



## BOARD REPORT

REPORT No.: 2025-33

MEETING DATE: SEPTEMBER 18, 2025

SUBJECT: ENTERPRISE RISK MANAGEMENT - ANNUAL UPDATE

---

### RECOMMENDATION

For information only.

### REPORT SUMMARY

To provide The District of Thunder Bay Social Services Administration Board (TBDSSAB or the Board) with an update on the organization's Enterprise Risk Management (ERM) Framework.

### BACKGROUND

Developing an ERM System was identified as a component of the 2017 - 2020 Practical Vision of TBDSSAB; specifically, as a component within Transparent and Sustainable Finances.

To strengthen TBDSSAB risk management functions and develop a fulsome process, Administration began the process of establishing a comprehensive risk management overview and framework.

The Board approved the ERM Policy at its November 2018 Meeting, which included direction that Administration complete an ERM Framework.

The Board approved the ERM Framework, and resultant risk tolerance at its November 2019 Meeting, and Risk Appetite Statement at its December 2019 meeting.

At its September 17, 2020, meeting, the Board approved the annual reporting template and cycle for the Residual Heat Map and Risk Trajectory Dashboard.

Updates have been made as a result of Administration's annual review process, in accordance with the approved ERM Policy (CS-01:120), and provided to the Board for information, prior to the budget process each year, to ensure resources can be aligned to address or continue to address risk areas.

## COMMENTS

In its first iteration of the ERM Framework, Administration worked to identify all possible risks to the organization with the understanding that through regular monitoring and measuring of the Framework, refinements would be made to identify the Key Risks more accurately or appropriately to TBDSSAB.

The effectiveness of the ERM Framework is reviewed through an ongoing monitoring process. Through this process, the appropriateness of the various risks is confirmed with further refinements made as a result of Administration's review of the ERM over the previous year.

### ERM Summary Updates

#### ***1. Change from Tier 1 Risk to Tier 2 Risk***

Originally, all risks were defined as Tier 1 risks; however, starting with the first annual review in 2021, certain items were reclassified as Tier 2 risks based on further review, as well as the results of measuring the risks during that year.

That same process was completed during the annual review this year. As a result, additional items were identified as Tier 2 risks where limited exposure continued based on the history as well as the results of measuring the risks during the year, and continued application of the identified Key Controls.

Based on continued monitoring of results, risks identified as Tier 2 Risks in 2024 will remain classified as such; additional items were reclassified as Tier 2 Risks through this year's review. Tier 2 risks will continue to be monitored to ensure the classification to Tier 2 remains relevant, however, would not be reported within the Residual Heat Map, nor the Risk Trajectory Dashboard due to their low risk assessment and results during the previous year.

In particular, the following risks were reclassified as Tier 2 risks:

#	Description – Nature of Risk	Rationale
<b>B58</b>	Risk of perceived unfair procurement activities	This risk is deemed low based on historical evidence and existing management strategies.
<b>P24</b>	Risk that server recovery is not timely or complete so that client/tenant service is impacted (Hardware/software applications)	This risk is deemed low based on historical evidence and existing management strategies.
<b>P25</b>	Risk that telecommunication system cannot be recovered on a timely basis so that client/tenant service is impacted	This risk is deemed low based on historical evidence and existing management strategies.

<b>T54</b>	Risk that there is a breach of confidential data: A) Risk that confidential/client/tenant files/sensitive documents leave the building in an inappropriate manner B) Risk that email with key information is sent to incorrect individuals C) Risk that storage and communication devices will be stolen or misplaced or fail (laptops, phones, etc) D) Risk that hard-copy files are lost, misplaced or destroyed	This risk is deemed low based on historical evidence and existing management strategies.
<b>T55</b>	Risk that partners do not have robust and resilient infrastructure to support 7/24/365 service (programs will be offline for extended periods of time) and impact operations (externally-hosted software)	This risk is deemed low based on historical evidence and existing management strategies.

## **2. Combined Risks**

In previous annual reviews, certain risks were identified as being fundamentally similar and could be combined without losing the integrity of the nature of risk and its potential impact on TBDSSAB. No risks were identified during this year's review.

## **3. Risks Removed**

Risks were considered for removal if, after monitoring for the past year, it was determined that they are not a risk for TBDSSAB. No risks were identified for removal.

## **4. Other Updates**

Further clarification/revisions were made to the Nature of Risks throughout the ERM summary to more closely align with the intent of the risks for TBDSSAB.

The updated ERM Summary is provided in Attachment 1.

## Summary

With the updated ERM Summary, and based on the experiences across the organization, the Assessed Residual Risk was also updated.

Overall, the risk exposure has remained largely consistent with the previous years' assessment of the Types of Risk identified within the ERM Summary, and that the key controls continue to be effective to treat the risks. The following exceptions are noted:

- B57 Risk that unfavourable events (e.g., security breach) impact TBDSSAB's reputation
- P27 Risk that tenant activities (negligence or criminal) could impact building operations and displace tenants or require financial investment
- H61 Risk that tenant or patron behaviours (physical, violent, harassment) impact staff, stakeholders and other tenant/ patron safety (HQ and offices, TBDSSAB facilities, vehicles)

Risk has increased from *No Action Required*, to *Monitor*. Although these have been increased, TBDSSAB continues to put in place measures that continuously safeguard the assets of the organization as well as staff and tenants served.

The updated Residual Heat Map is provided in Attachment 2, and the resulting Risk Trajectory Dashboard is provided in Attachment 3.

## STRATEGIC PLAN IMPACT

Monitoring, reviewing and updating the Enterprise Risk Management System aligns with the financial stewardship component of the strategic plan to support a strong organization.

## FINANCIAL IMPLICATIONS

There are no immediate additional financial implications associated with this report. Future decisions related to the management of risk may impact resource allocation, and will be identified during the annual budget process, or as required.

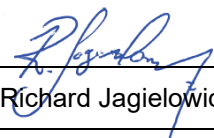

## CONCLUSION

It is concluded that the monitoring and updating of the ERM has been completed, and the results have been presented through the Residual Heat Map and Risk Trajectory Dashboard.

It is also concluded that Key Controls remain relevant to support the treatment of risk across the organization.

**REFERENCE MATERIALS**

- Attachment #1      [Updated Enterprise Risk Management Summary](#)
- Attachment #2      [Residual Heat Map](#)
- Attachment #3      [Risk Trajectory Dashboard](#)

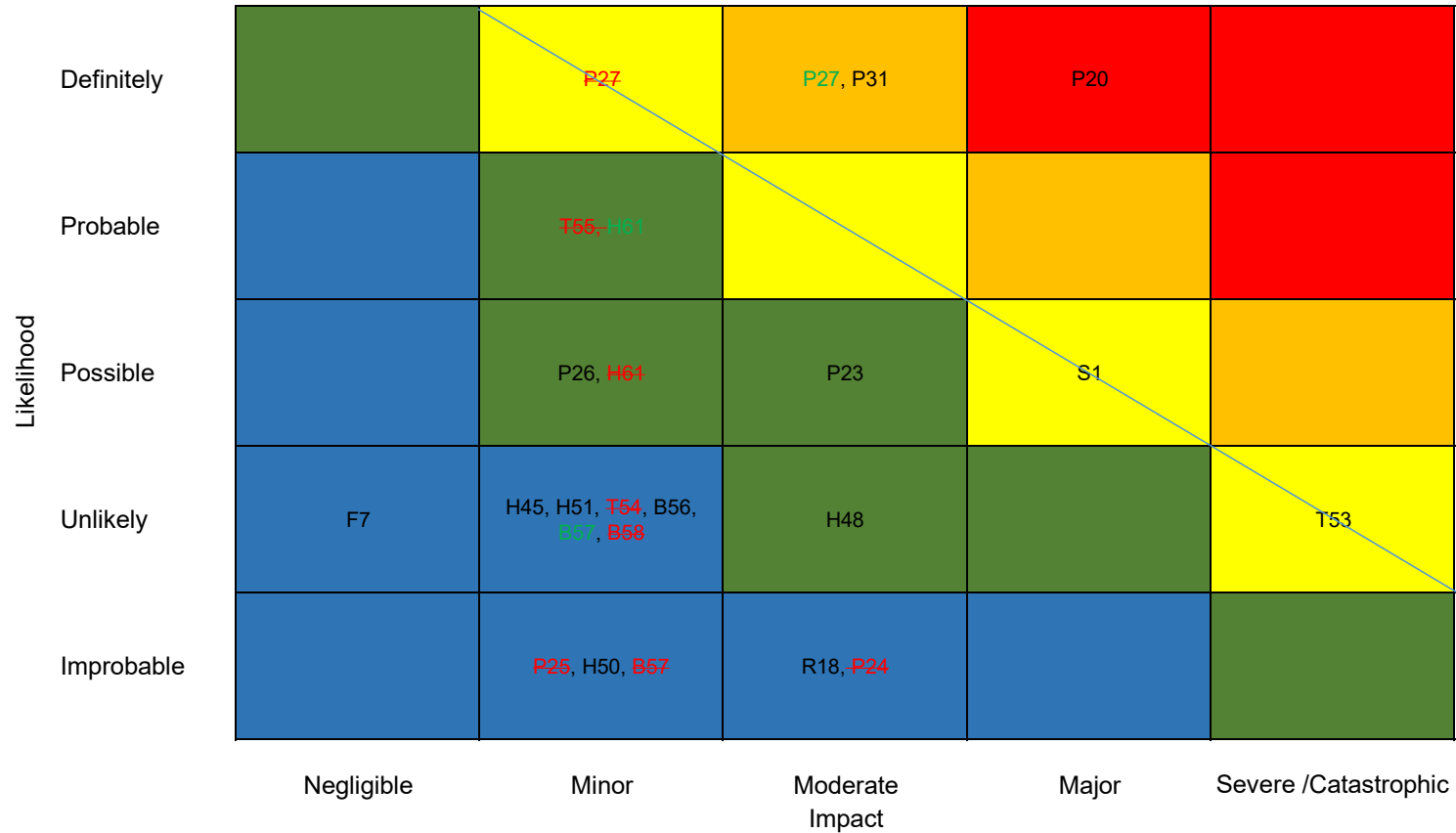
PREPARED BY:	Tafadzwa Mukubvu, CPA, Manager, Finance Shari MacKenzie, Manager, Human Resources Crystal Simeoni, Director, Integrated Social Services Division Richard Jagielowicz, CPA, CA, CBV Director, Corporate Services Division
SIGNATURE	
APPROVED BY	Richard Jagielowicz, CPA, CA, CBV Director, Corporate Services Division
SIGNATURE	
SUBMITTED BY:	Ken Ranta, Chief Executive Officer

Category	Type of Risk	#	Nature of Risk	Key Controls	Likelihood	Impact	Residual Risk Level
<b>STRATEGIC</b>  Risk of not being able to respond well to external changes as a result of inaction, ineffective strategies, or poor implementation of strategies	Management Information Risk	S1	Risk that information from funders about program operations is not available, timely, or accurate to enable informed decision-making and effective planning.	Proactively planning for local client/tenant needs, economic trends, and other factors impacting program delivery; monitoring monthly operational statistics; aligning resources through Performance Based Budgeting.	3	4	12
				Proper communication channels are in place to effectively communicate direction, program changes, etc.			
				Internal processes for finance, purchasing, IT; membership, effective management, professional development, best-practice research.			
				Proactively planning, process reviews, program realignment.			
<b>FINANCIAL AND LIQUIDITY</b>  Risk that TBDSSAB will be unable to meet its financial commitments in a timely manner (suppliers, lenders, investments, compensation, and benefits)	Financial Position Risk	F7	Risk of running an in-year operating deficit overall that can't be mitigated	Management processes, Levy Stabilization Reserve Fund, effective Reserve Fund Strategy, quarterly monitoring processes (i.e., variance reports); exceeding cost-sharing ratio, if required, with the ability to levy under DSSAB Act.	2	1	2
<b>REGULATORY/ COMPLIANCE</b>  Risk of not complying with regulatory and other obligatory authoritative requirements	Regulatory Change	R18	Risk that changes in building codes, fire safety requirements or regulatory inspections could have a financial and operational impact on current and future building operations	Planning, communication, capital reserves, external program funding.	1	3	3
<b>OPERATIONAL/ PROGRAMS</b>  The risk of operational/ program impact resulting from inadequate or failed internal processes, people and systems, or from external events	Environmental Risk	P20	Risk that Acts of Nature, including extreme weather events (fire, storm, wind, flood) or other events (explosion, power failure, biohazards) would negatively impact building operations and possibly displace tenants	Disaster Recovery Site; Property Insurance; HQ and Satellite Offices emergency plans; Reserve Funds.	5	4	20
	Property/ Equipment System Risk	P23	Risk that building systems' failures (heating, water heating, potable water, air exchange, emergency generators) could impact tenants and require financial investment	Emergency and Evacuation Plans, Property Insurance, Purchasing processes, Reserve Funds.	3	3	9
		P24 Move to Tier 2	<del>Risk that server recovery is not timely or complete so that client/tenant service is impacted- (Hardware/software- applications)</del>	<del>In-house expertise; Vendor/Partner Maintenance Agreements and SLAs- (Service-Level Agreements); OffSite and OnSite back-ups; Disaster Recovery Site; Network Security protocols; property insurance.</del>	4	3	3

Category	Type of Risk	#	Nature of Risk	Key Controls	Likelihood	Impact	Residual Risk Level
		<b>P25</b> <b>Move to Tier 2</b>	<del>Risk that telecommunication system cannot be recovered on a timely basis so that client/tenant service is impacted</del>	<del>In-house expertise; Vendor/Partner Maintenance Agreements and SLAs (Service Level Agreements); Off-Site and On-Site back-ups; Disaster Recovery Site; Network Security protocols; property insurance; mobile phones.</del>	<b>4</b>	<b>2</b>	<b>2</b>
		<b>P26</b>	Risk that Satellite Offices do not have appropriate, robust and resilient internet service infrastructure (vendor/ service provider) so that they cannot connect (via internet to HQ or other systems) for an extended period of time	Manual processes (paper documentation); back-up internet connection.	3	2	6
	Third-Party Risk	<b>P27</b>	Risk that tenant activities (negligence or criminal) could impact building operations and displace tenants or require financial investment	Security Infrastructure, Police relationships.	5	<b>2 3</b>	<b>15</b>
	Third-Party Risk (con't)	<b>P31</b>	Risk that community at large (inappropriate behaviour) negatively impacts TBDSSAB property (vandalism, dumping, theft)	Emergency plans, security systems, Resource centres, tenant support, use of alternate accommodations.	5	3	15
<b>HUMAN CAPITAL</b>  Risk associated with inadequate human resource policies, processes and practices to hire, develop and retain resources and appropriate competencies to operate the programs and maintain a safe, ethical, and non-discriminatory work environment that complies with employment law	Hiring/ Retention Risk	<b>H45</b>	Risk that we cannot attract suitable qualified candidates for key positions (skilled trades, technical, management )	Position description are monitored to ensure up-to-date requirements are identified; recruitment and selection practices/process. Comprehensive quarterly review of recruitment activities to identify trends.	2	2	4
		<b>H48</b>	Risk of unexpectedly losing a key member of the leadership team, or a high turnover rate (internal operations and public perception concerns)	Robust orientation and onboarding, Succession planning, documented policies and procedures, training.	2	3	6
		<b>H50</b>	Risk that labour discord impacts TBDSSAB work environment	Strong labour relations, planning, recovery site, use of external partners.	1	2	2
	Employee Misconduct	<b>H51</b>	Risk of violation of TBDSSAB Code of Conduct in the workplace (also brand reputation) and leads to negative legal/ reputation outcomes.	Appropriate onboarding, policies, procedures, training, supervision and corrective action. Annual review, and sign-off, of Policies and Procedures.	2	2	4

Category	Type of Risk	#	Nature of Risk	Key Controls	Likelihood	Impact	Residual Risk Level
	Third Party Risk	H61	Risk that tenant or patron behaviours (physical, violent, harassment) impact staff, stakeholders and other tenant/ patron safety (HQ and offices, TBDSSAB facilities, vehicles)	Emergency plans, security systems, alarms, emergency response schedule, security presence at HQ Intake, police presence, Resource Centres, insurance, use of alternate accommodations.  Appropriate corrective action, policies, procedures, protocols and training are in place.  Regular completion of Risk Assessments.	3-4	2	8
<b>TECHNOLOGICAL</b>  The risk associated with inappropriate access or use of information	Information Security Risk	T53	Risk of cyber threats and IT security vulnerabilities	IT infrastructure is current so that programming is supported to the extent possible/under the control of TBDSSAB.	2	5	10
				In-house expertise; Vendor/Partner Maintenance Agreements and SLAs (Service-Level Agreements); OffSite and OnSite back-ups; Disaster Recovery Site; Network Security protocols.			
				Mandatory Cyber Security training for all staff			
				Patch Management Procedure - CS-04:163-01			
	Information-Security Risk—Breach	<b>T54</b>  <b>Move to Tier 2</b>	Risk that there is a breach of confidential data: A) Risk that confidential/client/tenant files/sensitive documents leave the building in an inappropriate manner B) Risk that email with key information is sent to incorrect individuals C) Risk that storage and communication devices will be stolen or misplaced or fail (laptops, phones, etc) D) Risk that hard-copy files are lost, misplaced or destroyed	Confidentiality Agreements upon hire; security protocols for vendors within the building; records' management processes; policies and procedures; file encryption; file transportation security protocols; client communication protocols.	2	2	4
	Third-Party Risk	<b>T55</b>  <b>Move to Tier 2</b>	Risk that partners do not have robust and resilient infrastructure to support 7/24/365 service (programs will be offline for extended periods of time) and impact operations (externally-hosted software)	Manual processes (paper documentation); redundancy plans; back-up internet providers.	4	2	8
<b>BRAND/ REPUTATION</b>  The risk of the potential for negative publicity, public perception or uncontrollable events to have an adverse impact on TBDSSAB's reputation, thereby affecting program delivery.	Third-Party Risk	B56	Risk that a serious occurrence in a funded agency is reflected on TBDSSAB	Initiated Agreements process. Operational Reviews.	2	2	4
		B57	Risk that unfavourable events (eg., security breach) impact TBDSSAB's reputation	Policies, communications.	1-2	2	4
	Public Perception /Brand Risk	<b>B58</b>  <b>Move to Tier 2</b>	Risk of <u>perceived</u> unfair procurement activities	Broader Public Sector procurement directives; internal procurement policies and procedures; E-Bids and Tenders (transparent procurement processes); debriefing process.	2	2	4





Red	Immediate Focus/Action Required
Gold	Focus on best practice improvement
Yellow	Monitor, with a view to Best Practice improvement
Green	Monitor
Blue	No action required

Category	Type of Risk	#	Nature of Risk	Risk Exposure - Original Assessment*	Risk Exposure - at August 2024*	Risk Exposure at August, 2025	Trajectory**
<b><u>STRATEGIC</u></b>  Risk of not being able to respond well to external changes as a result of inaction, ineffective strategies, or poor implementation of strategies	Management Information Risk	<b>S1</b>	Risk that information is not available, timely, or accurate about program operations to enable informed decision-making				⇒
<b><u>FINANCIAL AND LIQUIDITY</u></b>  Risk that TBDSSAB will be unable to meet its financial commitments in a timely manner (suppliers, lenders, investments, compensation, and benefits)	Liquidity Risk	<b>F7</b>	Risk of running an in-year operating deficit overall that can't be mitigated				⇒
<b><u>REGULATORY/ COMPLIANCE</u></b>  Risk of not complying with regulatory and other obligatory authoritative requirements	Regulatory Change	<b>R18</b>	Risk that changes in building codes, fire safety requirements or regulatory inspections could have a financial and operational impact on current and future building operations				⇒
<b><u>OPERATIONAL/ PROGRAMS</u></b>  The risk of operational/ program impact resulting from inadequate or failed internal processes, people and systems, or from external events	Environmental Risk	<b>P20</b>	Risk that Acts of Nature, including extreme weather events (fire, storm, wind, flood) or other events (explosion, power failure, biohazards) would negatively impact building operations and possibly displace tenants				⇒
	Property/ Equipment System Risk	<b>P23</b>	Risk that building systems' failures (heating, water heating, potable water, air exchange, emergency generators) could impact tenants and require financial investment				⇒
		<b>P24</b>	<del>Risk that server recovery is not timely or complete so that client/tenant service is impacted (Hardware/software applications)</del>				⇒
		<b>P25</b>	<del>Risk that telecommunication system cannot be recovered on a timely basis so that client/tenant service is impacted</del>				⇒

Category	Type of Risk	#	Nature of Risk	Risk Exposure - Original Assessment*	Risk Exposure - at August 2024*	Risk Exposure at August, 2025	Trajectory**
		P26	Risk that Satellite Offices cannot connect for an extended period of time				⇒
	Third-Party Risk	P27	Risk that tenant activities (negligence or criminal) could impact building operations and displace tenants or require financial investment				↑
		P31	Risk that community at large (e.g., gangs, drugs) negatively impacts TBDSSAB property (vandalism, dumping, theft)				⇒
<b>HUMAN CAPITAL</b>							
Risk associated with inadequate human resource policies, processes and practices to hire, develop and retain resources and appropriate competencies to operate the programs and maintain a safe, ethical, and non-discriminatory work environment that complies with employment law	Hiring/ Retention Risk	H45	Risk that we cannot attract suitable qualified candidates for key positions (skilled trades, technical, management )				⇒
		H48	Risk of unexpectedly losing a key member of the leadership team, or a high turnover rate (internal operations and public perception concerns)				⇒
		H50	Risk that labour discord impacts TBDSSAB work environment.				⇒
	Employee Misconduct	H51	Risk of violation of TBDSSAB Code of Conduct in the workplace (also brand reputation), which may lead to negative legal/reputation outcomes.				⇒
		H61	Risk that tenant or patron behaviours (physical, violent, harassment) impact staff, stakeholders and other tenant/ patron safety (HQ and offices, TBDSSAB facilities, vehicles)				↑

Category	Type of Risk	#	Nature of Risk	Risk Exposure - Original Assessment*	Risk Exposure - at August 2024*	Risk Exposure at August, 2025	Trajectory**
<b>TECHNOLOGICAL</b>  The risk associated with inappropriate access or use of information	Information Security Risk	<b>T53</b>	Risk of cyber threats and IT security vulnerabilities				⇒
	<del>Information-Security-Risk—Breach</del>	<del><b>T54</b></del>	<del>Risk that there is a breach of confidential data: A) Risk that confidential/client/tenant files/sensitive documents leave the building B) Risk that email with key information is sent to incorrect individuals C) Risk that storage and communication devices will be stolen or misplaced or fail (laptops, phones, etc.) D) Risk that hard-copy files are lost, misplaced or destroyed</del>				⇒
	<del>Third-Party-Risk</del>	<del><b>T55</b></del>	<del>Risk that programs will be offline for extended periods of time, and impact operations (externally-hosted software)</del>				⇒
<b>BRAND/ REPUTATION</b>  The risk of the potential for negative publicity, public perception or uncontrollable events to have an adverse impact on TBDSSAB's reputation, thereby affecting program delivery.	Third-Party Risk	<b>B56</b>	Risk that a serious occurrence in a funded agency is reflected on TBDSSAB				⇒
		<b>B57</b>	Risk that unfavourable events (e.g., security breach) impact TBDSSAB's reputation				↑
	<del>Public-Perception-/Brand-Risk</del>	<del><b>B58</b></del>	<del>Risk of <u>perceived</u> unfair procurement activities</del>				⇒
<b>*Risk Exposure Legend</b>				<b>**Trajectory Legend</b>			
Red		Immediate Focus/Action Required		Significant Increase		↑	
Gold		Focus on best practice improvement		Moderate Increase		↑	
Yellow		Monitor, with a view to best practice improvement		No Change		⇒	
Green		Monitor		Decrease		↓	
Blue		No action required					