

CONSULTING AGREEMENT

McKinsey & Company Canada (“McKinsey”) and Manitoba Public Insurance Corporation (the “Client”), for good and valuable consideration the receipt and sufficiency of which is acknowledged, agree to the following terms in connection with consulting services that McKinsey will provide to the Client.

1. SERVICES. The working arrangements, including scope of the services, Deliverables (as defined in the Proposal), team composition and workplan, are described in McKinsey’s proposal initially presented September 13, 2021 as updated and finalized on October 7, 2021 and attached as Schedule A (the “Proposal”). The services shall include the work required to complete everything set out in the Proposal, and the parties may meet at mutually agreed times to discuss the progress of the services and to exchange feedback (the “Services”).

In order to be able to complete the Services within the agreed timeframe and budget and to fulfill its responsibilities on a timely basis, McKinsey will rely on the Client’s timely cooperation, including the Client making available relevant data, information and personnel, performing any tasks or responsibilities assigned to the Client and notifying McKinsey of any issues or concerns the Client may have relating to the Services. During the course of the Services, priorities may shift or unexpected events may occur which may necessitate changes to the Services. In this event, the parties will jointly discuss the anticipated impact on the Services and agree on any appropriate adjustments, including to the scope of work, timeframe and budget.

2. SERVICE DELIVERY. The delivery of the Services covered by this Agreement will be in accordance with the section “How we would partner together” set out in the Proposal. At each schedule meeting the Client’s core team will provide information, advice and feedback to McKinsey’s core team related to their progress. If there are any material disagreements that cannot be resolved by the core teams, these will be escalated to McKinsey’s Senior Partner on the Core Team, and the Client’s CEO for resolution and direction.

3. ACCEPTANCE OF DELIVERABLES. The Parties agree the acceptance procedures for Deliverables that are set out below. The acceptance procedures include the acceptance criteria, the period or length of time for acceptance (e.g. time for reviews, etc.), and the process for addressing failure of Deliverables to conform to the acceptance criteria.

The acceptance criteria are that the Deliverables:

1. Provide full and complete answers and clearly articulated solutions to the applicable “Questions to answer” as set out in the Proposal.
2. Meet the standard that they provide actionable recommendations (tactical and strategic as applicable) that will enable the Client to improve its ability to execute and deliver its Project NOVA transformation initiative.

The acceptance procedures are as follows:

1. If the Client determines that a Deliverable meets the acceptance criteria, in all material respects, the Client shall notify McKinsey in writing of Client’s acceptance of the Deliverable, within a 10-day period. In the absence of any notification within the 10-day period, the Deliverable will be considered to have been accepted by the Client.
2. If the Client determines that a Deliverable does not meet the acceptance criteria, in all material respects, the Client shall notify McKinsey in writing of Client’s rejection of the Deliverable, and describe in reasonable detail in such notice the Client’s basis for rejection of the Deliverable, within a 10-day period.
3. Upon receipt of notice of rejection, McKinsey shall, within a 10-day period, modify or improve the Deliverable at McKinsey’s sole expense so that the Deliverable meets, in all material respects,

acceptance criteria, and notify the Client in writing that it has completed such modifications or improvements and re-submit the Deliverable to Client.

- 4. Client shall then review the modified or improved Deliverable within 10-days of receipt of the McKinsey's delivery of the Deliverable. Failure of the Deliverable to meet in all material respects, the acceptance criteria after the second round of review shall constitute a default by McKinsey.
- 5. In the event of such default, Client may either (i) notify McKinsey of such default and instruct McKinsey to modify or improve the Deliverables, or (ii) notify McKinsey of such default and instruct McKinsey to cease work on the Deliverable, in which case McKinsey shall refund to Client all amounts paid by Client related to such Deliverable. Such refund shall be in addition to, and not in lieu of, any other remedies Client may have for McKinsey's default.

4. TEAM COMPOSITION. The Team Composition listed in the Proposal will be considered McKinsey's Designated Personnel to carry out the Services. McKinsey shall not substitute other personnel for those designated without the prior written consent of the Client. If any Designated Personnel become no longer available for any reason, McKinsey shall supply a similarly experienced and skilled individual as soon as practicable subject to approval of such individual by the Client.

McKinsey shall not engage or retain any agent, subcontractor or any other third party for purposes of providing the Services hereunder in whole or in part without the prior written consent of the Client (which cannot be unreasonably withheld) and on terms and conditions satisfactory the Client in its sole discretion. The use of any agents, subcontractor, or any other third parties by McKinsey shall in no way relieve McKinsey from its responsibility and obligation to provide the Services in accordance with the provisions of this Agreement.

5. COMPENSATION. The Client shall compensate McKinsey for its professional fees and expenses in connection with the Services, as set forth in the table below:

#	Service Description	Quantity	Unit Price	Extended Price
	Digital 2020 (Agile 360)			
	- Solution Fee Fee			
	Team B (Agile 360)			
	- Weekly Service Fee			
			Total	\$2,233,125

The Client agrees that it will not, without McKinsey's prior written permission, disclose the terms of this agreement or any Proposal (including McKinsey's fees, expenses and other commercial terms) to any third parties (including the Client's external procurement and other service providers).

McKinsey will invoice the Client for professional fees and expenses in connection with the Services monthly or as otherwise set forth in the applicable Proposal. All invoices are due and payable immediately on presentation. Should any invoice remain unpaid for more than 30 days after presentation, interest will accrue on the outstanding amount at the rate of 1% per month, calculated from the 31st day after presentation until the date of payment.

6. CONFIDENTIALITY. McKinsey will keep confidential any confidential information, including any personal data (as defined below), furnished by the Client to McKinsey in connection with the Services ("Confidential Information"). McKinsey will disclose Confidential Information only to its employees, agents and contractors who have a need to know and are bound to keep it confidential, will use Confidential Information only for purposes of performing the Services, including preparing Proposals and evaluating

potential Services, or as otherwise requested or authorized by the Client, and will protect Confidential Information in accordance with the McKinsey Data Protection Protocols available at <https://solutions.mckinsey.com/msd/data-protocols.pdf> (the “Protocols”).

Subject to its confidentiality obligations, where the agreed upon Services include benchmarking services McKinsey may also incorporate Confidential Information into its benchmarking databases for use in reporting on sanitized or aggregate trends and metrics without attribution to the Client. To bring the best of McKinsey’s global resources to serve the Client, the Client agrees that McKinsey may transfer Confidential Information to geographies other than those in which it was collected or received, including to McKinsey affiliates and sub-processors that comprise or support McKinsey’s infrastructure and maintenance functions as set forth in the Protocols, to facilitate any activities authorized by the Client, provided that at all times Confidential Information will be treated as confidential and protected in accordance with the terms of this agreement.

Confidential Information shall not include information that is or becomes publicly available, already known to McKinsey, independently acquired or developed by McKinsey or legally required to be disclosed. McKinsey will reasonably cooperate with the Client, at its expense, in responding to any legally required disclosure.

In performing the Services, McKinsey will use and rely primarily on information available from public sources and the Confidential Information, and Client acknowledges that it is authorized to provide McKinsey with such Confidential Information for its use in connection with the agreed Services and that McKinsey will have no obligation to independently verify such information.

At the Client’s election and notification to McKinsey, McKinsey shall promptly return or destroy any Confidential Information, including any personal data, in its possession or control when the same is no longer necessary for the provision of the Services, provided that McKinsey may retain such Confidential Information only as required by applicable law, regulation or documented professional archival policy or as otherwise authorized or instructed by the Client. Any Confidential Information so retained shall at all times remain subject to the terms and conditions of this agreement, including with respect to confidentiality, security and non-disclosure.

7. **DATA SECURITY.** Without limiting the foregoing, if McKinsey processes data as part of the Services and on behalf of the Client which relates to an identified or identifiable person (“personal data”), McKinsey shall (i) only process such personal data, including with respect to McKinsey’s use of subcontractors or sub-processors, as set forth in this agreement and the Protocols, as otherwise authorized in writing by the Client, or as required by applicable law, (ii) implement appropriate technical and organizational measures to protect such personal data as set forth in the Protocols, (iii) promptly notify the Client of any incident in which the confidentiality, integrity or security of the personal data has been compromised, and (iv) collaborate with the Client as required by applicable law or the Client’s request to document the personal data, data subjects and processing activities related to the Services, including as part of an applicable Proposal.

In the event that the Client transfers personal data that is subject to the General Data Protection Regulation (2016/679) to McKinsey outside of the European Economic Area, or where otherwise agreed by the parties or required by applicable law, the parties agree that the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (or any successor thereto), as applicable to McKinsey’s Services and available at <https://solutions.mckinsey.com/msd/sccs.pdf> shall be deemed automatically incorporated into this agreement and binding upon the parties hereto, unless an alternate data transfer arrangement authorized by applicable law is agreed by the parties.

McKinsey will comply with the Client’s reasonable requests to furnish information regarding McKinsey’s processing activities as is reasonably necessary to enable the Client to verify that McKinsey is complying with its obligations under this agreement, including by making its Director of IT Security or person of comparable knowledge and position available to provide information about the Protocols and McKinsey’s processing in connection with the Services, and the foregoing shall apply in full satisfaction of any Client audit or inspection

rights of McKinsey, but shall not limit or restrict the ability of any legal or regulatory authority to conduct such audit or inspection pursuant to applicable law.

The Client does not store any personal data outside of Canada, and the parties acknowledge that the General Data Protection Regulation will not be applicable to the Services provided under this Agreement. In addition, McKinsey does not and will not collect, use, or have access to personal data for the performance of the Services; and the Client acknowledges and agrees that it does not and will not provide access to any personal data to McKinsey.

All services performed by McKinsey under this Agreement, including remote work, will be performed in Canada or the United States, and will align to the Client's Remote Work Security Standard, attached as Appendix 1. If circumstances change such that the restrictions in the applicable governmental health advisories related to COVID-19 are lifted or relaxed, or if it otherwise becomes necessary for the Services to be performed on premises, Client will take all requisite or recommended precautions for the safety of the personnel at Client's premises and, prior to and as a condition to any such attendance on premises, the Parties will, acting reasonably, agree to mutual covenants designed to safeguard the health and safety of the personnel of both Client and McKinsey.

8. INTELLECTUAL PROPERTY. Upon payment in full of McKinsey's fees, the Client will own all reports and other deliverables prepared for and furnished to the Client by McKinsey in connection with the Services (the "Deliverables"), save that McKinsey retains ownership of all concepts, know-how, tools, questionnaires and assessments, modules, courses, frameworks, software, algorithms, databases, content, models, and industry perspectives developed or enhanced outside of or in connection with the Services (the "McKinsey Tools"), it being understood that none of the McKinsey Tools will contain the Client's Confidential Information.

To the extent the Deliverables include any embedded McKinsey Tools, McKinsey hereby grants the Client a non-exclusive, non-transferable, non-sublicenseable, worldwide, royalty-free license to use and copy the McKinsey Tools solely as part of the Deliverables and subject to the limitations herein on disclosure of McKinsey materials and publicity. The Client agrees that, without McKinsey's prior written permission, it will not, or permit any third party to (a) access, copy or reverse engineer any McKinsey Tool or Deliverable, or (b) remove or circumvent security or technological safeguards, including notices, digital protection mechanisms, metadata, watermarks, or disclaimers provided with any McKinsey Tool or Deliverable.

9. DISCLOSURE OF MCKINSEY MATERIALS; PUBLICITY. McKinsey's work for the Client is confidential and for the Client's internal use only. McKinsey will not disclose the Deliverables to any third parties without the Client's prior written permission. Similarly, the Client agrees that it will not disclose any materials or information that McKinsey furnishes to the Client, including the Deliverables, to any third parties without McKinsey's prior written permission, unless required to do so by law. Each party further agrees not to use the other party's name or trademarks in any communication with any third party without the other party's prior written permission.

McKinsey acknowledges and accepts that Client may be required to provide Deliverables to the Manitoba Public Utilities Board (PUB), provided that Client agrees to only provide Deliverables to the PUB through a confidential submission process, unless otherwise approved in writing by McKinsey. Through such confidential process, the PUB and all parties to a General Rate Application Proceeding in receipt of the Deliverables (e.g. the PUB panel, intervenors and consultants) will be required to keep the Deliverables confidential and sign the PUB's approved form of non-disclosure agreement, and undertaking to destroy all confidential information at the end of such proceeding.

10. SERVING COMPETITORS. It is McKinsey's long-standing policy to serve competing clients and clients with potentially conflicting interests as well as counter-parties in merger, acquisition and alliance opportunities, and to do so without compromising McKinsey's professional responsibility to maintain the confidentiality of client information. Consistent with such practice and McKinsey's confidentiality obligations

to its other clients, McKinsey is not able to advise or consult with the Client about McKinsey's serving the Client's competitors or other parties. Nothing in this section shall operate to limit or reduce McKinsey's obligations with respect to the Client's Confidential Information, including the confidentiality and non-disclosure obligations with respect thereto.

11. LIMITATION OF LIABILITY. The Services shall not be deemed investment, legal, tax, accounting or other regulated advice. McKinsey does not supplant the Client's management or other decision-making bodies and does not guarantee results. The Client remains solely responsible for its decisions, actions, use of the Deliverables and compliance with applicable laws, rules and regulations. The Client agrees to pay for any costs, including attorney fees, McKinsey incurs as a result of its participation as a non-party in any legal, regulatory, administrative or other proceeding relating to the Services. In no event shall McKinsey's liability to the Client in connection with the Services relating to an engagement for the Client exceed the fees received by McKinsey from the Client in connection with such engagement. Neither party will be liable for any lost profits or other indirect, consequential, incidental, punitive or special damages.

12. DISPUTE RESOLUTION. The parties shall first attempt to settle any dispute arising out of or relating to the interpretation of this Agreement and any Services, Acceptance Criteria and Deliverables provided hereunder (the "Dispute") through good faith negotiations in the spirit of mutual cooperation between representatives of each of the Parties with authority to resolve the Dispute.

Any Dispute remaining unresolved for more than sixty (60) days following a party's first notification of the issue under the Dispute to the other party or such longer period as the parties may mutually agree upon shall, as promptly as is reasonably practicable, be resolved by arbitration pursuant to the Arbitration Rules of the ADR Institute of Canada, Inc. (the "Arbitration Rules") that are in force at the time the Dispute is subject to arbitration. For certainty, the Parties hereby waive any right they may otherwise have to bring a court action in connection with a Dispute, except for injunctions or other equitable remedies required to address breaches of Confidentiality, or violations of Intellectual Property rights. The Parties also waive any right they may otherwise have to bring or participate in a class, collective or representative proceeding in connection with a Dispute, whether in court or before an arbitrator.

The arbitrator's decision shall be final, conclusive and binding upon the Parties, and the Parties shall have no right to appeal or seek judicial review of the arbitrator's decision. For certainty, the Parties hereby waive any right of appeal which may otherwise be available under applicable legislation or under the Arbitration Rules.

As a result of the COVID-19 global pandemic and travel restrictions the parties agree to make reasonable efforts to conduct the arbitration virtually on a mutually agreeable platform. If the parties and the arbitrator cannot agree to conduct the arbitration virtually on a mutually agreeable platform, the place of arbitration shall be in Toronto, Ontario.

13. TERM AND TERMINATION. This agreement takes effect on the date it is signed by the last of the two parties to sign this Agreement. The Services will then commence and shall continue until all Deliverables have either been accepted by the Client, or terminated in accordance with its terms. Except as otherwise provided in the applicable Proposal, either party may terminate the Services at any time effective upon written notice to the other and, in the event of such termination, the Client will pay McKinsey's fees and expenses up to the effective date of termination.

14. MISCELLANEOUS. This agreement and the Proposals constitute the entire agreement between the parties, and there are no prior or contemporaneous oral or written representations, understandings or agreements relating to this subject matter that are not fully expressed herein or therein. The Client warrants that it has obtained and complied with all relevant statutory and any other applicable approvals, provisions and requirements surrounding the authorization, negotiation, award, conclusion, signature and any other applicable aspect of this agreement including but not limited to any applicable public procurement regulation, in particular, as to the lawfulness of awarding this agreement to McKinsey on a sole-sourced basis. This agreement and the Proposals shall be governed by and construed in accordance with the laws of the Province

of Ontario without regard to conflicts of law principles and shall inure to the benefit of and be binding on the successors and assigns of the Client and McKinsey. The following Sections shall survive the completion or any termination of the Services: 6 (Confidentiality), 7 (Data Security), 8 (Intellectual Property), 9 (Disclosure of McKinsey Materials; Publicity), 10 (Serving Competitors), 11 (Limitation of Liability), 13 (Term and Termination) and 14 (Miscellaneous) and any other provision which by law or by its nature should survive. Neither party may assign its rights or obligations under this agreement to any person or entity without the written consent of the other party, not to be unreasonably withheld, provided, however, that either party may assign its rights and obligations under this agreement to its affiliates upon reasonable written notice to the other party but without the written consent of the other party. Assignment shall not relieve either party of its obligations hereunder. McKinsey is an independent contractor and not the Client’s agent or fiduciary. Notwithstanding any course of dealings of the parties at any time or any statement to the contrary contained therein, no purchase order, invoice or other similar document issued by a party shall be construed to modify the terms of this agreement. Rights and remedies provided in this agreement are cumulative and not exclusive of any right or remedy provided at law or in equity.

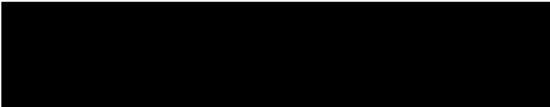
The parties agree that this Agreement may be signed in counterparts and each part shall when taken together be binding upon the parties. The parties agree to the use and acceptance of digital or electronic signatures.

In witness whereof: duly authorized representatives of the parties have signed this Agreement effective the dates noted below.

Manitoba Public Insurance Corporation

McKinsey & Company Canada

Eric Herbelin
Digitally signed by Eric Herbelin
Date: 2021.10.08 14:45:14 -05'00'



Name: Eric Herbelin
Title: President and CEO
Date: 10/8/21

Name: Erez Eizenman
Title: Senior Partner
Date: October 11, 2021

August 2, 2023

CONFIDENTIAL

MPI Exhibit #16
2024 GENERAL RATE APPLICATION
Part IX – EXP Appendix 23a - Redacted

June 15, 2023

CONFIDENTIAL

2024 GENERAL RATE APPLICATION
Part IX – EXP Appendix 23a - Confidential

McKinsey
& Company

Diagnostic of MPI's digital transformation program

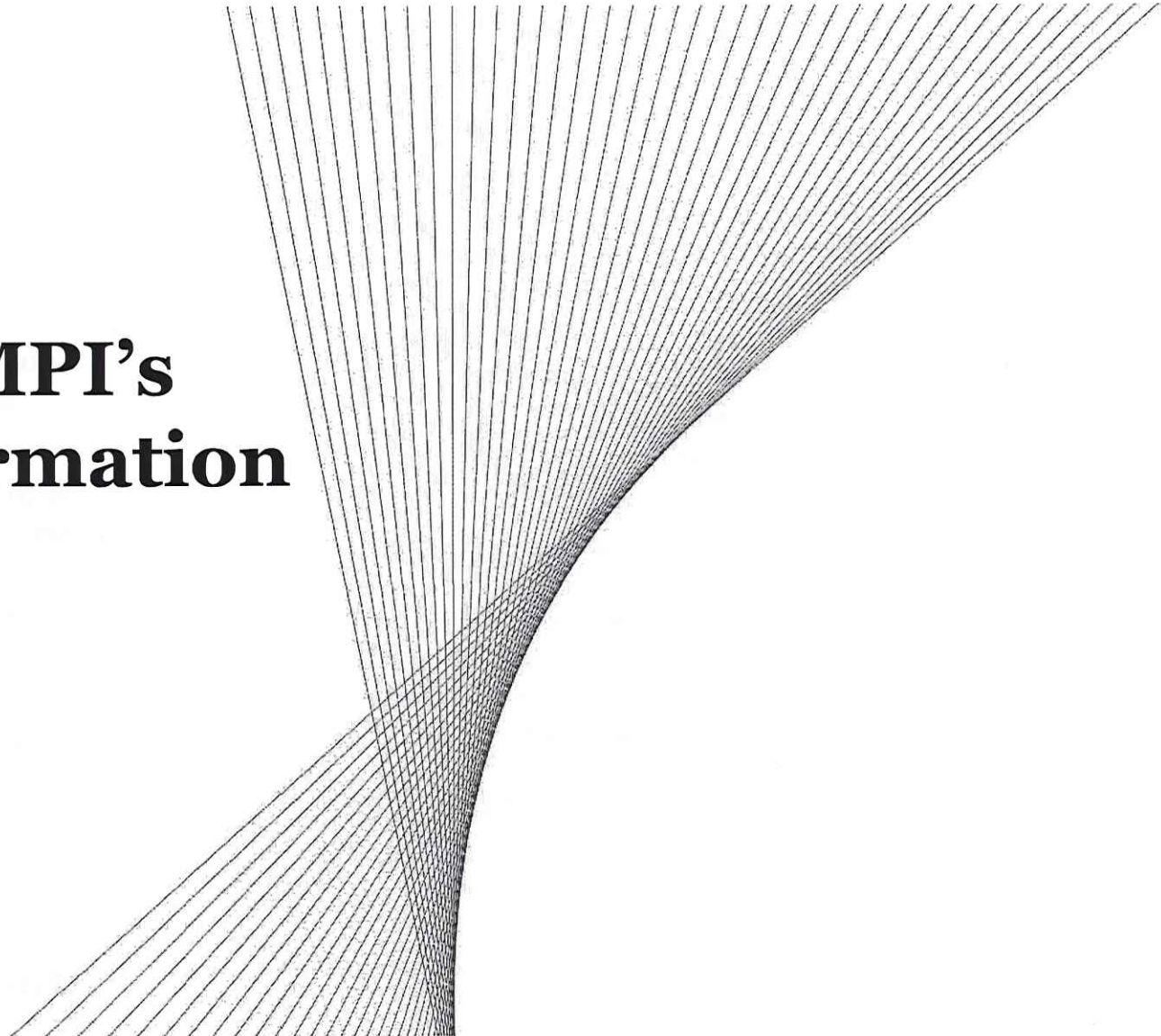
Partnership proposal

October 07, 2021



MANITOBA
PUBLIC INSURANCE

CONFIDENTIAL AND PROPRIETARY
Any use of this material without specific permission of McKinsey & Company
is strictly prohibited



Our understanding of your context and objectives

Context

MPI has recently launched **Project Nova**, a bold digital transformation to give customers more choice and a better experience

The primary deliverables of Project Nova are the **implementation of two COTS solutions, of new Partner and Customer Portals, and of an integration platform solution** to enable the integration of all systems

The Nova program has recently experienced **challenges with execution effectiveness and identified capability gaps**, resulting in potential risks to benefits realization

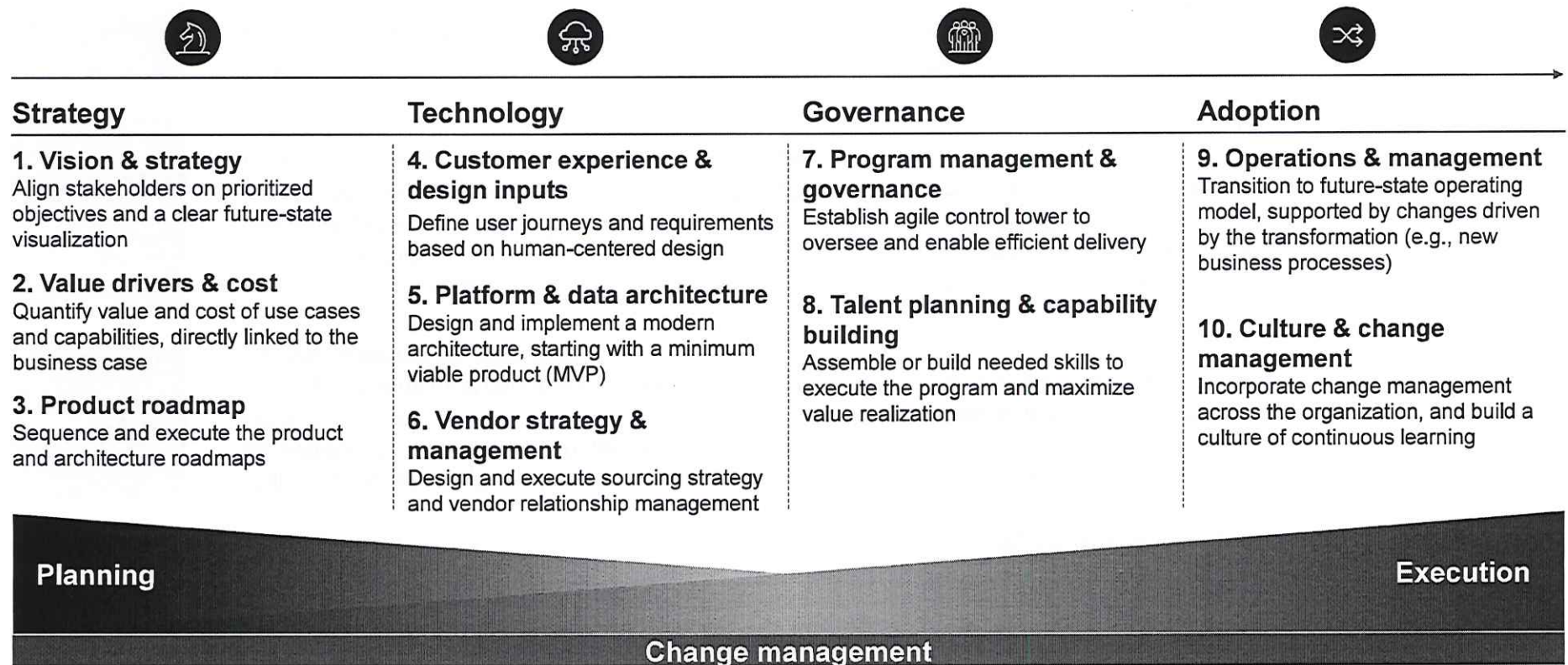
Objectives

MPI is seeking an independent partner to diagnose Nova and make recommendations to de-risk the program, to ensure the organization will achieve its transformation objectives, and to assure the realization of the expected value from this strategic investment.

The diagnostic should include:

- **Strategy:** validate that the program scope and roadmap will enable achievement of the business objectives and maximize value from investments
- **Technology:** ensure the technology foundations and capabilities required to achieve the business goals are included in the target state architecture
- **Governance:** validate that the program operating model, talent and skills will enable efficient delivery and effective risk mitigation

Digital transformation programs need to get ten critical factors right in order to minimize risk and assure value delivery



Main questions to answer and proposed approach to address them

Key questions

Key sources of insight and deliverables

Strategy

- Will the program scope and roadmap enable achievement of the business objectives and maximize value from investments?
- If not, what additional capabilities are required / how can the roadmap be enhanced?

- **Outside-in pressure test of current NOVA business case**, building from case library of similar transformations
- **Holistic diagnostic of the NOVA program** using McKinsey’s proprietary Value Assurance approach

Technology

- Are the technology foundations and capabilities (e.g., data, cloud, infosec, cyber) required to achieve the business goals included in the target state architecture?
- What risks are inherent in current legacy systems?
- What are the most important customer journeys and outcomes?

- **Architecture review and recommendations**, leveraging McKinsey’s global expert network to review current plans vs. that from peers
- **Prioritized set of journeys**, building McKinsey’s proprietary insurance journey taxonomy and extensive cross-industry core system transformation practice

Governance

- Will the program operating model, talent and skills enable efficient delivery and effective risk mitigation?
- How should MPI prioritize scope and investments in line with the expected outcomes of the program?
- Does MPI have the right internal capabilities to execute the transformation? If not, which capabilities require investment?

- **Benchmarking of current operating model** against industry leading practices and peer case examples – pinpointing specific internal capabilities to invest in
- **Integrated recommendations on governance**, leveraging McKinsey’s ‘control tower’ approach to large scale digital transformation program delivery

Agenda

Proposed approach to diagnose the Nova program

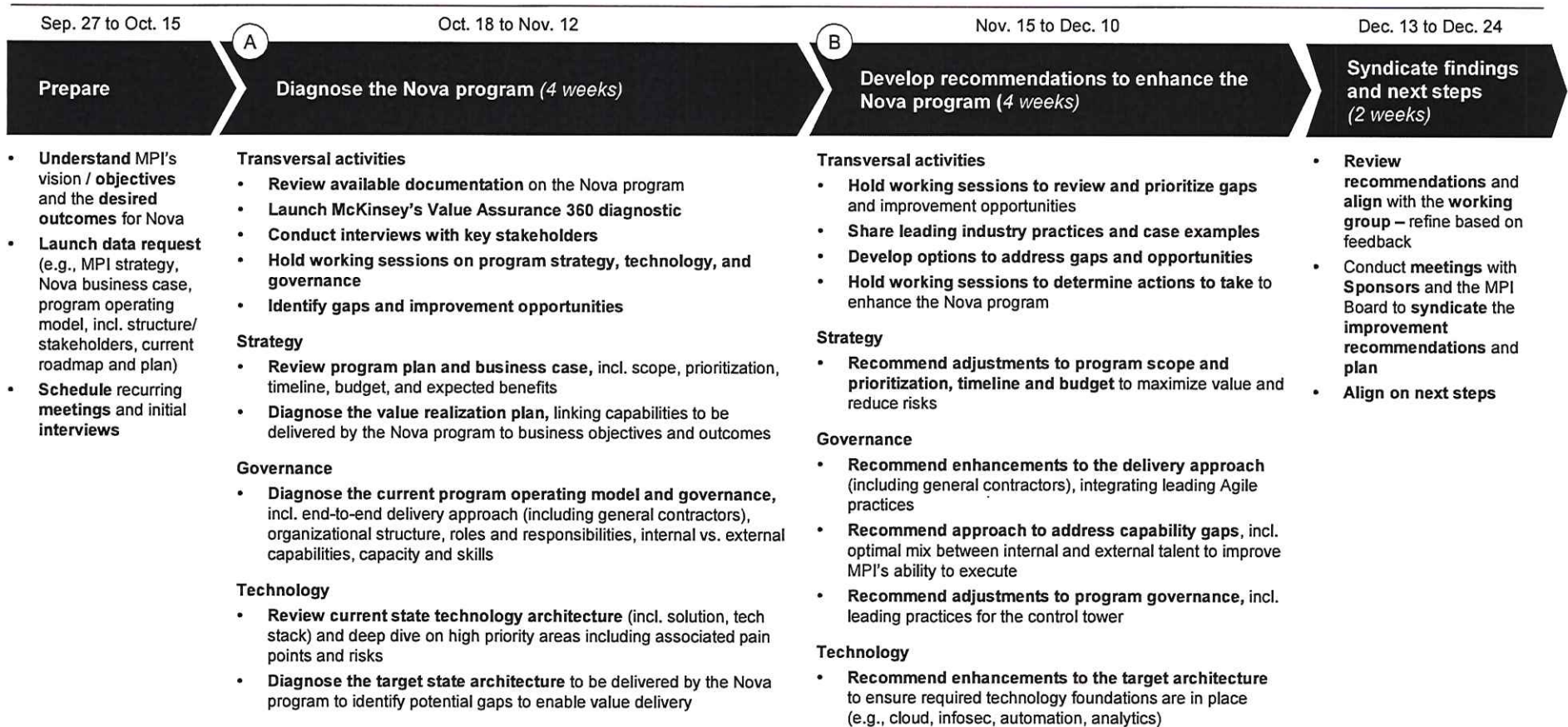
Team structure and profiles

Why McKinsey?




Professional arrangements

Proposed approach to diagnose and develop recommendations to enhance the Nova program

Tentative schedule; will be confirmed once the contract is finalized



A: Diagnose the Nova program

 Questions to answer	 Approach	 Deliverables
<p>Strategy</p> <ul style="list-style-type: none"> • What outcomes is MPI trying to achieve? What are the specific measures that you're trying to improve (e.g., KPIs)? • Is Nova's current plan and approach optimal to achieve the desired outcomes? <p>Governance</p> <ul style="list-style-type: none"> • Does MPI have the necessary digital talent, capabilities (e.g., Design, Agile, Cloud) and capacity to execute and sustain the transformation? • Where are additional talent, skills, and capabilities required in order to sustain the transformation? <p>Technology</p> <ul style="list-style-type: none"> • What are priority customer journeys to transform in order to achieve MPI's objectives? • Are the required technology foundations (e.g., architecture, cloud, infosec) in place to deliver against priority capabilities? 	<p>Strategy and Governance</p> <ul style="list-style-type: none"> • Deploy McKinsey's proprietary Value Assurance (VA) 360 diagnostic solution • Interview the 10-15 most important stakeholders from multiple organizations / functions / partners • Interview the 5-10 stakeholders leading and using digital capabilities • Review project documentation (business case, program plan, op. model etc.) • Identify high-level recommendations for the scope including prioritization, structure, governance and approach to improve the value realization • Determine the MPI's digital maturity and prioritize the capabilities required to execute Nova • Identify the largest project risks and mitigations <p>Technology</p> <ul style="list-style-type: none"> • Develop common taxonomy using McKinsey's insurance practice & prioritize • Review technical project documentation (cust. journeys, solution arch., tech stack etc.) • Conduct end-to-end review of tech. architecture and customer journeys • Identify technology potential gaps and high-level recommendations enable value delivery 	<p>Strategy and Governance</p> <ul style="list-style-type: none"> • Summary of VA360 results, VA index score and synthesized findings • High-level program improvement opportunities • Summary of MPI's Digital capability maturity findings • Prioritized list of Digital capabilities required to execute and sustain Nova • Project risk assessment, prioritization and updated mitigations <p>Technology</p> <ul style="list-style-type: none"> • High-level technology improvement opportunities to enable value delivery • Prioritized set of insurance and non-insurance journeys, with key pain points mapped to current system constraints

B: Develop recommendations to enhance the Nova program

Questions to answer	Approach	Deliverables
<p>Strategy</p> <ul style="list-style-type: none"> What changes are required to ensure the desired outcomes are met? How will the outcomes be measured? What is the optimal roadmap to maximize value delivery? <p>Governance</p> <ul style="list-style-type: none"> What is the necessary structure, oversight and approach to effectively execute the transformation? What are the priority of capabilities to be developed? How can they be developed? <p>Technology</p> <ul style="list-style-type: none"> Which current customer pain points in priority journeys cannot be resolved using legacy technology? What technical capabilities should be accelerated, paused, or deprioritized based on associated business value? 	<p>Strategy and Governance</p> <ul style="list-style-type: none"> Develop comprehensive scope, prioritization, timeline and budget improvement recommendations and plan Create a high-level prioritized roadmap (including quick wins) and change management recommendations to maximize value and reduce risks Quantify the impacts and benefits of the revised roadmap for the business case Detail improvements to them delivery approach including general contractors Define the Control Tower structure/mandate for ongoing governance and tied to enterprise governance outside of Nova Define the approach (build/buy/partner) to address prioritized capability gaps <p>Technology</p> <ul style="list-style-type: none"> Detail enhancements to target architecture and technology foundations – tying to business value Create high-level roadmap to implement technology enhancements Prioritize specific capabilities to accelerate vs. deprioritize using journey-based view of importance 	<p>Strategy and Governance</p> <ul style="list-style-type: none"> Holistic program improvement recommendations and plan Refined roadmap and value realization plan including quantified impacts Revised delivery approach and op. model Control Tower structure, roles and mandate Detailed approach to address prioritized capability gaps Evaluate MPI's role of a General Contractor and provide recommendations on its suitability for Program Nova <p>Technology</p> <ul style="list-style-type: none"> Detailed technology improvement recommendations Refined technical roadmap

How we would partner together

	Responsibility	Stakeholders and time commitment
Steering committee	<p>Provide direction and review recommendations and findings</p> <p>Identify boundaries and constraints</p> <p>Stress-test results / ensure objective assessment</p> <p>Sponsor working team</p>	<p>1-1.5 hour review every 2 weeks</p> <p>Attended by executive sponsors</p>
Weekly core team working sessions	<p>Working sessions with a small group of leaders</p> <p>Coordinate key activities and facilitate overall process (e.g., data requests, finding key SMEs, etc.)</p> <p>Pressure-test initial findings and recommendations</p> <p>Act as primary thought partner to McKinsey team in developing recommendations</p>	<p>2-3 “core” individuals who will liaise with McKinsey team; 1-2 working sessions per week</p>
SME interviews & survey participants	<p>Provide input through 1:1 interviews</p> <p>Participate in working session as needed</p> <p>Answer VA360 and/or DQ assessments</p>	<p>Interviews: 60mins with ~10-20 leaders</p> <p>Survey: ~30-45 mins survey response, total of ~30-40 participants</p>

August 2, 2023

CONFIDENTIAL

MPI Exhibit #16
2024 GENERAL RATE APPLICATION
Part IX – EXP Appendix 23a - Redacted

June 15, 2023

CONFIDENTIAL

2024 GENERAL RATE APPLICATION
Part IX – EXP Appendix 23a - Confidential

Agenda

Proposed approach to diagnose the Nova program

Team structure and profiles

Why McKinsey?

Professional arrangements

Team composition and expert panel

Exact team composition will vary depending on effort start date

August 2, 2023

CONFIDENTIAL

MPI Exhibit #16
2024 GENERAL RATE APPLICATION
Part IX – EXP Appendix 23a - Redacted

June 15, 2023

CONFIDENTIAL

2024 GENERAL RATE APPLICATION
Part IX – EXP Appendix 23a - Confidential

Agenda

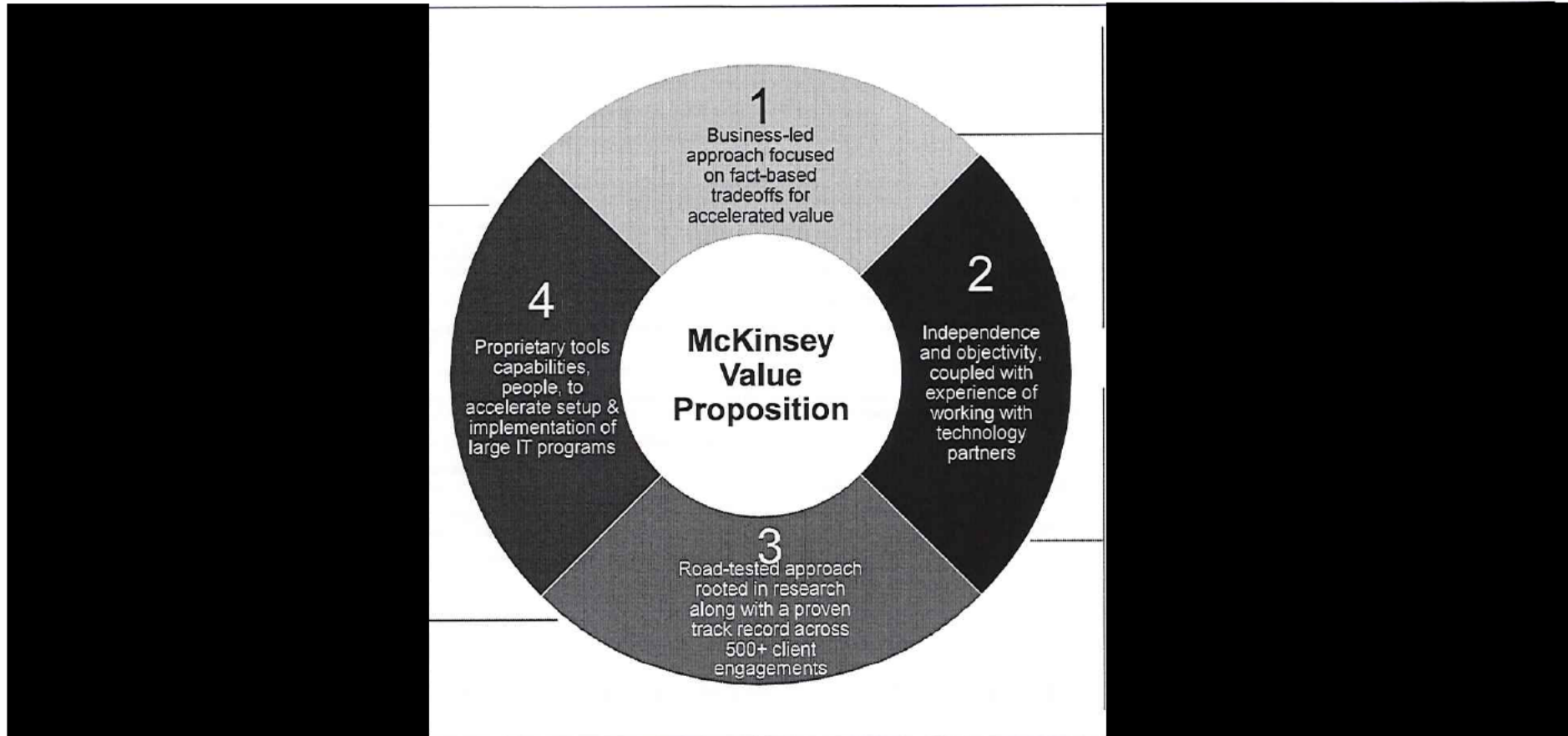
Proposed approach to diagnose the Nova program

Team structure and profiles

Why McKinsey?

Professional arrangements

McKinsey Value Proposition on Value Assurance



Examples of Value Assurance work with clients



Agenda

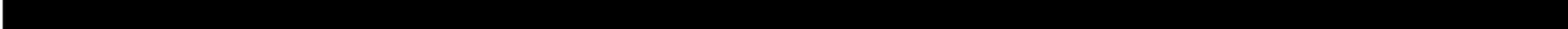
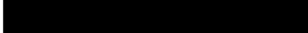
Proposed approach to diagnose the Nova program

Team structure and profiles

Why McKinsey?

Professional arrangements

Professional arrangements

- Our mission is to help our clients achieve distinctive, substantial and lasting improvements in their performance. We go beyond what is expected. We will provide with you the support you need to meet your priorities, including committing greater time and resources where necessary.
- For this effort, the team configuration will consist of the following:
 - Committed leadership by at least two McKinsey Partners/Senior Partners (part-time), who are accountable for delivery, actively manage the engagement, and lead problem solving with the team
 - A full-time team of one Engagement Manager and two Associates or Business Analysts, who lead the day- to-day work (e.g., interviews and data collection, analysis, problem solving, communications). The full-time team draws upon the following resources, capabilities, and expertise as much as needed to deliver superior results to the client
 - Subject matter experts (SMEs) and extended leadership (part-time), who bring world-class expertise and experience on relevant industry and functional topics
 - Proprietary knowledge and tools that help our clients solve problems more efficiently and effectively
 - Support for new solutions and advanced analytic techniques
 - A research team that is available around-the-clock to answer clients' questions about issues such as best practices or important trends
 - World-class graphics support
- 
 The total professional fees of the engagement will be \$2,233,125.
- Our fees are inclusive of all out-of-pocket expenses and support services such as research, report production, secretarial, IT, administrative and other experiences. Other fees do not include taxes.
- We will invoice our professional fees and taxes in arrears on a monthly basis, subject to the deliverables being complete to an acceptable standard and their acceptance being signed-off by MPI.

McKinsey Data Protection Protocols

McKinsey agrees and warrants that it has implemented technical and organizational measures appropriate to protect Confidential Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the information to be protected having regard to the state of the art and the cost of their implementation. These measures include, as appropriate and without limitation:

1. Implementing and complying with a written information security program consistent with established industry standards and including administrative, technical, and physical safeguards appropriate to the nature of the Confidential Information and designed to protect such information from: unauthorized access, destruction, use, modification, or disclosure; unauthorized access to or use that could result in substantial harm or inconvenience to the Client; and any anticipated threats or hazards to the security or integrity of such information;
2. Adopting and implementing reasonable policies and standards related to security;
3. Assigning responsibility for information security management and data protection and to provide to the Client contact details of responsible persons at McKinsey if requested;
4. Devoting adequate personnel resources to information security;
5. Carrying out verification checks on permanent staff that will have access to the Confidential Information;
6. Conducting appropriate background checks and requiring employees, vendors and others with access to the Confidential Information to enter into written confidentiality agreements;
7. Conducting training to make employees and others with access to the Confidential Information aware of information security risks and to enhance compliance with McKinsey's policies and standards related to data protection, as well as requiring such personnel to keep all such Confidential Information secure and confidential during their assignment and thereafter;
8. Sub-processing certain infrastructure and maintenance functions (e.g., hosting, backup, maintenance, administration, file sharing and storage, helpdesk) to third parties. With respect to such sub-processors:
 - a. The Client acknowledges that McKinsey shall be permitted to engage sub-processors for the processing of the Confidential Information subject to the controls and requirements set forth herein.
 - b. McKinsey will ensure that sub-processors are required to implement security controls no less stringent than those set forth herein, are subject to a legally recognized transfer mechanism, and are bound by written agreements reflecting the same.

offsite storage of data sufficient for disaster recovery, uninterrupted power supply, and disaster recovery and emergency programs;

- h. Measures to ensure that information collected for different purposes can be processed separately including, as appropriate and without limitation, adequate logical separation of Confidential Information (e.g., “internal client capability”/purpose limitation, separation of functions as production and test);
 - i. Notification to the Client within 30 days of any data subject request should a data subject directly contact McKinsey requesting any correction or deletion of her or his personal data;
 - j. Return or secure destruction of the Confidential Information as set forth in the Agreement.
10. Taking such other steps as may be appropriate under the circumstances.

Appendix 1 – MPI Remote Work Security Standard

Purpose

This standard describes Manitoba Public Insurance's (MPI) remote work security practices and standards which must be implemented and adhered to by Users who are required to work from remote locations (e.g. work from home).

Users in this standard refers to MPI employees, contracted individuals and companies, volunteers, students, board members, information managers and others working for or with MPI.

Scope and Applicability

This standard covers the security requirements for the access, use, configuration and maintenance of MPI information, systems and environments to reduce the likelihood of cyber security and privacy events occurring.

This standard applies to MPI employees, contracted individuals and companies, volunteers, students, board members, information managers and others working for or with MPI.

Standard

This section sets out the standard for remote work that must be adhered to by the Users:

1. Workstation Configurations:

All workstations (desktops, laptops, tablets and mobile devices) must have:

- Encrypted hard drives / storage media;
- Up to date patches to ensure that the workstations are kept current with all required operating system and application security patches;
- The ability to prevent unapproved software from being installed;
- Up to date antivirus software including the associated signature files, with real-time scanning enabled and a minimum of a weekly full scan;
- Firewalls installed and configured to protect the workstations from unauthorized access;
- Data loss prevention (DLP) capabilities;
- Web traffic directed through a web filtering technology to help prevent accidental access to malicious sites;
- A process to securely dispose of any hard drive or removable media storage device.

2. Access Control:

Access control mechanisms will be in place as follows:

- Multifactor authentication must be enabled for all types of remote access;
- User authentication credentials will be promptly deactivated where such credentials have not been used for a maximum period of 3 months, or within 2 days if the user has changed roles and no longer requires such access;
- User authentication credentials will be immediately (within 24 hours) revoked for all remote access capabilities (e.g.: VPN accounts, remote access tokens) in the event of an employee termination or end of supplier engagement;
- Where applicable, access controls will be provided using the least privilege access principles;
- Authentication credentials must not be shared with other individuals.

3. Connectivity:

- Users will only use workstations that are provisioned and managed by their organization;
- Users will only connect to secure Wi-Fi networks using strong encryption such as WPA2 or higher. If secure Wi-Fi is not available, a wired connection will be used instead;
- Users can only connect to MPI systems or environments from Public Wi-Fi networks if using an MPI approved Virtual Private Network (VPN) technology;
- Users using home Wi-Fi must change the default router or internet gateway passwords. Such passwords must be long and complex.

4. Physical Controls:

Users are:

- Responsible to ensure that physical working space is appropriately cordoned off to limit the exposure of Confidential Information to other individuals. This includes precautions related to preventing verbal communications from being overheard by other individuals;
- Responsible for protecting the workstations and software against unauthorized use and access;
- Authorized to print Confidential Information to local printers at remote locations, provided that printed materials are securely destroyed prior to disposal or recycling.

5. Collaboration Requirements:

Users must use MPI approved collaboration, storage and application platforms for conducting virtual meetings and sharing of documents.

6. Definitions

Definitions used in this standard:	<u>Definition / Description</u>
Access control	Means to ensure that access to assets is authorized and restricted based on business and security requirements.
Authenti-cation	Authentication refers to the verification of the authenticity of either a person or system. Authentication techniques usually form the basis for all forms of access control to systems and/or data.
Controls	The safeguards or countermeasures to avoid, counteract or minimize information security risks. May include people, process and/or technology.
Information asset	An information asset is a body of information, defined and managed as a single entity so it can be understood, shared, protected and exploited effectively. Information assets have value, risk, content and life cycles. Information assets also include devices such as computer devices and network or other electronic information systems which transfer or store information.
Intellectual property, intellectual capital	Intangible and commercially valuable property which is the product of the human intellect. At MPI, intellectual property is considered to be a type of information asset and includes, but is not limited to, designs, processes, methods, interfaces, networks and computer systems developed in-house or in association with business partners for the purposes of performing or representing MPI business.