Request for Proposals (RFP)

Toronto Neighbourhoods' Assessment Framework (TNAF)

Options Analysis of Technical Platforms for the TNAF Public Platform

1. Invitation

United Way Greater Toronto (UWGT) invites qualified consultants or community-based organizations with demonstrated expertise in community data platforms, public-facing analytics tools and applied research infrastructure to conduct an options analysis of technical platforms for the Toronto Neighbourhoods' Assessment Framework (TNAF).

The purpose of this engagement is to identify and assess possible technical platform options that could support the future public-facing TNAF platform and to provide recommendations that will inform a subsequent procurement for platform design and development. This is a planning and decision-support exercise only.

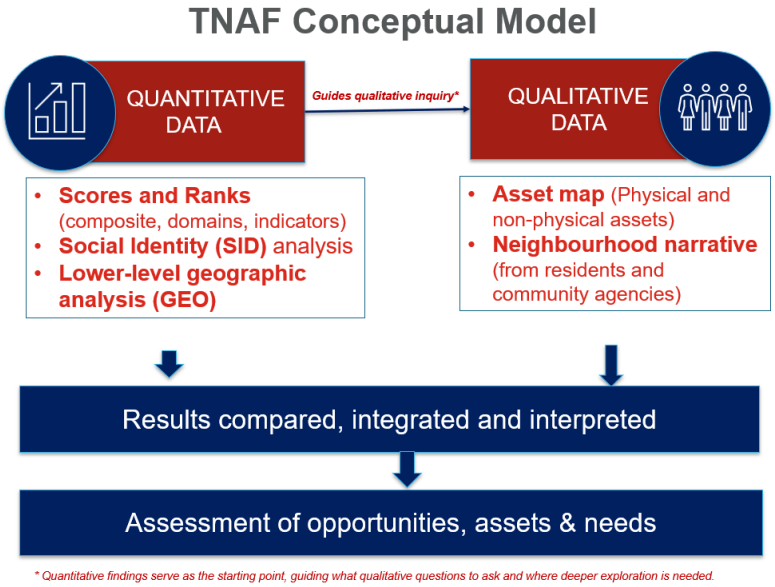
A separate consultant will be engaged later to design, build, and test a prototype of the selected platform. The outputs of this assignment are intended to directly inform the scope and design of that subsequent prototyping work.

Specifically, the consultant will:

- Review TNAF project documentation and technical requirements;
- Develop a Business Requirements Document (BRD). The BRD must be used a key input to the options analysis and must inform the assessment of potential technology platforms that could be used to prototype, design, develop and implement the future system.
- Conduct a market scan and comparative assessment of potential platform options;
- Recommend the most suitable platform(s), supported by a clear rationale and implementation considerations.

2. Background

Since 2023, the City of Toronto (City) and United Way Greater Toronto (United Way) have collaborated on the Toronto Neighbourhoods' Assessment Framework (TNAF)—a process to develop an evidence-driven community well-being tool designed to understand **opportunities, assets, and needs** within and across Toronto neighbourhoods and communities. Rooted in a history of partnership aimed at building stronger neighbourhoods and more equitable communities, TNAF refines and expands upon the legacy of the Urban HEART@Toronto neighbourhood equity index by integrating both quantitative and qualitative data.



- **Phase 1 (2023)** resulted in a community-informed conceptual model for TNAF and preliminary quantitative and qualitative data plans.
- **Phase 2a (2024)** focused on the quantitative components of TNAF, testing and validating indicators for 17 replicable measures.
- **Phase 2b (2025)** emphasized the qualitative elements of TNAF. A wide range of partners—including community leaders, residents, service providers, and design experts—were engaged to co-design the qualitative component. This includes asset mapping, storytelling, and other participatory methods to fill gaps and add nuance to the quantitative indicators.
- **Phase 3 (current)** is focusing on testing and refining the framework- including developing a working prototype or conceptual public platform. As part of this work, UWGT is seeking an independent assessment of technical platform options before making implementation decisions.

Expected Functionality of the Future TNAF Public Platform

The future TNAF public platform is expected to be a public-facing data and storytelling platform integrating curated quantitative data and qualitative insights collected externally through community engagement processes.

It supports the following core functions:

- Present neighbourhood-level data through interactive geospatial maps and dashboards;
- Integrate quantitative data (e.g., scores and ranks) and qualitative content (e.g., community stories, assets, and other narrative-based information);
- Support search, filtering, and navigation by geography, domain, and indicator where applicable
- Provide an accessible, user-friendly experience for a broad public audience;
- Allow periodic updates as new qualitative data and quantitative data is made available;
- Support future scalability as the TNAF framework may evolve.
- Ensure compliance with accessibility, privacy, and security requirements relevant to public-sector platforms

The platform is **not expected to support public crowdsourced content submission**. All qualitative content will be collected externally through engagement processes and curated internally before publication.

3. Scope of Work

The consultant will complete the following activities:

3.1. Project Review and Business Requirements Document (BRD)

The consultant will begin the engagement by reviewing key TNAF project documentation and developing a Business Requirements Document (BRD) for the future TNAF public platform. The BRD will establish a technology-neutral foundation for the options analysis and must be used as a key reference point when assessing and comparing potential technology platforms.

The consultant will:

- Participate in a project kickoff meeting with UWGT and possibly the City of Toronto.
- Review key TNAF documentation provided by UWGT, including relevant reports, the conceptual model, and quantitative and qualitative data plans.
- Confirm the functional requirements that the future platform should support.
- Develop a **Business Requirements Document (BRD)**.

The BRD will define:

- Functional requirements
- Non-functional requirements (performance, accessibility, scalability, security)
- Data requirements (quantitative and qualitative integration)
- Governance and compliance requirements
- Technical and integration requirements:
    - **Canadian hosting and data residency:** Platform options should be assessed for their ability to host production data, backups, logs, analytics, and related support data in Canada, including any cross-border data processing or access considerations.
    - **Privacy and compliance:** Assessment should consider alignment with applicable privacy obligations and the secure handling of personal information, sensitive community data, qualitative narratives, and metadata.
    - **Security controls:** Platform options should be assessed for authentication and access control, role-based administration, encryption in transit and at rest, audit logging, security monitoring, and available vendor security certifications or assurance reports.
    - **Accessibility and inclusive design:** Platform options should support WCAG 2.1 AA or the current applicable accessibility standard, including usability for mobile users, assistive technologies, and a broad public audience.
    - **Data integration and interoperability:** Assessment should consider the ability to ingest, manage, update, and display quantitative indicators, GIS or geospatial data, qualitative content, and public-facing metadata, as well as export options and potential API or connector availability.
    - **Content management and publishing workflow:** Platform options should be assessed for ease of content updates, administrative usability for non-technical staff, approval workflows, version control, and support for periodic updates as new data becomes available.
    - **Scalability, performance, and reliability:** Assessment should consider expected public usage, dashboard and map performance, ability to add indicators or neighbourhood-level content over time, uptime expectations, backup and recovery approach, and disaster recovery considerations.
    - **Platform ownership and portability:** Assessment should consider ownership of data, configuration, content, design assets, documentation, and source code where applicable, as well as the ability to migrate content and data if UWGT or the City of Toronto changes platforms in the future.
    - **Long-term sustainability:** Assessment should consider licensing model, dependency on proprietary tools or vendors, availability of implementation partners, long-term support requirements, and the total cost of ownership, including implementation, hosting, licensing, maintenance, training, and future enhancements.
        - **Data residency** - Canadian hosting/ data residency and compliance with applicable privacy requirements
        - **Privacy and compliance** –
            - alignment with applicable privacy obligations
            - Clear handling of personal information, sensitive community data and qualitative narratives
        - **Security Controls** –

- Security certifications and practices (e.g., SOC 2, ISO 27001 or equivalent)
- WCAG 2.1 AA or current applicable accessibility standard
- Usability for public audiences, including mobile users and assistive technologies

The BRD must be:

- sufficiently detailed to support a subsequent procurement process and prototype development;
- technology-neutral;
- validated with UWGT (and City of Toronto where applicable)
- structured so that a subsequent prototype and development consultant can use it to design a prototype demonstrating the expected functionality of the future TNAF public platform outlined in this RFP.

3.2. Options Analysis

The options analysis must be grounded in the approved BRD. Each platform option should be assessed against the business requirements.

The analysis should consider different platform approaches, including but not limited to:

- Business intelligence and dashboard platforms (e.g., Power BI)
- GIS-based platforms (e.g., ArcGIS Online)
- Open-source or custom web-based solutions
- Existing community well-being or neighbourhood indicator platforms used by other jurisdictions
- Other suitable technologies identified by the consultant

Platform options should be assessed against the BRD and criteria such as:

- Functionality (data visualization, search, filtering, and content management)
- Ability to integrate quantitative (numeric data like scores and ranks) and qualitative content (asset map and neighbourhood narrative)
- User experience for public audiences
- Accessibility and equity considerations
- Data governance, privacy, and security
- Ease of maintenance and future scalability
- Indicative implementation and ongoing operating costs

Evaluation criteria and weighting will be developed in consultation with UWGT and the City of Toronto. A numeric scoring framework and heat matrix are encouraged.

3.3. Recommendations and Implementation Considerations

- The consultant will prepare:
  - A comparison of 3-5 assessed platform options with advantages, limitations, and trade-offs of each shortlisted option, preferably presented in a numeric scoring heat matrix.
  - A recommendation on the most suitable platform(s) for TNAF, with clear rationale
  - Potential implementation risks, assumptions, and dependencies.
  - Hosting, data residency, and platform ownership considerations, including whether each recommended platform can be hosted in Canada and how Canadian data residency requirements would affect privacy, security, compliance, support access, vendor dependency and platform ownership.

- A summary of estimated monthly and annual costs, including hosting, licensing, and usage-based pricing models (e.g., storage, compute, API/credit consumption), with clear assumptions.
- Guidance on the technical, staffing, and financial resources required to implement and sustain the platform over time

3.4. Technical Coordination

The consultant will participate in meetings with UWGT and the City of Toronto's IT staff to understand existing technical environments, platform requirements, and implementation considerations. Insights from these discussions should inform the final recommendations.

4. Deliverables and Timeframe

The following table outlines the deliverables and a suggested timeframe. If the deliverables can be delivered earlier, this would be a bonus. Deliverables marked with an asterisk (*) require approval from United Way and the City of Toronto.

Deliverable/Milestone	Timeline
RFP released	July 8
Proposal submission deadline	July 21
Selection and awarding of contract	July 22-July 24
Kick-off meeting	Week 1 of engagement
Review of project documentation	Week 1 of engagement
Draft Business Requirements Document *	Week 1-2 of engagement
Draft Options Analysis*	Week 3-5 of engagement
Presentation of findings to UWGT and City	Week 6 of engagement
Final Options Analysis report*	Week 6 and 7 of engagement
Final Business Requirements Document*	Week 8 and 9 of engagement
Project close-out meeting	End of engagement

5. Budget

The expected budget for this project is up to **CAD $13,000 + HST.**

6. Consultant Qualifications

The successful consultant should demonstrate experience in one or more of the following areas:

- Conducting data platform evaluations or option analyses, particularly for public-sector, municipal, or non-profit contexts
- The Consultant must be familiar with Canadian municipal and government systems
- Experience with public-facing data systems such as dashboards, GIS platforms, or digital analytics tools
- Strong project management capacity to meet deadlines and ensure high-quality deliverables
- Demonstrate the ability to provide independent, platform-agnostic advice and assess technology options objectively. This includes experience in developing evaluation frameworks, comparing platform trade-offs, assessing technical architecture and implementation considerations, and preparing recommendations to inform a future procurement process.
- Knowledge of Data Governance and Equity-based government policies, initiatives or strategies.

Additional assets (preferred but not required):

- Knowledge of community well-being frameworks or neighbourhood indicator initiatives.
- Experience integrating quantitative and qualitative information into public-facing platforms.
- Experience working with municipal governments, non-profit organizations or community agencies
- Familiarity with accessibility standards and equity-informed digital design.

7. Proposal Requirements

The proposal should not exceed 2,500 words (12-point font), excluding appendices (CV, writing samples, references). It should include:

7.1. Name, Contact, and Reference Information

- Lead consultant and project team
- Relevant qualifications and experience
- Roles and responsibilities
- Two references from similar projects

7.2. Proposal

- **Project Understanding**: Overview of how the applicant interprets the scope, its requirements, and the approach to fulfilling it.
- **Methodologies**: Description of the proposed approach, including research methods, platform assessment methodology, evaluation criteria and how recommendations will be developed
- **Relevant Experience:** Provision of 2-3 examples of similar projects
- **Work Plan**: Timelines and key milestones.
- **Itemized Budget** aligned with the proposed work plan including daily rates.
- Completed UWGT CYBERSECURITY DUE DILIGENCE CHECKLIST FOR AGENCIES AND PARTNER ORGANIZATION document (refer to attached questionnaire with same title)

7.3. Applicants should describe how they will ensure the platform options analysis is independent, transparent, and not unduly influenced by vendor relationships or implementation preferences.

8. Submission Instructions

Please submit **one (1) electronic copy** of your proposal by **Tuesday, July 21, 2026, no later than 11:59 p.m. (EST)** to:

Thi Anh Nguyen
Senior Manager, Research and Evaluation
United Way Greater Toronto
Email: anguyen@uwgt.org
Subject/Reference: TNAF Options Analysis

All candidates can anticipate a response regarding the status of their application by **July 24, 2026.**

For inquiries related to this RFP, please get in touch with Thi Anh Nguyen at anguyen@uwgt.org.

We appreciate your time and look forward to reviewing your proposal.

United Way Greater Toronto

UWGT CYBERSECURITY DUE DILIGENCE CHECKLIST FOR AGENCIES AND PARTNER ORGANIZATION

Control	Control Name	Questions for Technology team	Responses
1.	Make an Inventory of Authorized Devices	How do you track devices that have been approved for use? Are you automatically alerted if an unapproved device connects to the network?	
2.	Make an Inventory of Authorized or Unauthorized Software	How do you track software installed on devices that access the network? Are you automatically alerted if unapproved software is installed on a network device?	
3.	Standard Secure Configurations	Has the firm established standardized secure configurations for desktops, laptops, mobile devices and network equipment (such as servers)?	
4.	Vulnerability Assessment and Remediation	How do you actively monitor for network vulnerabilities? Frequency What tools do you use? What security certification do you have? If you do external audits, can you provide the results of your most recent external audit	
5.	Malware Defenses	Do you have anti-malware software installed on workstations and servers? Do you use software to ensure that anti- malware software is active and working as intended on workstations and servers? Have you disabled the “auto-run” feature when USB drives, CDs and DVDs are inserted into workstations.	

Control	Control Name	Questions for Technology team	Responses
6.	Application Security	What systems and software are accessible over the internet? How are those systems and software protected from attack and/or segregated from other more sensitive data and systems? How do you assess the security controls implemented by third party service providers (such as 3rd party donation solution providers, customer relationship management software vendors)? What are you doing to prevent breaches?	
7.	Wireless Devices	Does the firm allow network access over wifi? If so, what protections are in place? Are there limits on employees' use company equipment on public wifi?	
8.	Data Recovery Capability	Do you test your backups and restoration ability for the operating system, the software, and the data? Are there multiple people who know how to restore the operating system, software and data from backup? Are backups encrypted and physically secure?	
9.	Security Skills Assessment and Training	Do the IT professionals have access to the training that they need? Are employees trained by IT on important policies and procedures? Do senior executives understand enough to make informed decisions about IT staffing, budgeting, and policy development?	

Control	Control Name	Questions for Technology team	Responses
10.	Secure Configurations for Network Hardware	Do you systematically change default passwords on network hardware? How do you control who within the firm can electronically access network hardware?	
11.	Control use of Administrator Privileges	How does the firm limit the employees who are granted system administrator privileges? How does the firm actively track all of the accounts that have been granted system administrator privileges? Do system administrator logins require multi- factor authentication?	
12.	Boundary Defense	Do you actively monitor for network attacks? How does IT track data transfers between the firm and partner organizations (such as technology SME or administrators)?	
13.	Audit Logs	How is remote network access activity logged? Do you log attempts to access files or folders that are not authorized?	
14.	Access Controls	How does the firm compartmentalize data and only give access to employees on a need- to-know basis?	
15.	Account Monitoring and Control	Do you periodically scan for inactive accounts? How do you disable access for terminated employees? Do you log attempts to access deactivated accounts?	
16.	Data Loss Prevention	Do you encrypt mobile storage media (such as laptops and thumb drives)?	

Control	Control Name	Questions for Technology team	Responses
		Do you use network-based data loss prevention software?	
17.	Incident Response and Management	Is there a written incident response plan? In the event of an information security breach, is there a member of senior management who would support IT's response efforts and needs? How soon will UWGT be notified if case of a breach or suspected security incident?	
18.	Secure Network Engineering	Is the network configured to separate sensitive data from more vulnerable systems (such as software accessible by the internet)?	
19.	Penetration Testing	Does the firm conduct any penetration testing? In what frequency? Does the firm scan for network files or emails containing the word "password"?	
20.	Work From Home	What measures has your agency/organization implemented to adjust for remote or hybrid work?	
21.	Other questions	Do you have cyber security or liability insurance?	