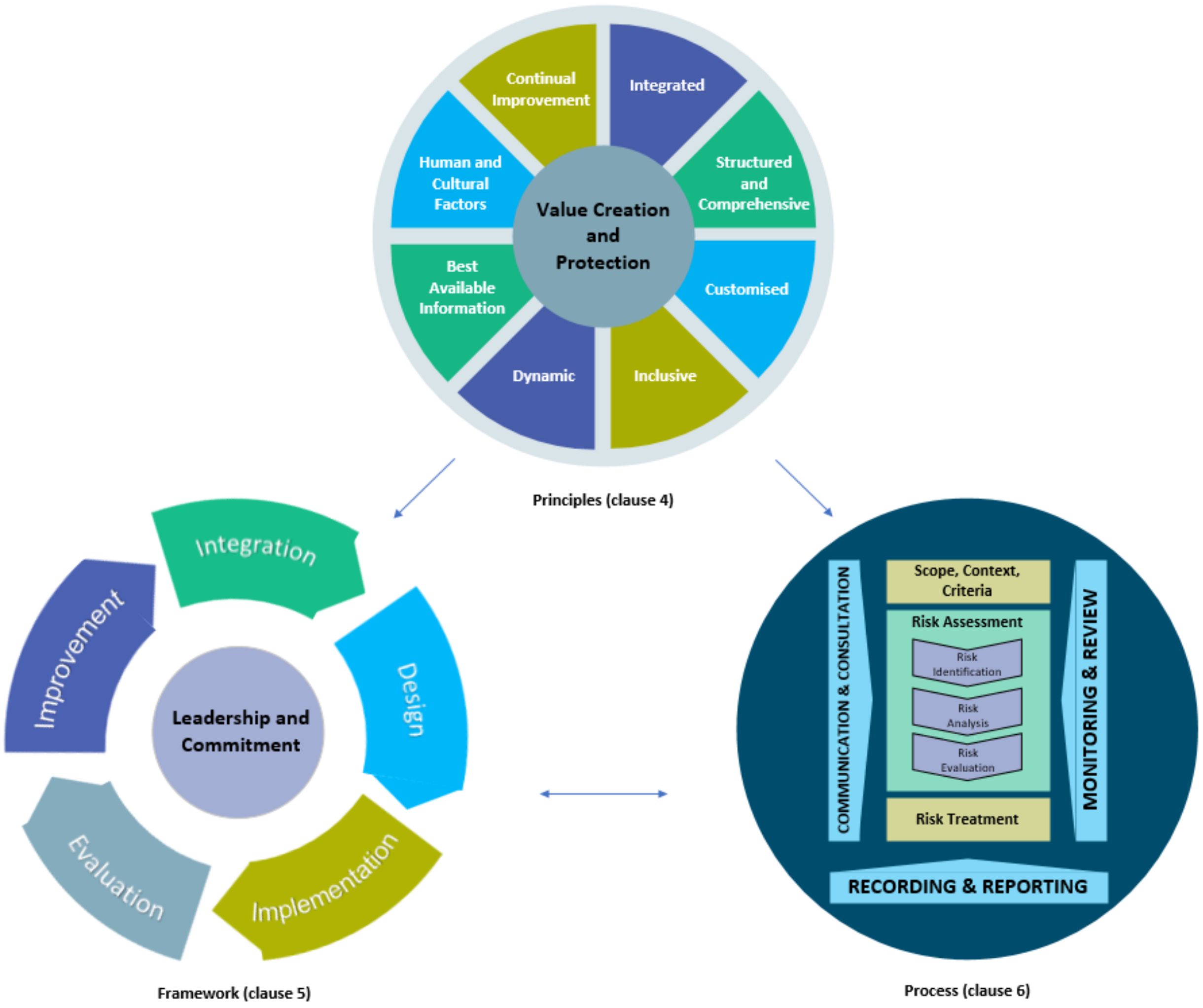
The improvement opportunities identified in the next section are aimed to unify and standardise a common approach to organisational risk management and should not be interpreted that the Town is devoid of safe work practices or risks are not being monitored operationally.

1. EXECUTIVE SUMMARY (CONTINUED)

1.6. Key Improvement Opportunities

Through the performance of this review, we identified key improvement opportunities to establish and promote a consistent and effective application of risk management practices across the Town. The following five priority key improvements will help to strengthen and standardise the Town's current risk management practices and support a sustainable risk culture across the organisation:

1. Establishing a Risk Management Framework that aligns to the AS/NZS 31000:2018 Risk Management depicted in Figure 1.
2. Establishing a Risk Appetite Statement to provide guidance on how much total risk the Town is willing to take. Update, communicate and disseminate the Town's risk appetite, risk vision and risk management rules and values within the Policy 1/022 Risk Management.
3. Enhancing the Risk Management Framework through the development of supporting procedures and guidelines, defining accountability and training and teaching staff.
4. Conducting a risk identification, assessment and evaluation exercise to establish the risk register, which engages the elected members, leadership team and key personnel across the organisation.
5. Embedding risk reporting requirements throughout the organisation so that it is actively used to support decision making at all levels.



Principles (clause 4)

Framework (clause 5)

Process (clause 6)

Figure 1: ***AS/NZS 31000:2018 Risk Management***

1. EXECUTIVE SUMMARY (CONTINUED)

1.7. Summary Evaluation

A Risk Management Framework refers to a collection of documents consisting of policy, procedures, processes, registers, and reports used for risk management purposes.

Figure 2 provides a summary of the documentations in a Risk Management Framework; and Figure 3, outlines the Town's current suite of risk-related documents and the associated status.

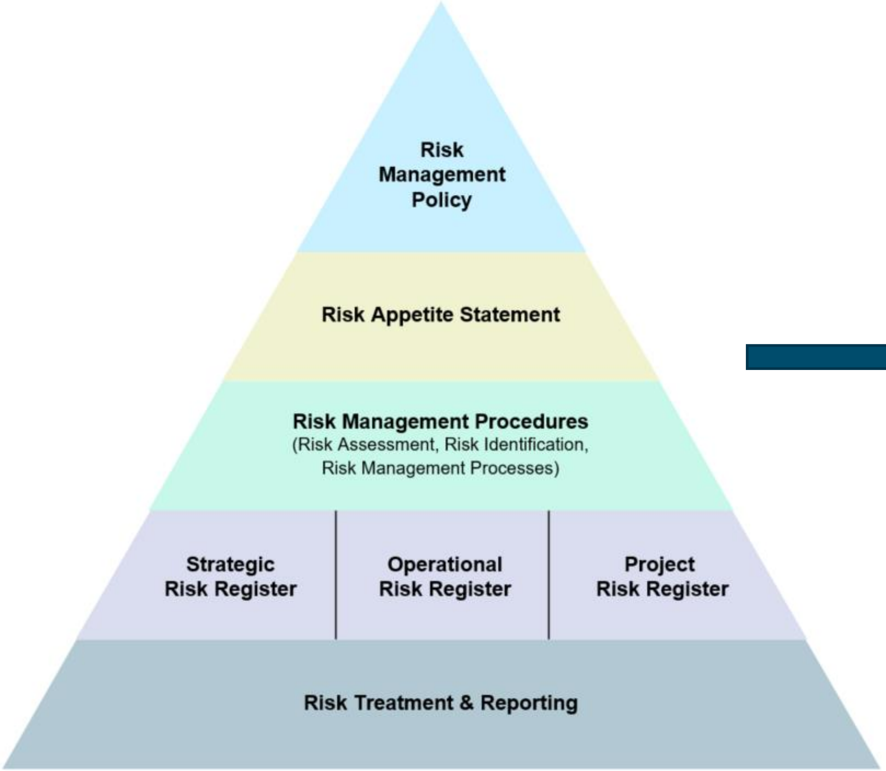

Risk Management Policy
Risk Appetite Statement
Risk Management Procedures
(Risk Assessment, Risk Identification, Risk Management Processes)
Strategic Risk Register
Operational Risk Register
Project Risk Register
Risk Treatment & Reporting

Figure 2: Risk Management Framework Documentation Hierarchy

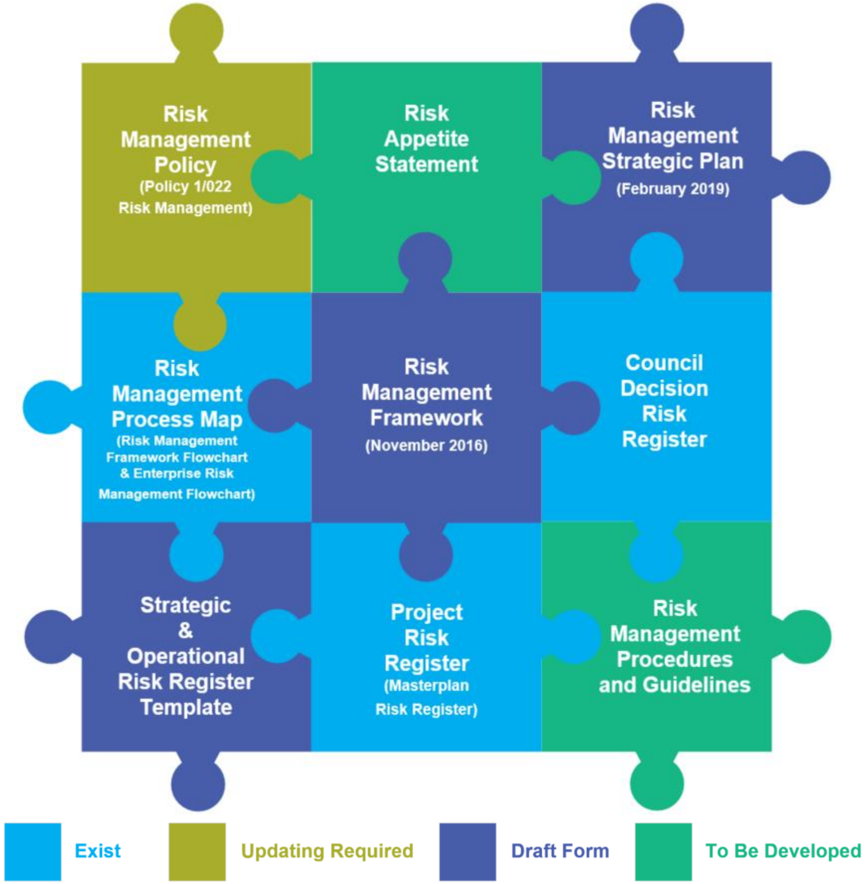

Risk Management Policy (Policy 1/022 Risk Management)
Risk Appetite Statement
Risk Management Strategic Plan (February 2019)
Risk Management Process Map (Risk Management Framework Flowchart & Enterprise Risk Management Flowchart)
Risk Management Framework (November 2016)
Council Decision Risk Register
Strategic & Operational Risk Register Template
Project Risk Register (Masterplan Risk Register)
Risk Management Procedures and Guidelines
Exist
Updating Required
Draft Form
To Be Developed

Figure 3: The Town's Current Documentations and Improvement Opportunities

1. EXECUTIVE SUMMARY (CONTINUED)

1.7. Summary Evaluation

Provided below is the summary of our review highlighting the current gaps in the Town's risk management framework. Further information is contained within the detailed observations section of this report.

	Better Practice	Detailed Observation Reference	Examples of Current Documentation	Summary of Gaps	Improvement Opportunities
Strategy and Culture	Executive sponsorship of risk management sets the 'tone at the top' and articulates the organisation's risk strategy.	1	• A risk matrix has been adopted as the Town's risk appetite statement (December 2015) • Draft Risk Management Strategic Plan (February 2019) • Draft Risk Management Plan (February 2017) • Policy 1/022 Risk Management (April 2016)	• The Town has a risk management Policy, 1/022 Risk Management, which will need to be updated in line with the new standard (AS/NZS 31000:2018 Risk Management) • The Town's Draft Risk Management Strategic Plan will need to be finalised in line with the updated 'Policy 1/022 Risk Management'. • Risk management should be clearly articulated and well understood; linked with risk appetite, business strategy; and consistently embedded into decision making throughout the organisation. This refers to the risk management process itself. A Risk Management Framework for how this could be achieved should be developed.	R1. Management should update Policy 1/022 Risk Management to clearly formulate the Town's risk strategy and communicate rules and values in relation to risk management. Specifically, this should include the following: • Clearly communicate the risk culture and behaviours that are expected, whereby risk standards are defined, assessed and embedded into business process and actively reinforced. • Promote the Town's risk appetite by providing practical examples to build a common understanding and consistent application across the business. The risk appetite and tolerance levels should be regularly and consistently communicated. • Require that risk identification, assessment and evaluation are directly linked to the Town's strategic objectives and business priorities/performance. • Encourage formulation of key business decisions with a 'risk/opportunity point of view' in ELT papers and other management committee meetings.

1. EXECUTIVE SUMMARY (CONTINUED)

1.7 Summary Evaluation (continued)

	Better Practice	Detailed Observation Reference	Examples of Current Documentation	Summary of Gaps	Improvement Opportunities
Risk Management Framework	• Regular review of risk profile, effectiveness of controls, and risk mitigation plan. • Oversight of organisation-wide assurance activities against strategic and business risks to support prioritisation and allocating resources to develop good risk controls. • Formal monitoring and reporting activities around risk management and outcomes.	2, 3	• Draft Risk Management Framework (November 2016) • Amended Audit, Risk and Compliance (ARC) Terms of Reference (November 2020) • Draft Risk Management Strategic Plan (February 2019) • Draft Risk Management Plan (February 2017) • Audit, Risk and Compliance (ARC) Committee meeting minutes • Policy 1/024 Fraud and Corruption Prevention (August 2016) • Occupational Safety and Health Management Plan • Workplace Health and Safety Policy • Local Emergency Management Arrangements (LEMA), pending adoption from Council	• A whole of organisation risk identification exercise is required to be undertaken. • While other key governance documents such as fraud and corruption, cybersecurity, business continuity, disaster recovery, emergency management have been developed, there is a need to review them to ensure they are based on a structured enterprise risk management approach. • Linkage between risk and the Town's strategic and business objectives can be more explicit. • Risk taxonomy for risk assessments and tangible measures and metrics linked with business process and performance need to be developed.	R2. Management should develop and approve fit for purpose procedures and supporting templates to promote effective risk management practices. These documents should include the end-to-end risk management activities, from risk identification, assessment, monitoring and reporting, risk response management (including controls and treatment action plans). [Please refer to Figure 2, the risk management framework documentation hierarchy] R3. Management should: • Define the requirement for risk discussions to be tabled routinely at key executive committees and management forums within the Risk Management Framework. (Risk theme discussions may vary and consider different aspects of the business area's objective and performance). In the first instance, breaches of the reporting requirement should be monitored and escalated to the Audit, Risk and Compliance Committee for action. • Update the reporting requirements to include relevant information on risk profile or control environment changes based on business performance.
Procedures and Guidelines	Clearly documents the scope, approach and requirements for the risk management activities.	2, 3	• Draft Risk Management Process Map for Enterprise Risk Management (ERM) • Draft Risk Profile System (RPS) Process Map • Policy 1/022 Risk Management (April 2016) • WHS Internal Operating Procedure 022: "Terms of reference: Workplace Safety and Health Representatives" • Internal Operating Procedure: "GOV012 Managing Conflicts of Interest" • Code of Conduct Breach Form	• Common organisational-wide procedures and templates for the performance of risk management activities require development. • Formal risk reporting and communications should be developed and used to support oversight from the management and operations.	R4. The Risk Management Framework should be developed and include the following, but not limited to (we acknowledge some of these elements which currently exist within the Draft Risk Management Strategic Plan (February 2019)): • Clarify the functional and reporting requirements for risk activities, including for staff, supervisors and management. • Provide management with clear responsibility over risk activities, including risk controls and mitigation (treatment) plans by linking risk with the business processes and performance; where possible

1. EXECUTIVE SUMMARY (CONTINUED)

1.7 Summary Evaluation (continued)

	Better Practice	Detailed Observation Reference	Examples of Current Documentation	Summary of Gaps	Improvement Opportunities
Risk Assessment	Risks are identified, evaluated and assessed consistently across the organisation, based on well-defined risk rating criteria and common risk taxonomy.	2, 3	• A draft Operational Risk Register Template (without any risk information) was created in 2019, but not approved by ELT for implementation. • A draft Strategic Risk Register Template (without any risk information) was created in 2019, but not implemented. • A Council Decision Risk Register is currently implemented. • Draft Business Continuity Plan, expected to be completed by March 2022. • 2020 Business Continuity Spreadsheet. • Project Management Framework Risk Register and Management Plan • Projects Masterplan Risk Register	• A whole of organisation risk identification exercise is required to be undertaken. • While other key governance documents such as fraud and corruption, cybersecurity, business continuity, disaster recovery, emergency management have been developed, there is a need to review them to ensure they are based on a structured enterprise risk management approach. • Linkage between risk and the Town's strategic and business objectives can be more explicit. • Risk taxonomy for risk assessments and tangible measures and metrics linked with business process and performance need to be developed.	R5. Management should perform a risk identification, assessment and evaluation exercise that engages the Council, the ELT, and key personnel across the Town with a view to: a) Update and Implement the Strategic Risk Register and Operational Risk Register with current and relevant risk information (Strategic and Business Risks). b) Update the risk definition, cause, and consequences. c) Clarify risk ownership roles at ELT and management level. d) Review the existing controls and assessment of control effectiveness. e) Link risk with strategic objectives, business performance and objectives. f) Identify metrics and measures, where possible to monitor effectiveness of controls and inform the risk profile.
Governance	Defined functional ownership, roles, and responsibilities for those involved in Risk Management.	2, 4	• Policy 1/022 Risk Management (April 2016) • TOPH Code of Conduct (December 2019. • Position Description – Senior Risk and Audit Advisor (April 2021). • Position Description – Risk and Insurance Advisor (May 2021).	• The Risk Management function can be better supported with a centralised approach. • The Risk Management function has been recently established, and there is a need to continue to build capacity and capability to effectively manage the Town's risks.	No further recommendation is proposed. Management has provided evidence for addressing the identified gap as part of the roles within the governance business unit.

2. OBSERVATIONS AND RECOMMENDATIONS

Strategy and Culture

Finding 1

Executive sponsorship of risk management sets the organisation's risk strategy. The risk management strategy reflects organisational governance decisions in terms of risk priorities, risk tolerance, and risk acceptance criteria. The typical main risk strategies are:

1. Risk avoidance – choosing to discontinue or not undertake an operation to avoid the risks involved. For example, discontinuing leisure service operations.
2. Risk mitigation or risk reduction – taking steps to reduce the probability or impact of a risk. For example, segregation of duties or multi-factor authentication.
3. Risk transfer – shifting the risk to another organisation by taking out insurance, or sub-contracting an activity to another organisation.
4. Risk acceptance – recognizing the risk but choosing not to take any specific action to control or reduce it.

As can be seen in the examples above, determining and communicating organisational risk tolerance is an important element in risk management strategy, as tolerance levels influence all risk management components.

Risk appetite is the amount of risk you are willing to take in pursuit of your strategic objectives. Defining risk appetite establishes boundaries for prudent decision making and risk taking. Figure 4 illustrates the concepts of Risk Appetite.

Risk Capacity	Risk capacity is, in simple terms, the boundary. It is the maximum amount of risk that the organisation can take and remain viable. Capacity is not a "single number"; it will vary across risk types, business units and strategic scenarios. Discussing capacity is a useful activity in considering how the organisation could fail.
Risk Appetite	Risk appetite is the aggregate level and types of risk an organisation is willing to assume within its risk capacity to achieve its strategic objectives and business plan.
Buffer	The buffer is the difference between risk capacity and risk appetite. One issue to discuss is how big the buffer between appetite and capacity should be. The buffer should consider the possibility of very extreme outcomes and errors in assumptions, analysis and modelling.

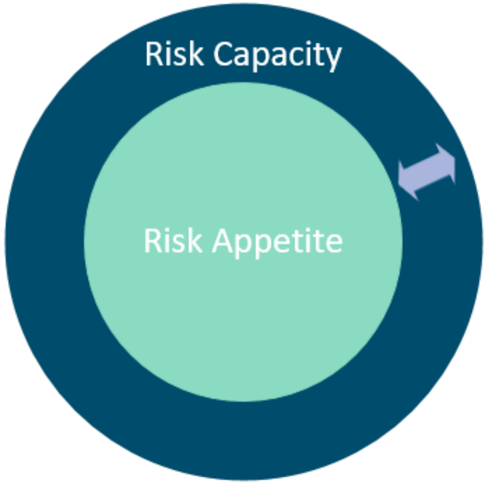


Figure 4: Risk Appetite Concept

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Strategy and Culture (continued)

Finding 1 (continued)

It is acknowledged that the Town currently has the following documents in various state of development:

- Policy 1/022 Risk Management (April 2016) – Updating is required.
- A risk matrix has been adopted as the Town's risk appetite statement (December 2015) – Risk Appetite Statement has yet to be developed.
- Risk Management Strategic Plan (February 2019) – Is currently in draft.
- Risk Management Plan (February 2017) – Is currently in draft.

Senior Management Stakeholders interviewed were cognisant of the key risks in their areas of responsibility and developed their own approach to treat and monitor those risks. Whilst risks are being managed in siloed, generally, Senior Management are risks averse and functions in a risk conscious manner, adopts processes that minimise the occurrence of risks and/or reduce the impact of risk on the Council.

Through discussions with stakeholders, we observed the following enhancement opportunities:

Clear articulation of a common approach to risk – The Town's perceived risk appetite is currently defined as per the risk assessment and acceptance criteria tables set in the Policy 1/022 Risk Management. (The risk rating criteria has not been formally re-evaluated for more than 3 years)

A Risk Appetite Statement has not been defined and communicated within the Town to provide practical guidance on how much 'total risk' the organisation is willing to take. Interviews with Management stakeholders reinforced the existence of inconsistent views on risk appetite, tolerance and/or limits.

Policy statement – There is no clear and specific definition of the benefits, principles and the structure within which risk management should operate. The risk strategy has not been defined in the Policy 1/022 Risk Management. Accordingly, the Town's risk strategy is unclear, and not aligned to the business strategy across the organisation to enable a common/integrated strategy and vision for risk management.

Linking Strategy with Risk – A review of the Policy 1/022 Risk Management, Draft Risk Management Strategic Plan and other documentation and feedback received from interviews with management members noted that risks (strategic, business and project) are openly discussed at the Executive Leadership Team ("**ELT**") and Council levels prior to making decisions, however there is no formal and direct link with the Town's strategic objectives and business performance.

A review of the Town's various documentations noted that risks are not formally and directly linked to a strategic and/or business objective; thus, limiting integration of risk management activities with strategic and business level priorities.

We also observed the strategic planning process outlined in the Draft Strategic Risk Management Plan does not formally incorporate risk information and appears to be independent from the risk assessment process.

Implications:

In a decentralised business environment such as at the Town, the lack of clearly defined and embedded risk strategy across the organisation, increases the risk of business practice, decision making and/or behaviours that may not be aligned to the Town's strategic and business objectives.

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Strategy and Culture (continued)

Finding 1 (continued)

Recommendation

R1. We recommend that Management update the Policy 1/022 Risk Management to clearly formulate the Town's risk strategy and communicate rules and values in relation to risk management. Specifically, this should include the following:

- Clearly communicate the risk culture and behaviours that are expected, whereby risk standards are defined, assessed and embedded into business process and actively reinforced.
- Promote the Town's risk appetite by providing practical examples to build a common understanding and consistent application across the business. The risk appetite and tolerance levels should be regularly and consistently communicated.
- Require that risk identification, assessment and evaluation are directly linked to the Town's strategic objectives and business priorities/performance.
- Encourage formulation of key business decisions with a 'risk/opportunity point of view' in ELT papers and other management committee meetings.

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Risk Management Framework

Finding 2

AS/NZS ISO 31000:2009 Risk Management – Principles and Guidance defines a risk management framework as a set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Figure 5 outlines the holistic aims of the Risk Management Framework and depicts the key elements.

Risk management enables the organisation to:

a) Challenge assumptions in decision-making;

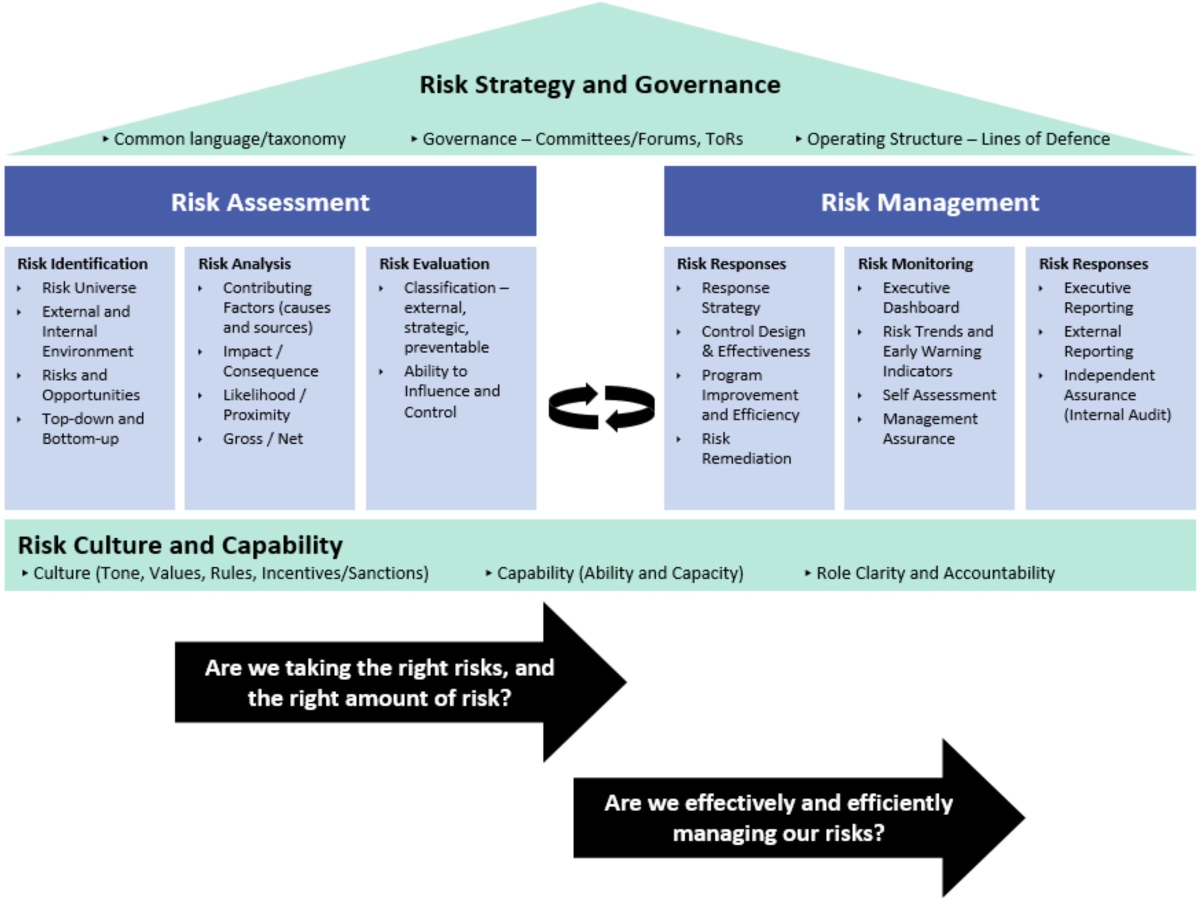
b) Take actions that will increase the likelihood that a desired outcome will be achieved;

c) Identify early signs that an undesirable event may occur and take pre-emptive action to address it;

d) Learn from successes and failures in a way that improves decision-making over time; and

e) Consider whether previous decisions remain valid and, if necessary, revise them.

Through the performance of our procedures, we identified a number of observations in relation to the Town's Risk Management Framework:



Risk Strategy and Governance

- Common language/taxonomy
- Governance – Committees/Forums, ToRs
- Operating Structure – Lines of Defence

Risk Assessment

Risk Identification
- Risk Universe
- External and Internal Environment
- Risks and Opportunities
- Top-down and Bottom-up

Risk Analysis
- Contributing Factors (causes and sources)
- Impact / Consequence
- Likelihood / Proximity
- Gross / Net

Risk Evaluation
- Classification – external, strategic, preventable
- Ability to Influence and Control

Risk Management

Risk Responses
- Response Strategy
- Control Design & Effectiveness
- Program Improvement and Efficiency
- Risk Remediation

Risk Monitoring
- Executive Dashboard
- Risk Trends and Early Warning Indicators
- Self Assessment
- Management Assurance

Risk Responses
- Executive Reporting
- External Reporting
- Independent Assurance (Internal Audit)

Risk Culture and Capability

- Culture (Tone, Values, Rules, Incentives/Sanctions)
- Capability (Ability and Capacity)
- Role Clarity and Accountability

Are we taking the right risks, and the right amount of risk?

Are we effectively and efficiently managing our risks?

Figure 5: Risk Strategy and Governance

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Risk Management Framework (continued)

Finding 2 (Continued)

It is acknowledged the Town has the following documents that support elements of a risk management framework:

- Risk Management Framework (November 2016) – Is currently in draft.
- Amended Audit, Risk and Compliance (ARC) Terms of Reference (November 2020).
- Risk Management Plan (February 2017) – Is currently in draft.
- Audit, Risk and Compliance Committee (ARC) meeting minutes.
- Policy 1/024 Fraud and Corruption Prevention (August 2016).
- Occupational Safety and Health Management Plan.
- Workplace Health and Safety Policy.
- Local Emergency Management Arrangements (LEMA), pending adoption from Council.

We identified the following improvement opportunities:

A. Methods, procedures and practices

Though the Policy 1/022 Risk Management establishes the risk management principles and a high-level process requirement in line with the ISO 31000 Risk Management standard, it does not sufficiently define the requirements of effective risk management processes for each risk activity. Further details can be included on risk management procedures to support the performance of risk management methods and practices across the Town.

B. Risk monitoring and reporting

There is an opportunity to enhance formal reporting of organisational risks, which currently occurs at Council level when considering a motion; and in ELT agenda meeting papers. At business unit levels, there is variability in business practices for recording risks. Whilst business units appear to be aware of the operational risks pertaining to their portfolio of responsibility, they are not recording these formally in a risk register. Other business unit such as Infrastructure Services identifies and records risk as part of the project management framework.

C. Roles and responsibility for risk response

Risk response accountability is defined in the Policy 1/022 Risk Management and Draft Strategic Risk Management Plan at a high level. It appears the roles and responsibility for risk response is not cascaded down and defined within business processes nor is it assigned to the same person responsible for the performance of that business process. Consequently, the role of management, supervisors and staff in relation to risk management is not clearly understood and does not promote personnel accountability for risk management.

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Risk Management Framework (continued)

Finding 2 (Continued)

D. Competency and capability

Training and awareness sessions can be enhanced on risk across the organisation. We observed the following:

- Inconsistent understanding and use of risk taxonomy/vocabulary by the Town personnel throughout the different stages of risk management processes with all areas of business exhibiting different practices and levels of competency.
- Inconsistent risk management practices, whereby each 'risk owner' have developed their own practices to assess and report on risk – ranging from ad-hoc risk assessments through to team workshops.

Implications:

- Without fit for purpose Risk Management Framework in place, there is an increased risk of failure to meet the Town's risk expectations and achieve risk strategy and overall business objectives.
- Without an end-to-end risk management framework, the response of the Town would be reactive in nature rather than a preventive one, resulting in an ineffective manner of managing risks.
- A lack of well-defined procedures and the provision of training in risk management may lead to inappropriate business practices, decision and/or behaviours that may not be aligned with the Town's strategy and business objectives.

Recommendation

R2 Management should develop and approve fit for purpose procedures and supporting templates to promote effective risk management practices. These documents should include the end-to-end risk management activities, from risk identification, assessment, monitoring and reporting, risk response management (including controls and treatment action plans). [Please refer to Figure 2, the risk management framework documentation hierarchy].

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Risk Management Framework (continued)

Finding 2 (Continued)

R3 Management should:

- Define the requirement for risk discussions to be tabled routinely at key executive committees and management forums within the Risk Management Framework. (Risk theme discussions may vary and consider different aspects of the business area's objective and performance). In the first instance, breaches of the reporting requirement should be monitored and escalated to the Audit, Risk and Compliance Committee for action.
- Update the reporting requirements to include relevant information on risk profile or control environment changes based on business performance.

R4 The Risk Management Framework should be developed and include the following, but not limited to [we acknowledge some of these elements which currently exist within the Draft Risk Management Strategic Plan (February 2019)]:

- Clarify the functional and reporting requirements for risk activities, including for staff, supervisors, and management.
- Provide management with clear responsibility over risk activities, including risk controls and mitigation (treatment) plans by linking risk with the business processes and performance; where possible.

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Procedures and Guidelines

Finding 3

It is acknowledged the Town has developed the following documentation:

- Risk Management Framework (November 2016) – Is currently in draft.
- Risk Management process Map for Enterprise Risk Management (ERM) – Is currently in draft.
- Risk Profile System (RPS) Process Map – Is currently in draft.
- Policy 1/022 Risk Management (April 2016) – Updating is required.
- WHS Internal Operating Procedure 022: "Terms of reference: Workplace Safety and Health Representatives".
- Internal Operating Procedure: "GOV012 Managing Conflicts of Interest".
- Code of Conduct Breach Form.
- An Operational Risk Register (Template) was created in 2019, but not approved by ELT– Is currently in draft.
- A Strategic Risk Register (Template) was created in 2019 – Is currently in draft.
- A Council Decision Risk Register – Is currently implemented.
- Project Risk Registers – Are currently implemented.
- Draft Business Continuity Plan, expected to be completed by March 2022.
- 2020 Business Continuity Spreadsheet.

At the business level, by way of example, the Town has the following in place to manage workplace health and safety:

Document	Functions in Risk Management	Details of Document's Purpose
Internal Operating Procedure WHS 005 Risk Management	• Outlining the WHS Risk Management process in 5 steps, in accordance with relevant legislative requirements stated in Context. • Utilizing the Town's consequence matrix, risk assessment and acceptance criteria, risk matrix to assess the risks	A process for the management of WHS risks within the Town's various business units to: **1) Identify risks** **2) reduce risks to reasonably practicable level.** The IOP includes: **1) 5 Steps of risk management for WHS:** • Identify hazards • Assess risks • Identify Appropriate controls for the risks • Implement control measures • Monitor and review for effectiveness **2) Hazard reporting** **3) Links to relevant WHS documents complementing the procedure.**

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Procedures and Guidelines (continued)

Finding 3 (continued)

Document	Functions in Risk Management	Details of Document's Purpose
Internal Operating Procedure WHS 006 Hazard Management	• Provides 2 distinct methods of identifying hazards in the workplace: 1) Systematic hazard inspection process 2) Hazard reporting system • Involves WHS Advisors, Safety & Health Representatives ("**SHR's**") and supervisors of the various business units. • Includes a flow diagram of the Hazard Reporting process • The hazard reporting system will require Town's staff to refer to the IOP WHS 005 risk management.	To provide the Town's business units, methods of identifying hazards/risks and reporting them appropriately. There are 2 methods of hazard identification, which the Town's staff can use depending on the situation. Below are some key steps in the process: **1) Systematic hazard inspection process** • All staff including WHS advisors, SHRs are responsible to inspect hazards • A Hazard Inspection Checklist will be used to evaluate the hazards in the workplace • Hazards which cannot be rectified will be attached to the Rectification Action Plan (RAP) **2) Hazard Reporting** • Staff to complete Hazard/Risk Report form which will be sent to supervisor to finalise. • WHS Advisor to review and record hazards from the form into the hazard register • WHS Advisor and SHR committee meeting will discuss the hazards gathered.
ELT Incident Data Charts	• Provides data on the incidents which occurred within the directorate's business units • Includes a breakdown of type of incidents occurred. (e.g., injury, plant/equipment damage etc.)	The incident data – smartsheet provides the information from the Executive leadership Team (ELT) on the frequency of incidents occurring within their business units.

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Procedures and Guidelines (continued)

Finding 3 (continued)

Document	Functions in Risk Management	Details of Document's Purpose
Town of Port Hedland Tier 3 WorkSafe Plan Report 2018 (LGIS)	The report covers different assessments of the elements listed: • Management commitment • Planning • Consultation and Reporting • Hazard Management • Training and Supervision LGIS had provided an elaboration of the findings (scored based on a scoring methodology in the report), observation and possible recommended actions (not all were given a recommendation).	The report is part of a 3-step program: • Step 1 – Assessment • Step 2 – Planning • Step 3 – Action The report encompasses Step 1- assessment of risks • The report was completed by LGIS on site to provide the Town with a summary of the assessment findings • The assessment was performed against the WorkSafe Plan using the LGIS scoring methodology
Town of Port Hedland Tier 3 WorkSafe Plan Report 2021 (LGIS)	The report covers different assessments of the elements listed: • Management commitment • Planning • Consultation and Reporting • Hazard Management • Training and Supervision LGIS had provided an elaboration of the findings (scored based on a scoring methodology in the report), observation and possible recommended actions (not all were given a recommendation).	This is the latest WorkSafe Plan Report (2021) The report is part of a 3-step program: • Step 1 – Assessment • Step 2 – Planning • Step 3 – Action The report encompasses Step 1- assessment of risks • The report was completed by LGIS on site to provide the Town with a summary of the assessment findings The assessment was performed against the WorkSafe Plan using the LGIS scoring methodology

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Procedures and Guidelines (continued)

Finding 3 (continued)

Through our discussion with Management and reviews of existing risk documentation, we observed that risk management processes are not consistently integrated into the Town's business activities. Specifically, we identified the following improvement opportunities:

A. Risk identification and assessment

- End-to-end enterprise risk identification and assessments have not been performed in recent times. There is no organisational wide risk register aligned to current business priorities and practices.
- Risk ownership and responsibility is unclear due to inconsistent definitions of risks.
- Variable understanding of risk identification, assessment and reporting.

B. Risk response management

- There is no clear link between the business process performance and the effect of risks to objectively measure the impact of the business controls on the risk mitigation strategy.
- While other key governance documents such as fraud and corruption, cybersecurity, business continuity, disaster recovery, emergency management have been developed, there is a need to review them to ensure they are based on a structured enterprise risk management approach.
- Inconsistent and/or insufficient documentation of existing risk controls. The effectiveness and efficiency of risk controls are based on informal assessment only, and not documented.
- There is limited overarching visibility of the risk assurance activities performed across the Town and the corresponding evaluation of the 'cost of controls' (i.e., resources, effort, internal/third party cost) across key strategic and business risks.
- Risks identified within the reports from Town officers communicated to the council were not consistently presented with the details setting out the basis of the assessment (e.g., financial, health, reputation, etc.).
- As such, 'investment' decisions in risk controls and mitigation plans remain unknown, and do not consider the holistic risk profile and assurance activities to target risk control 'gap' areas and rationalise risk control areas where 'overlaps' are identified.

Implications:

- Without fit for purpose risk management framework in place, there is an increased risk of failure to meet the Town's risk expectations and achieve risk strategy and overall business objectives.
- A lack of an updated risk matrix and rating scale may lead to inaccurate prioritization of risks and misalignment with the Town's strategic and business objectives

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Procedures and Guidelines (continued)

Finding 3 (continued)

Recommendation

R5. Management should perform a risk identification, assessment and evaluation exercise that engages the Council, the ELT, and key personnel across the Town with a view to:

a) Update and Implement the Strategic Risk Register and Operational Risk Register with current and relevant risk information (Strategic and Business Risks).

b) Update the risk definition, cause, and consequences.

c) Clarify risk ownership roles at ELT and management level.

d) Review the existing controls and assessment of control effectiveness.

e) Link risk with strategic objectives, business performance and objectives.

f) Identify metrics and measures, where possible to monitor effectiveness of controls and inform the risk profile.

2. OBSERVATIONS AND RECOMMENDATIONS (CONTINUED)

Governance

Finding 4

The Town’s approved Risk Management Policy formalises the intent of the organisation’s approach to risk and captures the overarching structure, roles, responsibilities, and requirements to manage risk across the organisation.

Interviews conducted with stakeholders indicate that due to the unclear functional and reporting principles and requirements regarding risk activities across the organisation, there appears to be a lack of certainty as to the responsibility and ability to ‘act on risk and controls’ at management level.

There is a general perception that there lacks a structure that supports and coordinates risk management, works with business units to educate risk concepts and principles so that risk identification and assessment is performed consistently and accurately.

In the current decentralised environment where risk is managed separately by each ‘risk owner’, the lack of a centrally governed model increases the possibility that risk activities are not delivering the expected strategic and business objectives.

It is acknowledged that the role of a Senior Risk and Audit Advisor will be the coordinator of risk management activities going forward. It is our understanding that this role will be supporting business units with risk management activities and education on risk concepts and related principles. By way of example, we note the Position Descriptions of two advisors within the Town’s governance business unit include, but not limited to the following duties:

Senior Risk and Audit Advisor (April 2021)	Risk and Insurance Advisor (May 2021)
Coordinate independent reviews on functions, programs or activities as identified in risk and audit plans and seek feedback, provide analysis, develop recommendations, and report information to relevant stakeholders.	Support the Senior Risk and Audit Advisor in all areas of risk, audit, and business improvement activities.
Provide expert and practical information on all aspects of risk, internal audit, insurance, and associated matters.	Provide advice, guidance, and clarification to customers (internal and external) on all insurance, risk, and audit matters.
Develop partnership and collaborate with others to effectively identify, review, treat, monitor, and manage risks.	Assist with the implementation and ongoing administration of Town’s Risk Management Framework.
Support the Executive Leadership Team, the Audit and Risk Committee and Council by way of periodic reporting, practical recommendations, and advice to achieve all required accountabilities.	Administer Council’s Audit, Risk and Compliance Committee meetings, including agendas, minutes and follow up actions.

Implications:

- Risk not being embedded in business decision making, leading to inadequate control over risk;
- Capacity, complexity, and resourcing within risk activities resulting in teams being widely stretched, not having the right skills, or not keeping up with changes in the Town’s risk profile; and/or
- Risk of multiple cultures within one organisation resulting in conflicting messages.

Recommendation

No further recommendation is proposed. Management has provided evidence for addressing the identified gap as part of the roles within the governance business unit.

3. OTHER

3.1 Disclaimers

Moore Australia (WA) Pty Ltd as agent, an independent member of Moore Global Network Limited, and a Perth based partnership of trusts carries on business separately and independently from other Moore Global Network Limited member firms worldwide.

Services provided under this engagement are provided by Moore Australia (WA) Pty Ltd as agent and not by any other independent Moore Global Network Limited member firms worldwide. No other independent Moore Global Network Limited member has any liability for services provided.

3.2 Limitations of Scope

Our work is limited by the following:

- Our work did not constitute an assurance examination or a review in accordance with Australian Auditing and Assurance Standards. Accordingly, we do not provide an opinion or other form of assurance with regard to our work or the information upon which our work was based. We did not audit or otherwise verify the information supplied to us in connection with this engagement, except to the extent specified in this report or our approved objectives and scope.
- Our engagement is not designed to detect all weaknesses in control procedures as it is not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis. Any projection of the evaluation of the control procedures to future periods is subject to the risks that the procedures may become inadequate because of changes in conditions or that the degree of compliance with them may deteriorate.

3.3 Basis of Use

This report has been prepared in accordance with the objectives and approach agreed in the engagement document and subject to the following limitations:

- Other than use by you for the purpose, our report cannot be issued, accessed, or relied upon by any third party without our prior written approval. Furthermore, neither the report nor extracts from it will be included in any document to be circulated to other third parties without our prior written approval of the use, form, and context in which it is proposed to be released. We reserve the right to refuse to grant approval to issue the reporting to any other party.
- The matters raised in this report are only those which came to our attention while performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made. We cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud. Accordingly, management should not rely on our report to identify all weaknesses that may exist in the systems and procedures under examination, or potential instances of non-compliance that may exist.
- We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy or reliability is given in relation to statements and representations made by, and the information and documentation provided by, Management and personnel. We have indicated within this report the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the report. We are under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form unless specifically agreed with the client. The findings expressed in this report have been formed on the above basis.
- Recommendations for improvement should be assessed by management for their full commercial impact before they are implemented.

3. OTHER (CONTINUED)

3.4 Conflicts of Interest

The firm is not aware of any existing or potential relationship, transaction or holding that would compromise its objectivity in the conduct of the services rendered. Should the possibility of a perceived or actual conflict arise the matter would be raised with the Chief Executive Officer immediately and activities suspended until the issue was resolved to your satisfaction.

3.5 Liability

Moore Australia (WA) Pty Ltd trading as agent – ABN 99 433 544 961, an independent member of Moore Global Network Limited - members in principal cities throughout the world.

Liability limited by a scheme approved under Professional Standards Legislation.

APPENDIX 1: KEY PERSONNEL CONTACTED

We would like to thank the following personnel for their assistance in the conduct of this gap analysis.

Number	Name	Roles
1	Angelique Cook	Senior Risk and Audit Advisor
2	Cara Cascao	Manager Community Development
3	Cherry McNicol	Manager Human Resources
4	Cheye Hill	Manager Leisure Facilities
5	Christine Pidgeon	Manager Financial Services
6	Craig Watts	Director Regulatory Services
7	Florian Goessmann	Manager IT Program & Delivery
8	Grant Voss	Manager Infrastructure Operations
9	Josephine Bianchi	Director Community Services
10	Lee Furness	Director Infrastructure Services
11	Peter Chandler	Manager Infrastructure Projects and Assets
12	Sandra Brockwell	Senior WHS Advisor
13	Stephanie Sikaloski	Risk and Insurance Advisor
14	Tammy Wombwell	Senior Project Officer – Business Infrastructure Projects

CONTACT US

Moore Australia (WA)

Level 15, 2 The Esplanade,
Perth WA 6000
T +61 8 9225 5355
F +61 8 9225 6181

MOORE

HELPING YOU THRIVE IN A CHANGING WORLD