2024 Public Health Services Organizational Risk Management Plan

The chart below shows the current ratings for 2024 risks categorized by low, medium, and high.

IMPACT \ LIKELIHOOD	1	2	3	4	5
5		8.3 Information space limitations in key technology applications	8.1 Network outage		2.2 Impact and duration of direct disruptions to program and service delivery due to the cybersecurity incident
4		6.1 outdated organizational policies and procedures 13.1 Health inequities 14.4 Change to Provincial policies and the Ontario Public Health Standards	10.1 Privacy breaches	5.1 ineffective management of records and information throughout its lifecycle 9.1 Incomplete risk management implementation	2.1 Lack of capacity to meet growing demand

LIKELIHOOD

IMPACT	1	2	3	4	5
3	12.1 Theft of assets or physical harm in facilities 1.3 Financial fraud or corruption		3.1 Precarious staffing 4.1 Environmental emergency 8.2 Use of dated software/technology or ones reaching end of life 8.5 Non-compliance with provincial legislation as it relates to privacy, security, records, and information management 9.2 Elected officials' balancing responsibilities 9.3 Impact of changing priorities with changes in local positions and Board of Health governance structure		

LIKELIHOOD

IMPACT	1	2	3	4	5
2		1.4 Unfinished capital projects due to the inability to spend Provincial funding within required timeframe 7.1 Non-compliance with varied program obligations imposed by statues and regulations	1.1 Uncertainty related to the impact of programs and services due to budget pressures 1.2 Financial forecasting gaps 11.2 Negative image due to reduced access to services 11.3 Negative image due to limits in data sharing	6.2 Unmet strategic goals due to competing priorities between the City of Hamilton and the Ministry of Health 8.4 Insufficient capacity to improve existing and implement new information technologies and processes	
1					

2024 Public Health Services Organizational Risk Management Plan

Overall Objective: Public Health Services will use a formal risk management framework that identifies, assesses, and addresses risk.

2. Operational / Service Delivery Risks	
ID #	**2.1**
RISK IDENTIFICATION	
Risk Exposure	The Board of Health may not be able to fully address increased demand and expectations of public health's role in the community due to the integration of COVID-19 work into existing business operations and other issues arising from a lack of capacity.
Description of Risk	- Adapting to the evolution of Public Health Services' role post-pandemic, as it relates to immunizations, emergency response, and communications, may be challenging as Provincial COVID-19 funding ended in December 2023. - There are competing Council-directed priorities at the local level that reflect the multi-faceted needs and interests of the community, which may impact Public Health Services' ability to deliver planned core public health programs and services. - Some recruitment and retention challenges remain that are resulting in limited resources available to meet the growing demands of public health programs and services in the community.
Cause/Source of Risk	- The new Provincial funding levels are less than increases in wages, benefits, and inflation, alongside rising costs associated with population growth and increased service demand, resulting in budget pressures. - The Ministry of Health has also discontinued Provincial COVID-19 funding at the end of December 2023 and directed that this work be integrated into existing programs, services, and business processes and funded by the existing cost-shared base budget. - Public Health Services is responsible for addressing its population's health needs in accordance with the Ministry of Health's Ontario Public Health Standards and the City of Hamilton's Strategic Plan using its finite resources. There is an increase in the number of corporate requests, beyond what is captured in the Annual Service Plan and Budget, that Public Health Services receives from its Council and Senior Leadership Team, which limits Public Health Services' ability to address service demands and advance priorities.

Cause/Source of Risk	- The recent approval of a new Public Health Standing Committee by the City of Hamilton's Council introduces changes to the governance structure of Public Health Services for the first time since 2006 by including community representatives. This new structure may impact the decisions made and the decision-making process surrounding public health matters.
RISK ASSESSMENT	
Current Controls/ Mitigation Strategies (What Are We Doing?)	1. Continue to identify Public Health Services' priorities and related action areas by balancing core public health functions and mandates, local population health needs, Council priorities, and Provincial direction. 2. Identify and communicate Public Health Services' priorities and action areas to adapt and improve existing programs and services to address population health needs. 3. Regularly review program and financial performance data to ensure effective delivery of services in an efficient and fiscally responsible manner.
Rating Scale 1 (Low) - 5 (High) (Likelihood x Impact)	**L5, I4**
RISK REDUCTION	
Action Plan (What Else Can We Do?) Only for High Risks	1. Continue to identify Public Health Services' priorities and related action areas by balancing core public health functions and mandates, local population health needs, Council priorities, and Provincial direction. 2. Continue to strategically allocate resources with the least impact on service levels and staff. 3. Strengthen program efficiency, while preserving essential services to improve population health outcomes for equity-deserving populations. This includes adapting programs for ongoing COVID-19 work, piloting Public Health Services Centres that integrate public health services in high-needs neighbourhoods, and engaging with communities and partners on public health needs. 4. Realign core supports to best practices and evolving public health role. 5. Continue participating in Provincial discussions on the roles and responsibilities of public health at the local level. 6. Continue to regularly review program and financial performance data to demonstrate accountability and ensure effective delivery of services in an efficient and fiscally responsible manner. 7. Continue to raise key issues and participate in corporate discussions related to recruitment and retention. Participate in corporate recruitment and retention improvements.

Action Plan (What Else Can We Do?) Only for High Risks	8. Request Human Resources to analyze staff demographics to inform the development of targeted retention strategies for different workforces. 9. Work with Human Resources to implement short-term continuous quality improvement activities to support recruitment (e.g., periodic positing to have a staffed candidate pool) and increase job satisfaction.
Person(s) Responsible	1. Public Health Leadership Team (PHLT) 2. PHLT, Finance & Administration (F&A) 3-5. PHLT 6. PHLT, F&A 7-9. PHLT, Public Health Services' Human Resources Business Partner
Estimated Residual Risk Once Action Plan is Fully Implemented (Likelihood x Impact)	**L3, I3**

ID #	**2.2**
RISK IDENTIFICATION	
Risk Exposure	The impact and duration of direct disruptions to program and service delivery from the cybersecurity incident, which has hindered access to critical documents, applications, and communication and connectivity infrastructure.
Description of Risk	- Uncertainty surrounding the recovery of data or files and access to networks. - Inability to access core business planning and reporting documents. - Inability to retrieve policies, procedures, records, medical directives, and other critical documents from shared network drives. - Service disruptions due to the inability to use communication and connectivity infrastructure, such as phone lines, Wi-Fi, fax machines, and other City network applications.
Cause/Source of Risk	- Ongoing recovery efforts resulting from the cybersecurity incident. - Continued challenges with communication and connectivity infrastructure due to the cybersecurity incident.

RISK ASSESSMENT	
Current Controls/ Mitigation Strategies (What Are We Doing?)	1. Maintain open and transparent communication with staff, partners, and service users to keep them informed about the cybersecurity incident and ongoing recovery efforts. 2. Implement alternative work arrangements, such as remote work and temporary relocation, to minimize the impact of service disruptions. 3. Provide training and raise staff awareness about cybersecurity best practices to mitigate the risk of future incidents. 4. Maintain detailed documentation of the cybersecurity incident, including impact assessments and recovery efforts.
Rating Scale 1 (Low) - 5 (High) (Likelihood x Impact)	**L5, I5**
RISK REDUCTION	
Action Plan (What Else Can We Do?) Only for High Risks	1. Prioritize and restore critical applications needed for service delivery in collaboration with Corporate IT. 2. Collaborate with Corporate IT to identify and restore the most impacted programs and services, ensuring compliance with legislative and regulatory requirements. 3. Implement backup and recovery plans for quick restoration of critical data and systems. 4. Identify and implement secure workarounds that prioritize privacy and comply with Records and Information Management policies. 5. Conduct a comprehensive analysis of the cybersecurity incident's impact on Public Health Services. 6. Based on the analysis, develop action plans to mitigate and minimize the impact of risks arising from future cybersecurity incidents. 7. Develop recovery plans within Public Health Services for post-access restoration, including supporting programs to ensure smooth transitions from interim to normal state operations post-cybersecurity incident. 8. Allocate resources to support Corporate IT's restoration and recovery efforts. 9. Identify and maintain accessible backups of 'critical documents'. 10. Enhance program business continuity plans to address network outages and IT dependencies, including contingency strategies, annual reviews, and key information and privacy policies for leaders during disruptions.

Action Plan (What Else Can We Do?) Only for High Risks	11. Collaborate with Corporate IT and cybersecurity experts to assess vulnerabilities, strengthen defenses, and develop robust incident response plans. 12. Maintain detailed documentation of the cybersecurity incident, including impact assessments and recovery efforts, to aid in future planning, reporting, and risk management plans.
Person(s) Responsible	1. Public Health Leadership Team (PHLT), Epidemiology & Wellness (EW) Division Director, Data Management (DM) Program Manager, Corporate IT 2. Corporate IT, DM Program Manager 3. Corporate IT 4. DM Program Manager 5-6. Emergency Response Coordinator, DM Program Manager, Planning & Competency Development (P&CD) Program Manager 7. DM Program Manager 8. Corporate IT, DM Program Manager 9. EW Division Director, DM Program Manager 10. Emergency Response Coordinator, EW Division Director, DM Program Manager 11-12. Corporate IT, DM Program Manager
Estimated Residual Risk Once Action Plan is Fully Implemented (Likelihood x Impact)	**L2, I3**

5. Information / Knowledge Risks	
ID #	**5.1**
RISK IDENTIFICATION	
Risk Exposure	The Board of Health faces a potential risk of ineffective records and information management throughout its lifecycle.
Description of Risk	Public Health Services' varied information management practices and the lack of a formal record management platform may lead to information loss, privacy breaches, and non-compliance with record management obligations, including privacy and security requirements.

Cause/Source of Risk	There is an absence of robust records management policies, training, systems, and governance to support Public Health Services' ability to effectively meet the records and information management requirements
RISK ASSESSMENT	
Current Controls/ Mitigation Strategies (What Are We Doing?)	1. Re-established Public Health Services' internal Privacy, Security and Information Management (PSIM) Committee. 2. Completed a review of existing privacy and records and information management policies. 3. Developed new privacy and records and information management policies.
Rating Scale 1 (Low) - 5 (High) (Likelihood x Impact)	**L4, I4**
RISK REDUCTION	
Action Plan (What Else Can We Do?) Only for High Risks	1. Identify and address gaps in records and information management policies, including the development of necessary policy documents. 2. Provide staff training on privacy and records and information management policies across Public Health Services, including Corporate IT staff authorized to access Public Health Services' records. 3. Identify and address any governance gaps in records and information management. 4. Data Management Program Manager to participate as a Corporate Enterprise Data Management Steering Committee member.
Person(s) Responsible	1-3. Epidemiology & Wellness (EW) Division Director, Data Management (DM) Program Manager 4. DM Program Manager
Estimated Residual Risk Once Action Plan is Fully Implemented (Likelihood x Impact)	**L3, I3**

8. Technology Risks	
ID #	**8.1**
RISK IDENTIFICATION	
Risk Exposure	The Board of Health remains at risk of a network outage, threats to network security and hard files, and loss of access to critical applications impacting service delivery.
Description of Risk	The recent cybersecurity incident caused network outages, phone and fax line disruptions, and loss of access to critical applications, which significantly impacted Public Health Services' ability to work effectively and/or carry out some of its work.
Cause/Source of Risk	- Technology error or external disaster. - Risk of outage at the local and/or provincial levels. - Introduction of new technologies, increased mobile technology use, and exposure to network or cybersecurity threats.
RISK ASSESSMENT	
Current Controls/ Mitigation Strategies (What Are We Doing?)	1. Implement the City's Cybersecurity Incident Response Plan. 2. Implement Public Health Services' business continuity plans. 3. Apply corporate-led security hardening measures. 4. Use interim alternative business processes. 5. Plan for the transition from mitigation to recovery in collaboration with Corporate IT and Public Health Services program areas.
Rating Scale 1 (Low) - 5 (High) (Likelihood x Impact)	**L3, I5**
RISK REDUCTION	
Action Plan (What Else Can We Do?) Only for High Risks	1. Activate Public Health Services' emergency management structure to navigate the immediate and long-term impacts of any network outages. 2. Develop protocols and communications to enable teams to work in an offline environment and/or remotely. 3. Coordinate the implementation of appropriate measures to reduce security breaches and network issues. 4. Coordinate the implementation of other Corporate-led security hardening measures to reduce security breaches and network issues.

Action Plan (What Else Can We Do?) Only for High Risks	5. Collaborate with Corporate IT to support mitigation and recovery for Public Health Services programs to resume normal business operations with improvements where needed. 6. The Data Management Program to support Public Health Services programs with mitigation and recovery measures as required to resume normal business operations with necessary improvements. 7. The Data Management Program to respond and collaborate with Corporate IT on all information needs, application testing, and assessing any data loss and/or functionality as part of the Emergency Operations Centre response. 8. Ensure business requirements and privacy impact assessments are completed for all software used by Public Health Services, collaborating with IT to ensure effective implementation. 9. Work with Corporate IT to ensure compliance with corporate policies, including in-house solutions. 10. Complete required cybersecurity trainings. 11. Continue to participate in provincial programs to mitigate risks to applications.
Person(s) Responsible	1. Medical Officer of Health 2. Public Health Leadership Team 3-8. Data Management (DM) Program Manager 9. Corporate IT, DM Program Manager 10-11. DM Program Manager
Estimated Residual Risk Once Action Plan is Fully Implemented (Likelihood x Impact)	**L3, I5**

9. Governance / Organizational Risks	
ID #	**9.1**
RISK IDENTIFICATION	
Risk Exposure	The Board of Health may be at risk of incomplete risk management due to the delay in fully implementing the risk management framework in Public Health Services' program and project planning due to the cybersecurity incident.

Description of Risk	Effective risk management and mitigation plans require understanding risk management principles. This has not been shared at the program level since before 2020; this gap may lead to unprepared responses to emergencies, such as cybersecurity incidents.
Cause/Source of Risk	- Limited documented mechanisms are in place to prioritize work across Public Health Services based on risk assessment. - Delay in implementing the previously developed 2024 Public Health Services Organizational Risk Management Plan due to the cybersecurity incident.
RISK ASSESSMENT	
Current Controls/ Mitigation Strategies (What Are We Doing?)	1. Continue to use the Public Health Services Risk Management Framework to identify and assess organizational risks. 2. Incorporate risk assessment into program and project planning processes.
Rating Scale 1 (Low) - 5 (High) (Likelihood x Impact)	**L4, I4**
RISK REDUCTION	
Action Plan (What Else Can We Do?) Only for High Risks	1. Continue to use the Public Health Services Risk Management Framework to identify and assess organizational risks. 2. Re-establish risk management practices at the program and project levels.
Person(s) Responsible	1. Public Health Leadership Team (PHLT) 2. PHLT, All Public Health Services' Program Managers

Estimated Residual Risk Once Action Plan is Fully Implemented (Likelihood x Impact)	**L3, I3**

10. Privacy Risks	
ID #	**10.1**
RISK IDENTIFICATION	
Risk Exposure	The Board of Health faces potential risks such as privacy breaches, unauthorized external access to Public Health Services' information, and non-compliance with privacy legislation (i.e., the Personal Health Information Protection Act and the Municipal Freedom of Information and Protection of Privacy Act).
Description of Risk	- Privacy breaches may occur due to staff or technology errors. Public Health Services may lack sufficient policies, procedures, security, and management mechanisms to ensure compliance with privacy policies and legislation. - External cybersecurity threats targeting health care and municipalities are increasing, and may result in unauthorized access to sensitive data and the loss of organizational records.
Cause/Source of Risk	Use of outdated technology (e.g., faxing), the introduction of new technologies, unrecognized third-party vendor outsourcing for security requirements, lack of Public Health Services policies for the acquisition and use of non-standard applications, increased mobile technology use, and required organizational process changes due to Information and Privacy Commissioner of Ontario decisions and orders.

RISK ASSESSMENT	
Current Controls/ Mitigation Strategies (What Are We Doing?)	1. A review of existing privacy and records and information management policies was completed. 2. Developing new or updated privacy and records and information management policies are in progress. 3. Updating and revising a privacy training e-module. 4. Ongoing monitoring of incidents and breaches, with process, policy, and procedure adjustments as needed. 5. Sharing a summary of privacy, security, and records and information management concerns with Corporate IT Services. 6. Enhancing the protection of technology assets by implementing corporate-led security hardening measures.
Rating Scale 1 (Low) - 5 (High) (Likelihood x Impact)	**L3, I4**
RISK REDUCTION	
Action Plan (What Else Can We Do?) Only for High Risks	1. Increase staff awareness of and competence in applying privacy policies with updated e-modules and tailored training for Public Health Services and relevant Corporate IT staff. 2. Transition the e-module to the Corporate Learning Management System, which all Public Health Services staff must complete annually. Note that Public Health Services' policy requires annual privacy training. 3. Engage Corporate IT to address concerns of the Privacy, Security and Information Management (PSIM) Committee. 4. Engage a consultant to evaluate Office 365 and its ability to meet Public Health Services' privacy, security, records and information management, and business requirements, as well as to develop an implementation plan. 5. Continue to educate, prohibit, and restrict Public Health Services staff's use of any corporate enterprise software solutions that Public Health Services has not yet approved for use.
Person(s) Responsible	1-5. Epidemiology & Wellness Division Director, Data Management Program Manager

Estimated Residual Risk Once Action Plan is Fully Implemented (Likelihood x Impact)	**L3, I4**