

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

CONSULTING AGREEMENT**Between:****McKinsey & Company Canada****("McKinsey")**

and

The Manitoba Public Insurance Corporation**("MPI")**

For good and valuable consideration the receipt and sufficiency of which is acknowledged, the parties agree to the following terms and conditions in connection with consulting services that McKinsey will provide to MPI.

1. **BACKGROUND AND PURPOSE.** MPI engaged McKinsey in October 2021 to perform a diagnostic analysis of MPI's Project NOVA and prepare recommendations to de-risk the project. McKinsey performed the analysis and prepared recommendations, which it delivered to MPI in January 2022. Based on the recommendations, MPI requested McKinsey provide a proposal for McKinsey to support MPI implementing the recommendations. McKinsey provided this proposal to MPI in February 2022. The Proposal breaks down the work into two six month phases, and a summary based on the Diagnostic Recommendations, the Proposal and Key Outcomes for phases 1 & 2 is attached as Schedule A.

2. **TERM OF AGREEMENT AND RENEWALS.** This Agreement comes into effect as of March 7, 2022, and shall continue for six (6) months until and including September 6, 2022 (the "Initial Term" / Phase 1), unless otherwise terminated, suspended or extended in accordance with the terms and conditions of this Agreement. MPI may, at its sole option, not later than thirty (30) days prior to the expiration of the Initial Term of Agreement, renew the Agreement for an additional six (6) month term, until and including March 6, 2023 (the "Renewal Term" / Phase 2), on the same terms and conditions as were in force during the Initial Term.

3. **SERVICES.** The working arrangements, including scope of the services, are set out in detail, attached as Schedule B – Scope of Work, which sets out the specific outcomes, Deliverables, and Milestones, more generally described in McKinsey's proposal dated February 2022, attached as Schedule C – Proposal. The services shall include the work required to complete everything set out in the Scope of Work, and the parties may meet at mutually agreed times to discuss the progress of the services and to exchange feedback (the "Services").

4. **WORKPLAN.** The first task set out in the Scope of Work is for McKinsey to develop an initial workplan to be approved by MPI, (the "Workplan"). After the approval of the initial Workplan, it will become a working document subject to constant change and updating by McKinsey and approval by MPI throughout the term of this engagement.

5. **MPI RESPONSIBILITIES.** 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 MPI's timely cooperation, including MPI making available relevant data, information and personnel, performing any tasks or responsibilities assigned to MPI and notifying McKinsey of any issues or concerns MPI 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 material adjustments, to the Scope of Work, Deliverables, Deliverable Requirements, Key Performance Indicators, Acceptance Criteria, timeframe and budget and sign off on them by way of a mutually acceptable change order.

6. **SERVICE DELIVERY.** The delivery of the Services covered by this Agreement will be led by a joint McKinsey and MPI core team in accordance with team support model set out in the Scope of Work, and structure set out on page 5 of the Proposal. At each scheduled meeting MPI's core team will provide information, advice and feedback to McKinsey's core team related to their progress.

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

7. DELIVERABLES. The Deliverables to be produced by McKinsey for MPI under this Agreement, and the responsibilities of each Party for each Deliverable are set out in Schedule B, attached hereto and incorporated herein as if set forth in full. Deliverable Requirements have been established for each Deliverable (defined as the requirements listed for each Deliverable set out in Table 1 of the Scope of Work). Any Interim Deliverables dates required will be established during the development of the Workplan. Deliverables will be provided as and when available throughout the engagement in accordance with the Milestones target dates set out in the Schedule B – Scope of Work (Table 1).

8. ACCEPTANCE OF DELIVERABLES. The Parties agree to the acceptance procedures for Deliverables set out below. The acceptance procedures include an assessment of whether the Deliverable meets the Deliverable Requirements, 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 Deliverable Requirements and Key Performance Indicators (defined as the list in the Key Outcomes column in Schedule A).

The Acceptance Criteria are that each Deliverable:

1. Provides a full and complete solution in accordance with Deliverable Requirements articulated in Schedule B – Scope of Work Table 1.
2. Meets the standard that it achieves the Key Performance Indicators, to assure the execution and delivery of the Project NOVA transformation initiative.

The acceptance procedures are as follows:

1. If MPI determines that a Deliverable meets the Acceptance Criteria, in all material respects, MPI shall notify McKinsey in writing of MPI's acceptance of the Deliverable, within a 5-day period.
2. If MPI determines that a Deliverable does not meet the Acceptance Criteria, in all material respects, MPI shall notify McKinsey in writing of MPI's rejection of the Deliverable within a 5-day period, and describe in reasonable detail in such notice MPI's basis for rejection of the Deliverable.
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, the Acceptance Criteria, and notify MPI in writing that it has completed such modifications or improvements and re-submit the Deliverable to MPI.
4. MPI shall then review the modified or improved Deliverable within 5-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, MPI 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, notwithstanding any other remedies MPI may have for McKinsey's default in law or equity.

9. DECISION ESCALATION AND ISSUE MANAGEMENT FRAMEWORK. If there are any material disagreements that cannot be resolved by the core teams, these will be escalated. Appropriate, decisions and Workplan issues that cannot be resolved within the allocated timeframe will be escalated to leadership for resolution as per the escalation table below. Any decision or issue that remains unresolved to the satisfaction of both Parties beyond the thresholds (number of days from identification of issue) below shall be escalated to the next resource level in writing. Escalation communications must include current status as well as the actions and timelines taken to resolve and the timelines.

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

Resource Level	Threshold to Resolve
McKinsey Program Delivery Lead / MPI Senior Leader	1 Business Day
McKinsey Delivery Executive Lead / MPI Program Director	3 Business Days
McKinsey Senior Leadership / MPI CEO	5 Business Days

10. **TEAM COMPOSITION.** McKinsey shall not substitute other personnel for those designated without the prior written consent of MPI. 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 MPI.

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 MPI (which cannot be unreasonably withheld) and on terms and conditions satisfactory to MPI 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.

To clarify the Proposal and the Scope of Work the following individuals are considered McKinsey's Designated Personnel to provide the Services:

McKinsey Designated Personnel, and Role	
	Senior Partner
	Partner, Director of Consulting Services
	Partner, Engagement Director
	Expert, Core Tech advisor / content leader
	Value Assurance
	Design / CX
	Enterprise Architecture
	Product Management
	Insurance (Digital and Analytics)
	Day to day program manager
	Execution owner for a specific workstream with skills aligned to the workstream assigned
	Execution owner for a specific workstream with skills aligned to the workstream assigned

11. **COMPENSATION.** The MPI shall compensate McKinsey for its professional fees and expenses in connection with the Services, as set forth below.

MPI 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 MPI's external procurement and other service providers).

McKinsey will perform its Services on a fixed fee basis plus applicable taxes (MPI's GST exemption Certificate is attached as Schedule D). Based on the terms set forth in this Agreement, McKinsey's maximum fees for its Services during the Initial Term (Phase 1) will be \$4,982,250.00 (CAD) and includes all costs associated with service fees and travel related expenses.

If MPI renews the Agreement for the additional six (6) month Renewal Term, McKinsey's maximum fees for its Services during the Renewal Term (Phase 2) will be \$4,982,250.00 on the same terms and conditions as were in force during the Initial Term; however, a new Schedule B – Scope of Work and Milestones for the attached Schedule B Table - Deliverables shall be created and agreed to in writing with upon renewal, along with a revised table for Section 12 Payment table.

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.

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

12. **PAYMENT.** McKinsey will invoice MPI for professional fees and expenses in connection with the Services in accordance with the Milestones and Deliverables in the Schedule B – Scope of Work.

The table set out below is based on the Deliverables set out in the Schedule B – Scope of Work, which sets out the Deliverables, Acceptance Criteria and Milestones developed and agreed to by the parties. The process for payment is as follows:

- A. MPI will review all Deliverables provided by the Milestone Target Date and pay the monthly fees.
- B. If any one or more Deliverables detailed in each of the Milestone payments detailed below is not accepted by MPI by the Milestone Target Date, MPI will retain 25% of the monthly Milestone payment as fees at risk and provide McKinsey with a written explanation of why such services have not met the Acceptance Criteria.
- C. The only basis for rejection of Deliverables will be the failure of the Deliverables to materially comply with the Acceptance Criteria.
- D. To the extent McKinsey has cured any issues and completed the Deliverable in accordance with the Acceptance Criteria associated with the applicable Milestone Target Date, MPI will accept the Deliverable and pay out the fees at risk on the Milestone payment at the end of the month.

Month	Milestone Target Date	Milestones and Deliverables by Workstream				Fees as Risk	Price
1	March 31, 2022	Workplan & A1		C1		25%	
2	April 30, 2022	A2 & A3	B1 & B2	C2		25%	
3	May 31, 2022	A4 & A5	B3	C3		25%	
4	June 30, 2022		B4	C4	D1	25%	
5	July 31, 2022	A6	B5 & B6	C5	D2	25%	
6	August 31, 2022	A7	B7 & B8	C6	D3	25%	
						Sub Total	\$4,982,250.00
						(MPI is GST exempt & the Services are PST Exempt) Total	\$4,982,250.00

13. **CONFIDENTIALITY.** McKinsey will keep confidential any confidential information, including any personal data (as defined below), furnished by MPI 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 MPI, 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", attached as Schedule E).

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 MPI. To bring the best of McKinsey's global resources to serve MPI, MPI 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 MPI, 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

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

disclosed. McKinsey will reasonably cooperate with MPI, 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 MPI 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 MPI'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 MPI. 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.

14. DATA SECURITY. Without limiting the foregoing, if McKinsey processes data as part of the Services and on behalf of MPI 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 MPI, 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 MPI of any incident in which the confidentiality, integrity or security of the personal data has been compromised, and (iv) collaborate with MPI as required by applicable law or MPI'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 MPI 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> (the Standard Contractual Clauses, attached as Schedule F) 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 MPI's reasonable requests to furnish information regarding McKinsey's processing activities as is reasonably necessary to enable MPI 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 MPI 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.

MPI 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 MPI 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 MPI'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, MPI will take all requisite or recommended precautions for the safety of the personnel at MPI's premises and, prior to and as a condition to any such attendance

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

on premises, the Parties will, acting reasonably, agree to mutual covenants designed to safeguard the health and safety of the personnel of both MPI and McKinsey.

15. INTELLECTUAL PROPERTY. Upon payment in full of McKinsey's fees, MPI will own all reports and other deliverables prepared for and furnished to MPI 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 MPI's Confidential Information.

To the extent the Deliverables include any embedded McKinsey Tools, McKinsey hereby grants MPI 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. MPI 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.

16. DISCLOSURE OF MCKINSEY MATERIALS; PUBLICITY. McKinsey's work for MPI is confidential and for MPI's internal use only. McKinsey will not disclose the Deliverables to any third parties without MPI's prior written permission. Similarly, MPI agrees that it will not disclose any materials or information that McKinsey furnishes to MPI, 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 MPI may be required to provide Deliverables to the Manitoba Public Utilities Board (PUB), provided that MPI 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.

17. 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 MPI about McKinsey's serving the MPI's competitors or other parties. Nothing in this section shall operate to limit or reduce McKinsey's obligations with respect to MPI's Confidential Information, including the confidentiality and non-disclosure obligations with respect thereto.

18. LIMITATION OF LIABILITY. The Services shall not be deemed investment, legal, tax, accounting or other regulated advice. MPI remains solely responsible for its decisions, actions, use of the Deliverables and compliance with applicable laws, rules and regulations. MPI 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 MPI in connection with the Services relating to an engagement for MPI exceed the fees received by McKinsey from MPI in connection with such engagement. Neither party will be liable for any lost profits or other indirect, consequential, incidental, punitive or special damages.

19. 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

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

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.

20. TERMINATION. The Services will commence and shall continue until all Deliverables have either been accepted by MPI, or terminated in accordance with the terms of this agreement. MPI may terminate the Services at any time effective upon written notice to McKinsey and, in the event of such termination, MPI will pay McKinsey's fees and expenses up to the effective date of termination.

21. INTERPRETATION AND ENTIRE AGREEMENT. This Agreement and the attached schedules 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. Any conflicts and inconsistencies between this agreement and the various schedules will be resolved in accordance with the following order of precedence: 1) this Agreement, 2) Schedule A – Key Outcomes 3) Schedule B – Scope of Work, 4) Appendix 1 – MPI Remote Work Security Standard, 5) Schedule C – Proposal, 6) Schedule D – Protocols, 7) Schedule E – Standard Contractual Clauses, 8) Schedule F – GST Exemption Certificate.

22. MISCELLANEOUS. MPI 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 MPI and McKinsey. The following Sections shall survive the completion or any termination of the Services: 13 (Confidentiality), 14 (Data Security), 15 (Intellectual Property), 16 (Disclosure of McKinsey Materials; Publicity), 17 (Serving Competitors), 18 (Limitation of Liability), 20 (Termination) and 22 (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 MPI's agent or fiduciary. Notwithstanding any course of dealings of

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

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.

23. **SIGNATURES.** 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 on the dates noted below.

The Manitoba Public Insurance Corporation

McKinsey & Company Canada

Eric Herbelin Digitally signed by Eric Herbelin
Date: 2022.03.08 15:38:10
-06'00'



Name: Eric Herbelin
Title: President and CEO
Date: March 8, 2022

Name: Erez Eizenman
Title: Senior Partner
Date: March 8, 2022

The Manitoba Public Insurance Corporation

Shayon Mitra Digitally signed by Shayon Mitra
Date: 2022.03.08 13:38:47
-06'00'

Name: Shayon Mitra
Title: VP and Chief Transformation Officer
Date: March 8, 2022

August 2, 2023

CONFIDENTIAL

June 15,2023

CONFIDENTIAL

Schedule A - Key Outcomes

Diagnostic Recommendation	Label and Description	Activities	Key outcomes
i. Strategy and Roadmap	A. Launch online/"self-service" MVPs for Consumer Insurance and DVA starting Q1 2023, and validate the Claims technology using a "proof of concept" in Q1 2023		Phase 2 (1) upcoming release milestones de-risked - Nova leaders aligned and are prepared to act on recommendations around MVPs/POC; MVP candidate list identified for R3/4 with alignment on "go, no-go" on MVP implementation based on being able to address all prerequisites and receiving approval on a documented decision capturing risk, impact and benefits (2) "Go, no-go" decision made for Claims POC based on being able to address all prerequisites and receiving approval on a documented decision capturing risk, impact and benefits
i. Strategy and Roadmap	B. Pilot defining and measuring business and customer centric OKRs with Release 1 to show immediate impact of releases, and stand-up OKR tracking through VA control tower		Phase 1 (1) MPI outcome-oriented governance model (incl. PMO roles, forums) designed, approved and fully mobilized. (2) Outcomes Identified and OKRs confirmed. (3) Critical operational readiness elements identified and MPI owner assigned. (4) Critical operational readiness elements in place for Release 1 success
			Phase 2 (1) Critical OKRs measured & impact published for Release 1
ii. Operating Model and Governance	C. Starting with Release 3, structure teams around customer / employee journeys and shared platforms		Phase 1 (1) Implement shifts in delivery mechanism aligned with MPI Leadership with tangible recommendations to improve coordination among teams

Schedule A - Key Outcomes

ii. Operating Model and Governance	D.	Clarify role and accountability of Business, CX, and Tech leaders; appoint persistent leads with required coaching and governance		Phase 1	(1) Roles and accountability of Business, CX, and Tech leaders formalized, and coaching and governance in place before September 1
				Phase 2	(1) Business and CX leadership discovery completed and "future state" design is in place based on best practices
ii. Operating Model and Governance	E.	Embed CX/Design & product management people and practices in the current Agile ways of working, and build their capability through "Product management coaching"		Phase 1	(1) Accountabilities & organization model adapted for new execution roles (2) CX/Design & product management is embedded in the current Agile ways of working, through capability building and "Product management coaching".
iii. Change Management	F.	Execute end to end operational readiness plan for Release 1 immediately, led by Business and Operational Readiness team		Phase 1	(1) Critical operational readiness elements in place for Release 1 success
				Phase 2	(1) Critical OKRs measured & impact published for Release 1
iii. Change Management	G.	Ensure there is a responsible and accountable MPI owner for each of the Culture and Change Management work-streams		Phase 1	(1) MPI owners and accountabilities in place for change management for Release 1 success
iv. Technology	H.	Develop a plan to address the capability gaps and needs of the Nova program and create an integrated view of tasks Nova depends on		Phase 1	(1) Leadership alignment on Integrated Execution Plan steps to address the identified capability gaps. (2) Coaching plan in place for IT, CX and business roles with the ability to measure improved maturity in these roles. (3) Approved MPI Integrated Execution Plan for NOVA and its IT and non-IT enablers (4) Establish go forward guardrails and best practices for capability development and management for MPI in next phase of effort

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

Schedule A - Key Outcomes

Overarching	I.	Set-up a Value Assurance "control tower" to enhance MPI's general contractor capability for Nova, including responsibility for decisions that maximize value for MPI and acting as a clearing house for addressing impediments, risks, and dependencies.	[REDACTED]	Phase 1	(1) Approved MPI Integrated Execution Plan defined for NOVA and its IT and non-IT enablers (2) Nova Control Tower stood up (3) Approved governance, scope, roles and responsibilities and interaction models (4) Initial knowledge transfer of Control Tower skills to Nova Team
				Phase 2	(1) MPI Value Assurance Leadership Model established (e.g. leadership and product coaching) (2) Tools and work-arounds defined, where needed

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

SCHEDULE B – SCOPE OF WORK

Background and description of services:

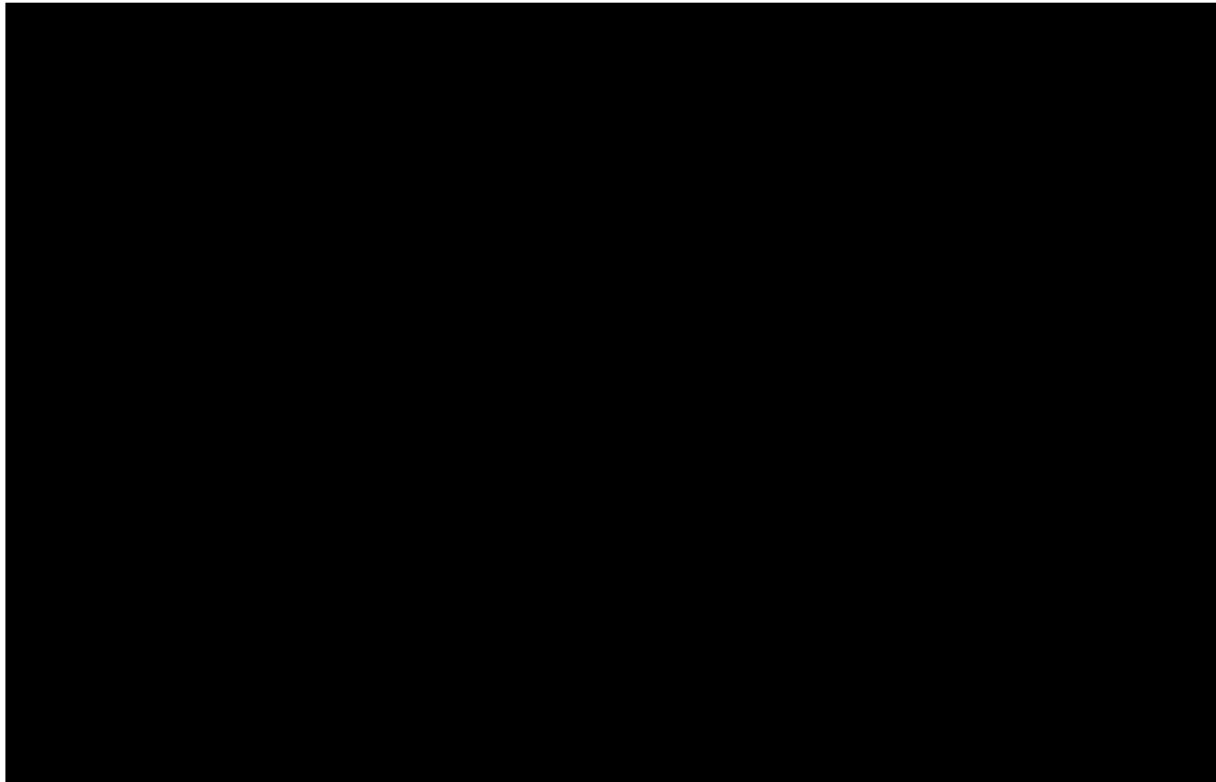
In the fall of 2021, MPI conducted an internal re-baseline of the project based on the review by its internal governance PWC. Following this McKinsey was retained to perform an assessment and develop actionable recommendations to address issues identified by PWC, MPI. The diagnostic established several steps to ensure Nova and other related initiatives will be ready to execute as per plan.

This outcome and deliverables for this Scope of Work are for McKinsey to identify program and enterprise level requirements to set MPI and the Nova program up for success. MPI is looking to ensure these recommendations get implemented using industry tested best practices.

MPI requires McKinsey's guidance to:

- strengthen its core execution capabilities;
- de-risk upcoming release milestones;
- leverage lessons learned in the diagnostic; and
- obtain targeted problem solving and coaching support for Nova leaders.

During the Initial Term, MPI will be looking for support from McKinsey to stand up core foundational capabilities across Nova and beyond, which would include addressing the “**enterprise level requirements**”, including:



In the process of operationalizing these capabilities, **McKinsey will also help MPI stand up its own Value Assurance Control Tower** that can start shadowing the McKinsey team in the immediate term and **start taking over the “enterprise level requirements” by the second half of 2022.**

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

At the end of the first 6 months of this partnership, McKinsey and MPI will jointly evaluate any continued need for McKinsey support – especially towards ensuring **Nova's upcoming releases. are "ready"** to deliver impact as per their target plan. This may include ensuring that Release 1 is delivering on its critical operational readiness elements (ahead of its Q3 2022 release), and preparing Release 3 (and optionally, Release 4) for a full-fledged Business and CX led discovery in Q4 2022 (including identifying potential MVPs to solve for, and conducting a Claims POC if needed) .

Timeline and Deliverables

MPI has committed to a 6-month deployment of Phase 1 activities that will build/address the foundational capabilities for Project Nova that can be applied to future initiatives. **McKinsey team leads are responsible to set up the enterprise requirements and ensure the core enablers for Release 1 is on-track**, while MPI initiative leaders will engage as SME, including an MPI-sponsored Value Assurance lead throughout the program.

The timeline for the effort will run over **6 months starting in March 2022 and concluding in August 2022**. At the end of August 2022, MPI and McKinsey will discuss a "go, no-go" decision point on an option to continue support for 6 additional months based on program status and evolving priorities. At that time, a new staffing plan, priorities, deliverables and outcomes would be discussed based on the current state and needs.

To support the achievement of the priorities of the first 6 months, McKinsey will execute on the following deliverables, across 4 key workstreams:

- A. Integrated Enterprise Execution Plan for MPI**
- B. Value Assurance Control Tower (Outcome-oriented governance model)**
- C. Accountabilities & org. model for new execution roles**
- D. Shifts in delivery mechanism**

In parallel to the above, McKinsey will also provide leadership coaching to MPI senior leaders on their respective priorities as needed (e.g., IT strategy/end state operations, standing up CX capabilities, operational readiness in SRE, etc.), through targeted topical expert backed working sessions and problem-solving discussions.

Milestones, Deliverables and Deliverable Requirements

The milestone target dates are set monthly, to measure progress in each applicable workstream by assessing the Deliverables (set out in Deliverables column in Table 1). The parties have established requirements for each Deliverable (set out in the Deliverables Requirements column in Table 1) for the purpose of the assessment.

Key Performance Indicators and Acceptance Criteria

McKinsey and MPI have agreed that that in addition to completing the Deliverable Requirements in Table 1, the Schedule A – Key Outcomes table summarizes how the initial recommendations were structured and how these have evolved from the Proposal into key outcomes or key performance indicators, which will be used to assess the Deliverables.

Therefore the Approval Criteria for each milestones in this Scope of Work, will be based both on the Deliverable Requirements in Table 1 and on the Key Performance Indicators in the Key Outcomes column of Schedule A.

In the event that MPI determines that Acceptance Criteria (as set out in Section 7 – Acceptance of Deliverables of the Agreement) have not been met, MPI shall provide McKinsey with a written explanation of why such Services have not met the Acceptance Criteria.

August 2, 2023

CONFIDENTIAL

June 15,2023

CONFIDENTIAL

Workplan

MPI is requesting McKinsey develop an initial Workplan to complete the work and a template to track progress. After the approval of the initial Workplan, it will become a working document subject to constant change and updating by McKinsey and approval by MPI throughout the term of the engagement.

Team Support Model

McKinsey will support the effort with a dedicated team of experts and consultants. McKinsey will support the effort with a dedicated team of experts and consultants. There are 4 functional groups within the team model:

1. **Client Service Leadership Team** [Redacted]
2. **Core fully dedicated Team** [Redacted]
3. **Subject Matter Experts** [Redacted]
4. **Research Support Services** [Redacted]

The following is a table describing the team members and their commitments of time and effort to the program, the listing of designated resources is set out in the Agreement.

Name	Position, Role	Time Commitment as FTE%
	Senior Partner, Project Sponsor	
	Partner, Director of Consulting Services provided	
	Partner, Engagement Director more hands on with day-to-day delivery	
	Expert, Core Tech advisor/content leader	
	Day to day program manager	
	Execution owner for a specific workstream, with skilled aligned to the workstream assigned	
	Execution owner for a specific workstream, with skilled aligned to the workstream assigned	

August 2, 2023

CONFIDENTIAL

June 15,2023

CONFIDENTIAL

Name	Position, Role	Time Commitment as FTE%
Experts, engaged based on topical requirements – to participate in McKinsey’s internal or MPI facing problem solving sessions and workshops		

The following table is a list MPI’s key resources involved in the engagement and their estimated level of effort

Name	Position, Role	Estimated % effort to be confirmed in the Workplan
Eric Herbelin	President & CEO	As needed
Shayon Mitra	VP & Chief Transformation Officer	As needed
Siddhartha Parti	VP & Chief Information Office	As needed
Satvir Jatana	VP & Chief Customer Officer	As needed
Alex Ramirez	Director Nova Program Delivery	10-20%
Stephen Ramchandar	Director Strategy & Portfolio Management	10- 20%
Shawn Campbell	Director Enterprise Architecture	10-20%
Darryl Beckett	Manager, Nova Program Delivery	10-20%
Tamara Boblinski	Director Change & Knowledge Management	10-20%
Bradley Moore	Director Customer Experience	10-20%
	MPI has a variety of individuals at the program Manager level	Varies by role. To be confirmed in the Workplan

The parties agree that the above are estimates only, the actual time per month or week may vary, but should on average conform to these estimates.

The parties agree that the following Table 1 outlines the Deliverables and Deliverable Requirements agreed to by the parties for the Initial Term.

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

Schedule B – Scope of Work Table 1: Deliverables and Deliverable Requirements

MONTH (*) MPI MILESTONE	DELIVERABLES	DELIVERABLE REQUIREMENTS
MONTH 1	<p>Workplan</p> <p>A1. Approval of an Enterprise Execution Plan (the “Plan”)</p> <p>C1. Document common role taxonomy created (especially for PM, PO, and other new Business/CX roles)</p>	<ul style="list-style-type: none"> • Define and prepare the deliverable schedule and mechanism to track progress, to be approved by MPI • Approach to working together agreed to be approved by MPI. <p>Deliverable Requirements for Approval of A1:</p> <ul style="list-style-type: none"> • Create an inventory of various Nova and non-Nova initiatives in-flight across MPI, by leverage existing work. • The Plan must include a summary of all NOVA and non-NOVA initiatives inventoried and prioritized by tier to minimize non-critical work. • Conduct sessions with initiative owners to pressure test relevancy of scope/timing of work and connected dependencies. • Identify potential to optimize any effort non-critical to Nova/MPI for the time being • Stress-test the linkages with relevant initiative owners and consumers to ensure the dependencies are understood at a high level, and initiate clarification of understanding by corporate stakeholders. • Define a relational view of all initiatives prioritized – showing upstream and downstream linkages • The plan should include guidance on the necessary adjustments to MPI’s current plan to ensure Project NOVA success • Integrated execution plan refined with feedback from individual owners/stakeholders • Areas of uncertainty understood, and execution plan adjusted with necessary buffers • Finalize an integrated organization execution plan, for approval by MPI senior leadership. <p>Deliverable Requirements for Approval of C1:</p> <ul style="list-style-type: none"> • Prepare draft of common role taxonomy document, for feedback and by MPI which includes the following • Define baseline for Business & CX roles (what roles exist, the nomenclature and accountabilities) • Refine the target state role taxonomy for Business/CX

August 2, 2023

CONFIDENTIAL

June 15,2023

CONFIDENTIAL

<p>MONTH 2 * BOARD MEETING TO SHARE THE INTEGRATED EXECUTION PLAN</p>	<p>A2: Integrated execution plan shared with the board; refinements incorporated based on feedback</p> <p>A3. Stakeholder Alignment Plan</p> <p>B1. PMO bodies across MPI baselined (incl. existing roles, cadences, scope of control)</p> <p>B2. Enhanced governance blueprint drafted, with role of Value Assurance Control Tower and other PMO bodies clarified</p> <p>C2. Existing resources and skills baselined against the new taxonomy and gaps identified</p>	<p>Deliverable Requirements for Approval of A2:</p> <ul style="list-style-type: none"> • Plan shared with the board and feedback collected • Plan refined based on input from board, for board approval <p>Deliverable Requirements for Approval of A3:</p> <ul style="list-style-type: none"> • Develop strategies to engage stakeholders and help align each MPI Division. • The draft strategies and plans should be based on interviews with NOVA stakeholders and stakeholders from each Division and common understanding. • Document stakeholder alignment achieved with each group of stakeholders. <p>Deliverable Requirements for Approval of B1:</p> <ul style="list-style-type: none"> • Document baseline Nova PMO functions (incl. roles, cadences, control points) • Draft baseline A-PMO functions (incl. roles, cadences, control points) • Document baseline IT strategy related PMO and governance functions (incl. roles, cadences, control points) • Synthesize and document key requirements across all that the governance blueprint needs to solve for <p>Deliverable Requirements for Approval of B2:</p> <ul style="list-style-type: none"> • The following should be included and documented in the enhanced governance blueprint. • Define the ideal state “common” governance blueprint based on best-in-class practices • Define mandate/structure for the VA Control Tower & other PMO bodies, based on the new blueprint • Clarify, and define PMO roles & accountabilities across MPI, and how they will interact with each other <p>Deliverable Requirements for Approval of C2:</p> <ul style="list-style-type: none"> • Create a documented inventory of existing resources/skills across the new business and CX roles • Work with MPI leaders to frame hypothesis on areas to keep as-is, upskill, fill through internal transition, fill through external hiring
--	--	--

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

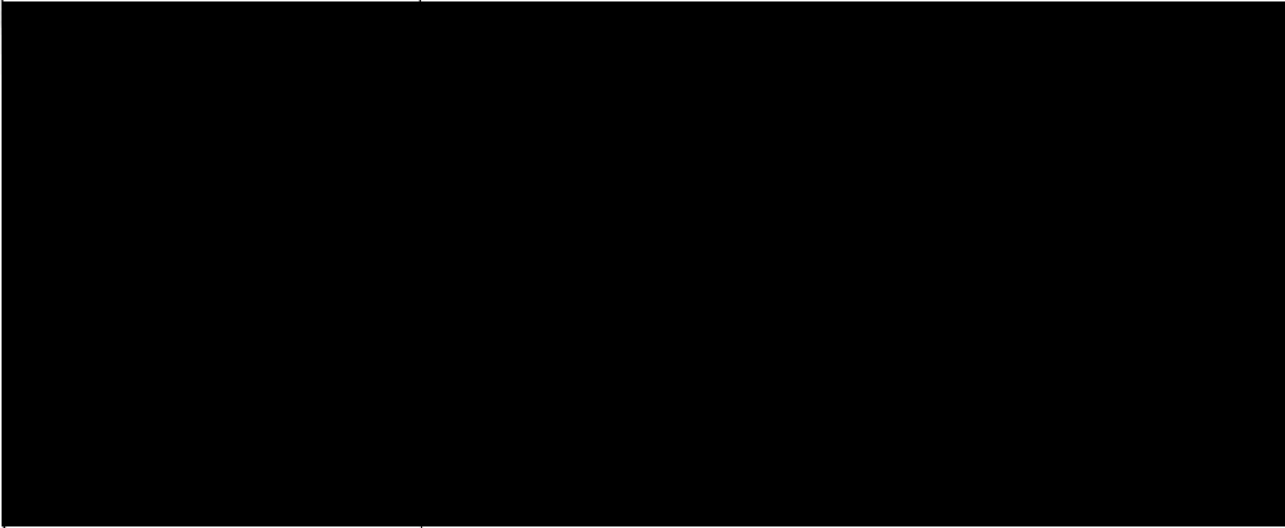
<p>MONTH 3 * MVP FOR RELEASE 1 READY (BUT NOT IN PRODUCTION)</p>	<p>A4. Risks to Nova roadmap identified (especially for Release 1) & mitigation options outlined</p> <p>A5. Identify gaps in corporate roadmap to align with Nova's roadmap including risk identified from A4</p> <p>B3. Plan an approach to align MPI's multiple PMOs and piloting the new governance model blueprint to test and refine</p> <p>C3. Revise and document Organizational model based on C2</p>	<p>Deliverable Requirements for Approval of A4</p> <ul style="list-style-type: none"> Assess sensitivity of how various enablers may impact Nova's timeline/scope – especially for Release 1 (based on MVP progress and readiness of key enablers) Create options for how to mitigate impact, where required Meet with steering committee to provide risk advice and guidance to mitigate Align with steering committee on implications <p>Deliverable Requirements for Approval of A5</p> <ul style="list-style-type: none"> Revise Enterprise Execution Plan based on identified shifts needed in other MPI priorities needed to support Nova's timeline, based on timing of and level of confidence in the enablers Align on the revised requirements with each dependent group (in joint working sessions, to ensure full transparency and coordination) Create and document a watch-list of milestones, along with decisions needed at these points (if any) <p>Deliverable Requirements for Approval of B3</p> <ul style="list-style-type: none"> Initiate lean portfolio management project to assist non-NOVA PMOs to support NOVA PMO Define the tools, processes and control points required to operationalize the pilot Outline the plan for mobilizing the new model Syndicate the plan for pilot with the key stakeholders/participants <p>Deliverable Requirements for Approval of C3</p> <ul style="list-style-type: none"> Define new roles, and clarifying reporting lines based on C2 Align on future state business roles to be split across various MPI functions (based on the resource mapping) <p>Define the org structure (through potential options and decision consideration) for these new roles based on C2</p>
---	---	---

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

MONTH 4	B4. Pilot minimum viable product (MVP) version of integrated governance, Value Assurance Control Tower for Nova launched & changes in other PMO bodies rolled out for testing	Deliverable Requirements for Approval of B4 <ul style="list-style-type: none">• Launch the Value Assurance Control Tower for Nova, with leadership level cadences piloted• Implement the changes in other PMO functions• Gather initial feedback and gaps from stakeholders/participants• Refine the blueprint based on inputs• Implement (or prepare to implement) the changes in the next iteration of cadences
		

August 2, 2023

CONFIDENTIAL

June 15,2023

CONFIDENTIAL

MONTH 5	A6. Assess and document MPI's performance on the integrated execution plan created based on cadence initiated, and develop tracking and measurement templates	Deliverable Requirements for Approval of A6 <ul style="list-style-type: none"> • Document and report how Nova and related enablers are performing vs. the integrated execution plan • Draft subsequent decisions/mitigations needed, and clarify (incl. who should own what part of these decisions)
	B6. Risk mitigation process initialized via Value Assurance Control Tower, to address and prioritize top 4-5 program risks already identified.	Deliverable Requirements for Approval of B6 <ul style="list-style-type: none"> • Run quick diagnostic and fact collection to identify open impediments and program risks • Prioritize and address top 4-5 program risks already identified that need enterprise level intervention and start drafting the solution on these • Identify and report any improvements needed in the path for identifying and escalating such risks, • Provide guidance and recommendations, and document the changes needed in accountabilities/processes to drive more proactive risk identification and resolution

August 2, 2023

CONFIDENTIAL

June 15,2023

CONFIDENTIAL

MONTH 6	<p>A7. Quarterly tracking of the roadmap mobilized through the VA Control Tower (including identifying risks and options for roadmap adjustment)</p> <p>B7. Value Assurance Control Tower Outcome tracking</p> <p>B8. Continuous risk mitigation process mobilized via Value Assurance Control Tower – top 4-5 program risks acted on</p>	<p>Deliverable Requirements for Approval of A7, B7, B8:</p> <ul style="list-style-type: none"> • Create, implement and document the integrated “monthly” vs. “quarterly” review cadence for the Value Assurance Control tower (incl. agenda, artefacts for these control points) – covering roadmap, outcome and risk tracking and decision making • Ensure all key roles and accountabilities are fully understood between the various governance/execution roles, to feed the new Agile cadence • Stress-test the amount of prep/overhead required to execute on the Agile cadence and provide guidance on design to automate/optimize any inefficiencies, for MPI approval • Create outcome tracking for Value Assurance Control Tower

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

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.

August 2, 2023

CONFIDENTIAL

June 15,2023

CONFIDENTIAL

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

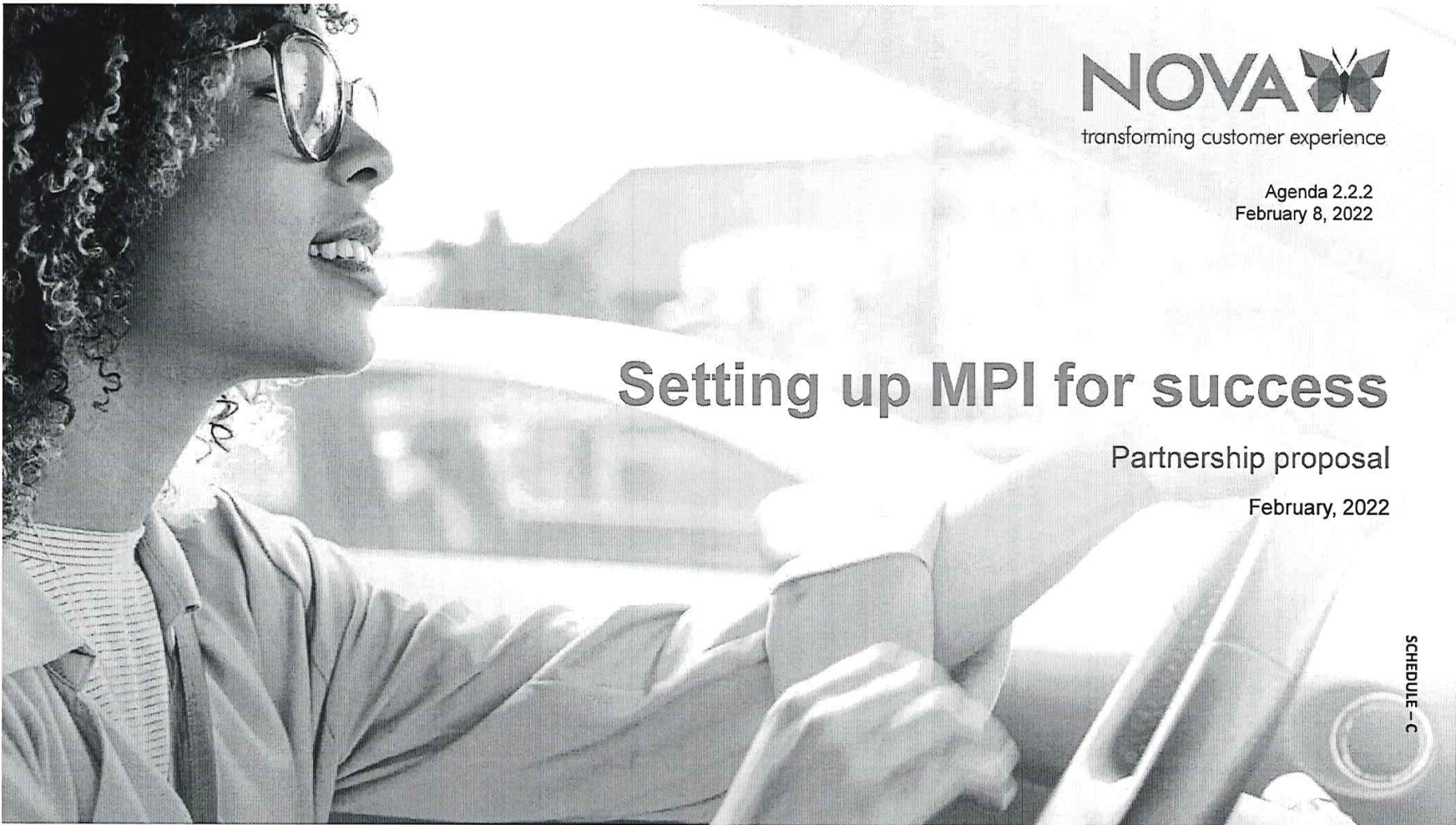
Definitions used in this standard:	<u>Definition / Description</u>
Access control	Means to ensure that access to assets is authorized and restricted based on business and security requirements.
Authenti-cation	Authentication refers to the verification of the authenticity of either a person or system. 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.

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL



NOVA 
transforming customer experience

Agenda 2.2.2
February 8, 2022

Setting up MPI for success

Partnership proposal

February, 2022

SCHEDULE - C

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

The diagnostic identified program and enterprise level requirements to set MPI and the Nova program up for success

What MPI requires to ensure Nova and other related initiatives will be ready to execute as per plan

Program level requirements

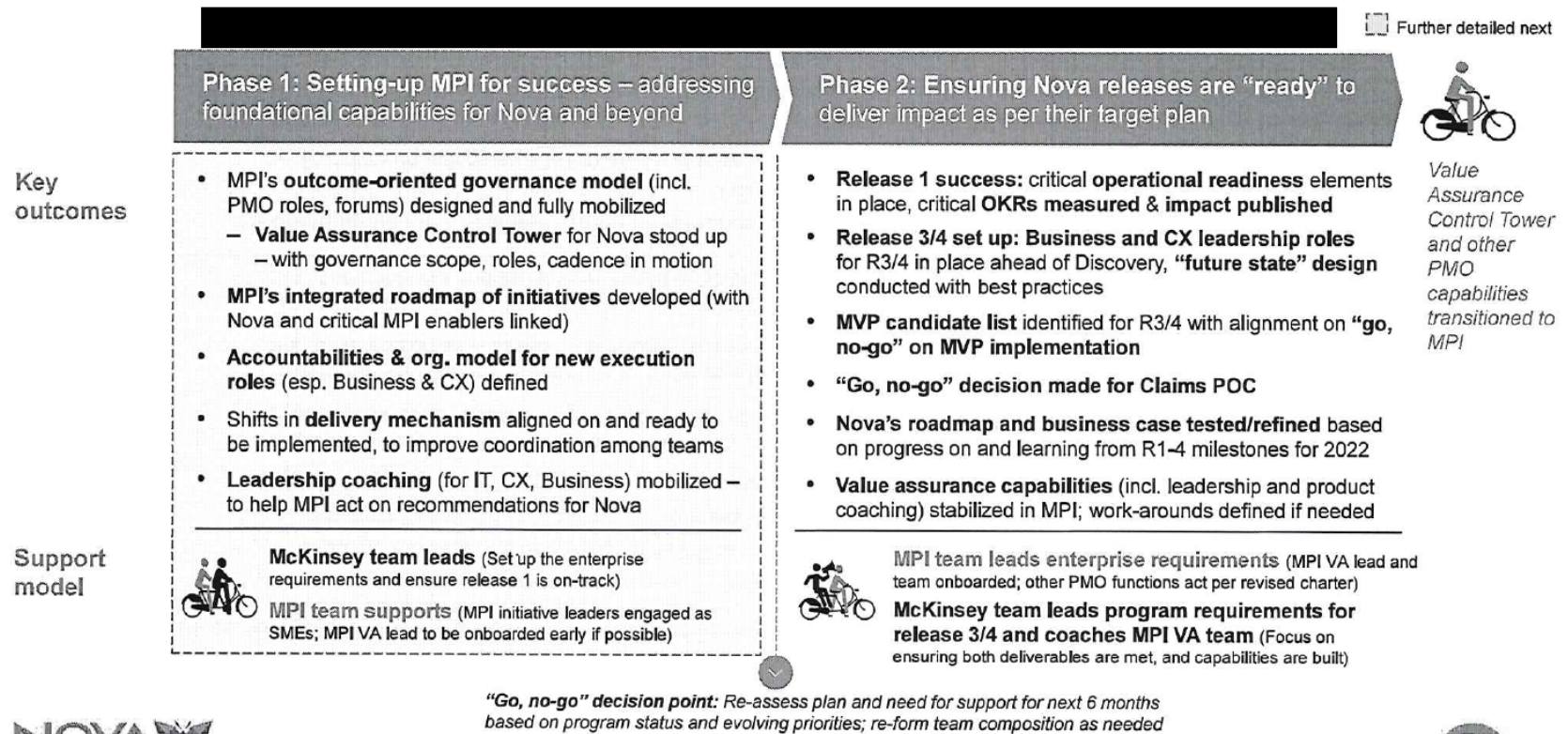
- **De-risking upcoming release milestones**, through targeted problem solving and coaching support for Nova leaders
 - Ensuring Release 1 is delivering on its critical operational readiness elements, ahead of its Q3 2022 release
 - Preparing Release 3 (and optionally, Release 4) for a full-fledged Business and CX led discovery in Q4 2022
 - Helping Nova leaders identify and prepare to act on recommendations around MVPs/POC
- **Expediting impediment resolution**: especially programmatic issues that are cross-functional and go beyond the Nova and PMO teams' current scope (e.g., any changes needed in operating model to improve velocity, resolving architectural issues)
- **Providing “on the job” coaching to business leads** (especially Business Owners, and Product Managers) on how to own and drive outcomes – based on product management best practices that have been identified as a gap
- **Operationalizing the Value Assurance Control Tower** – including clarifying the central role this needs to play beyond the scope of Nova and its closely related enablers.

Enterprise level requirements

- **Standing up an outcome-oriented governance model to oversee critical MPI initiatives**:
 - Clarifying governance roles, processes and control points needed to proactively track and course correct MPI initiatives
 - Standing up outcomes (OKRs) as a tool to scope, prioritize, and show value from each initiative
- **Defining a common integrated roadmap** for Nova and its IT and non-IT enablers (e.g., IT strategy implementation, build out of CX capabilities etc.), and **standing up the mechanism to manage dependencies across initiatives**
- **Clarifying how MPI needs to organize new roles/skills** being introduced (e.g., Business roles like Product Manager/Owner, CX, etc.) – including how to manage and upskill individuals to be productive in their roles
- **Refining the delivery mechanism** to ensure teams of different types (journey vs. platform teams, shared services, etc.) understand how to work with each other (through common Agile cadences, joint planning and governance, etc.)



Proposed support to help MPI address these requirements over the next 12 months to de-risk Nova while building MPI’s capabilities to execute



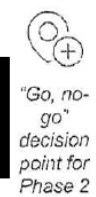
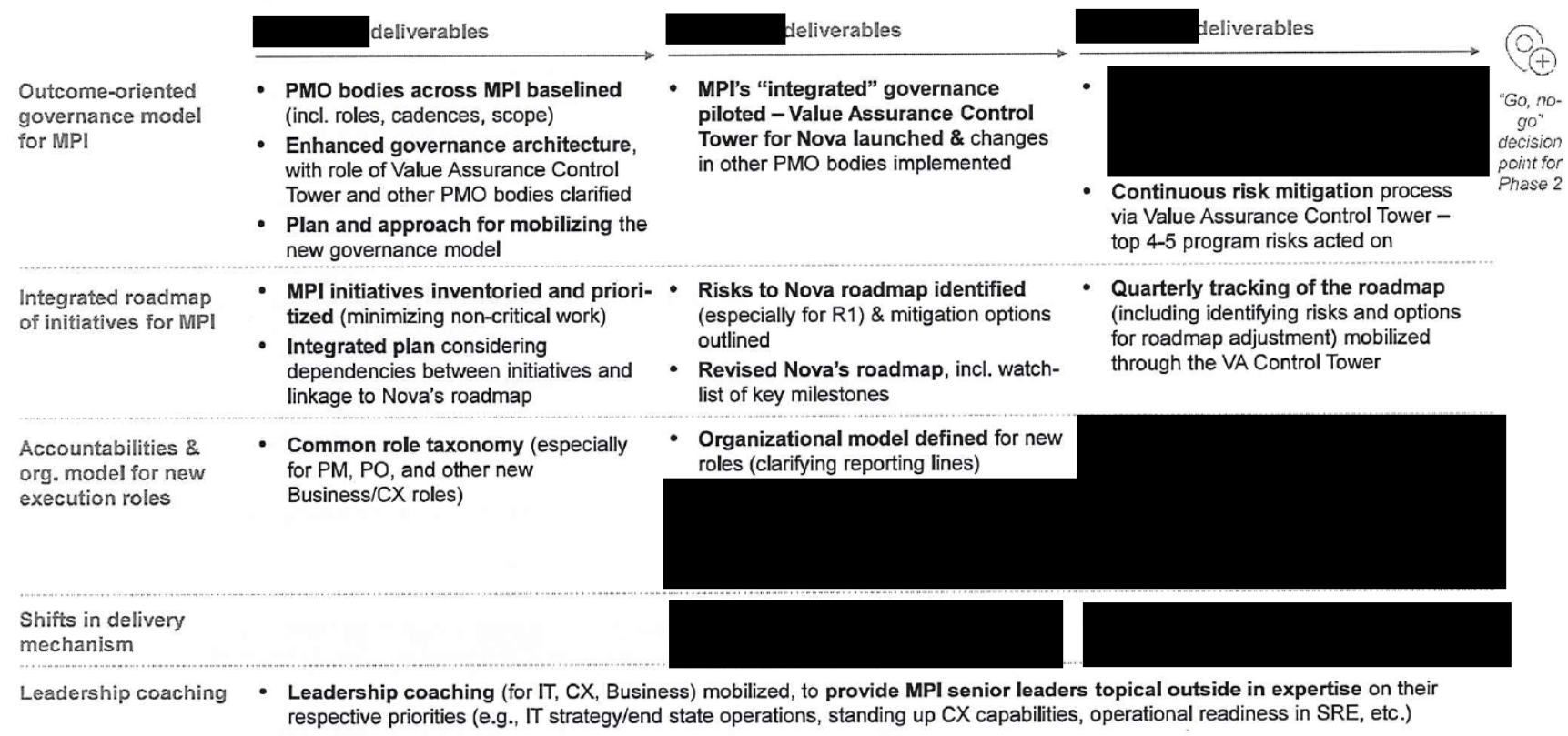
August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

Execution plan for Phase 1 – path to setting up MPI for success



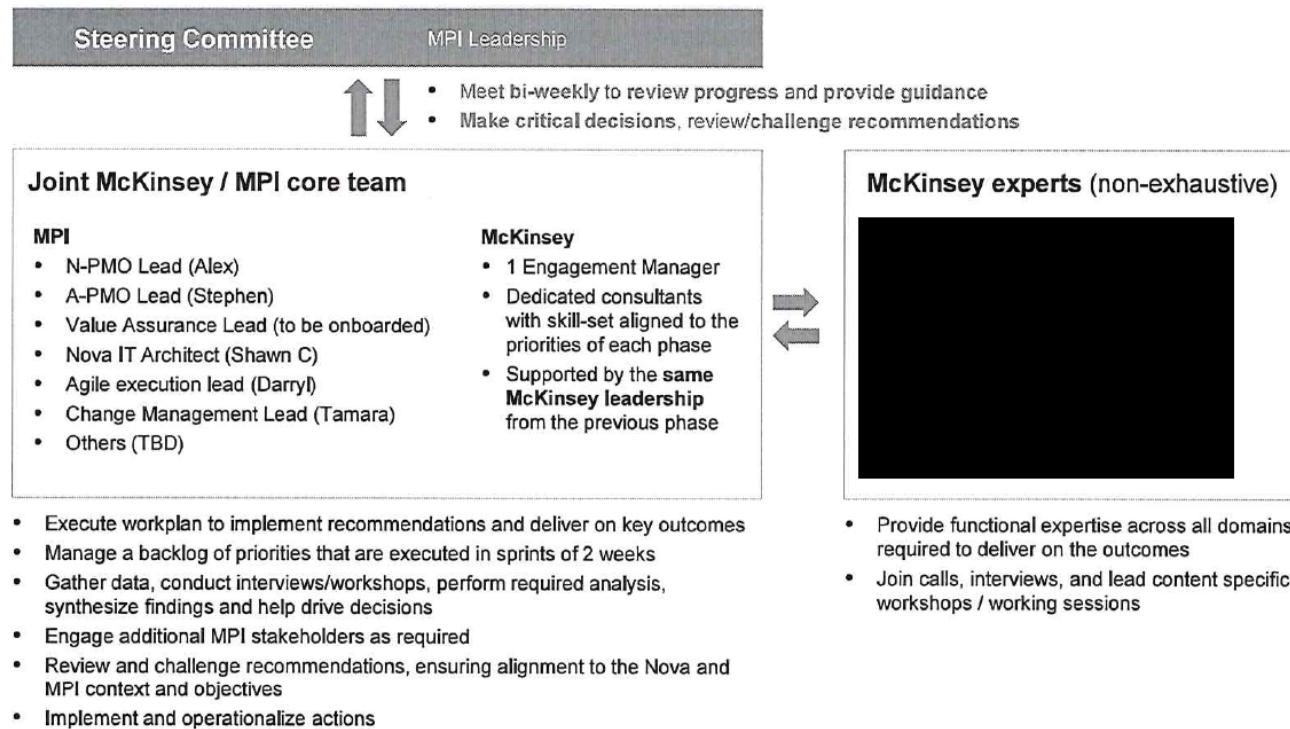
August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

This effort will be led by a joint McKinsey / MPI core team



August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

Backup



6

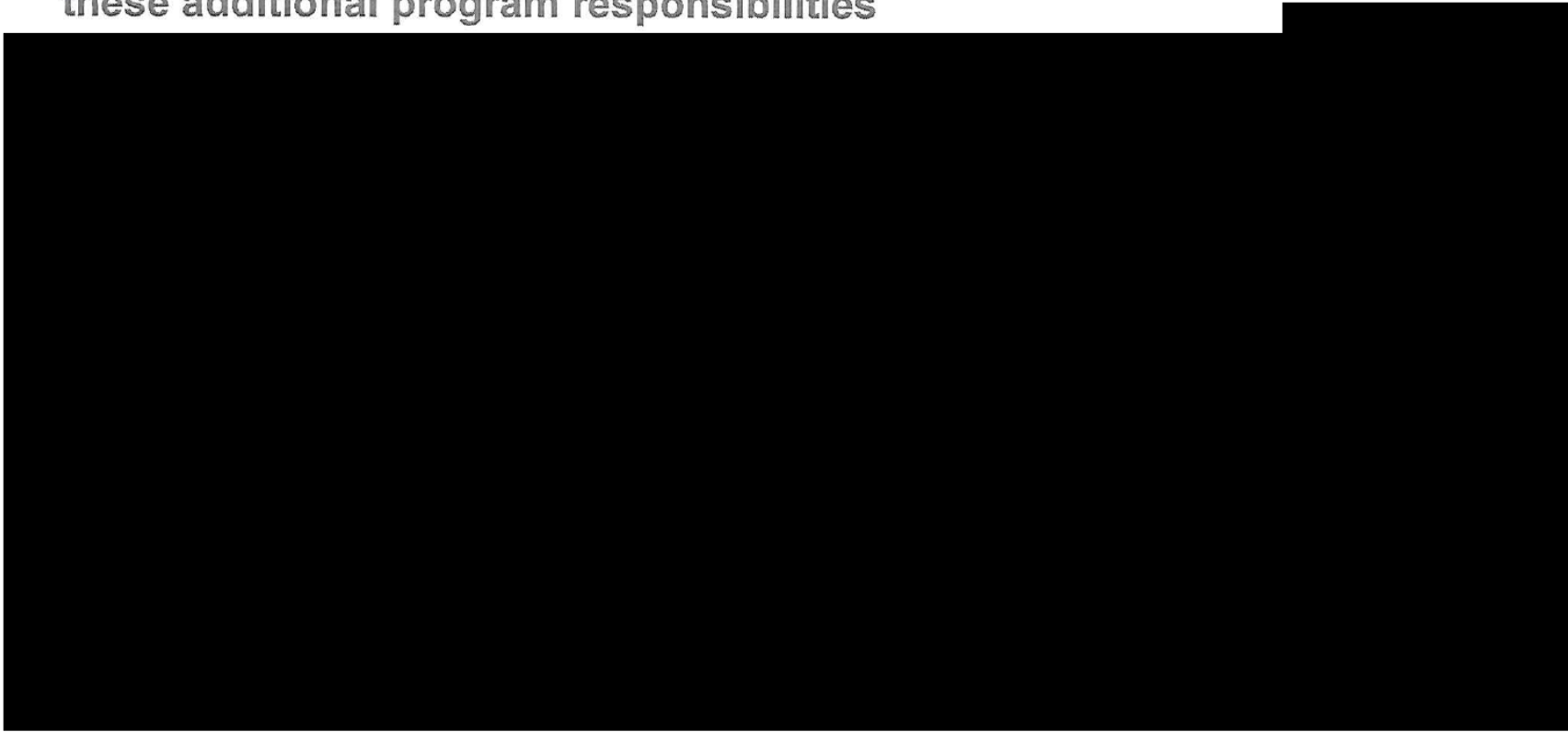
August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

Nova should stand up a Value Assurance “control tower” to address these additional program responsibilities



1. To oversee the coordinated IT strategy execution over multiple dependent Nova and MPI workstreams



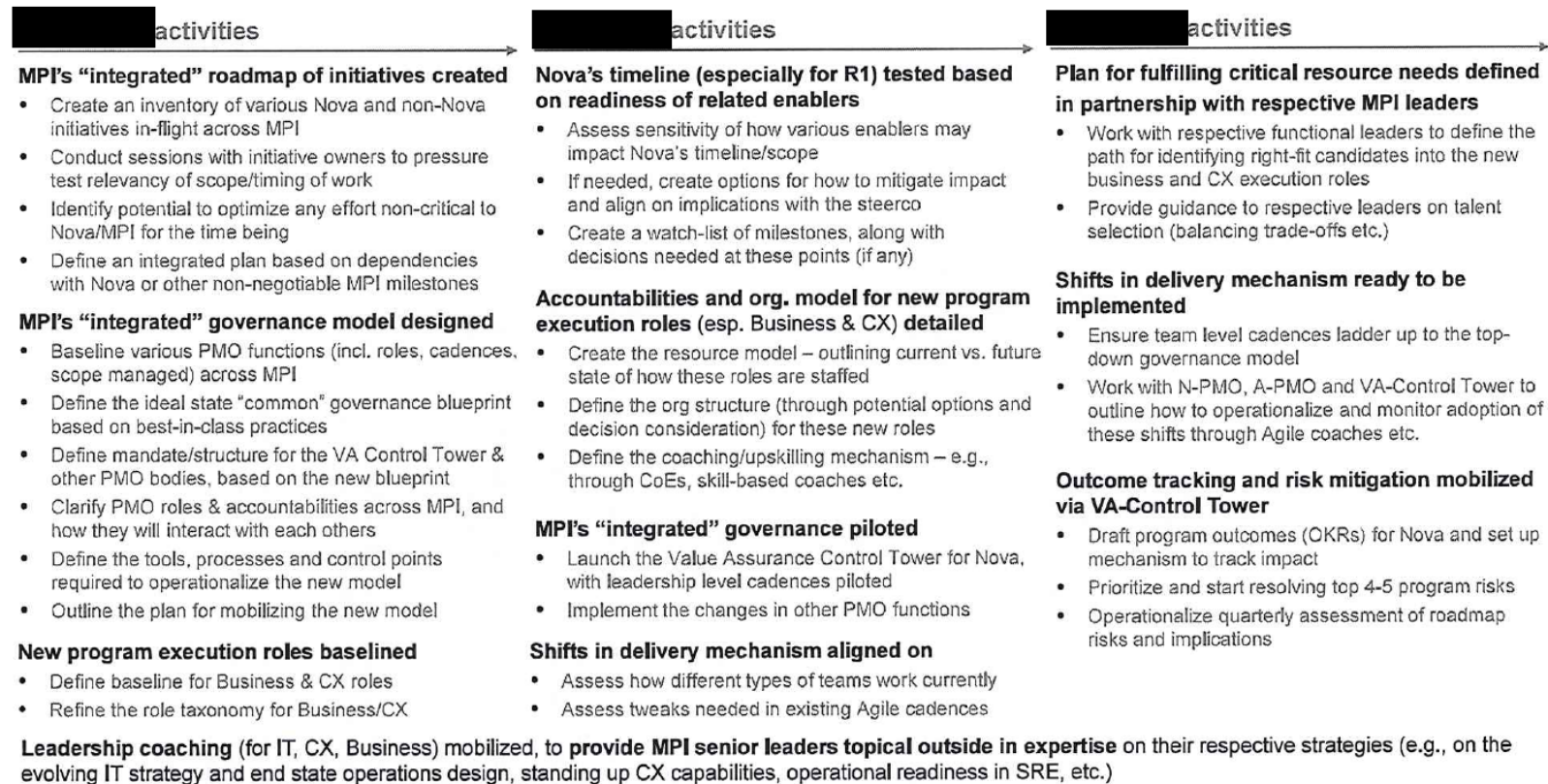
August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

Detailed activities for Phase 1



"Go, no-go" decision point for Phase 2



August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

2024 GENERAL RATE APPLICATION
Part IX – EXP Appendix 23b - Confidential**SCHEDULE – D****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.

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

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

- c. A list of McKinsey's current sub-processors, which shall be updated when new sub-processors are engaged, can be accessed at <https://solutions.mckinsey.com/msd/subprocessors/>, and McKinsey will provide the Client with a mechanism to obtain notification of such updates. McKinsey may also directly notify the Client in the event additional sub-processors may be required to process Confidential Information in connection with the Services.
 - d. If the Client does not approve of any new sub-processor, such approval not to be unreasonably withheld, then Client shall notify McKinsey of such determination and the parties agree to work together in good faith to resolve such concerns. To the extent that they cannot be resolved, McKinsey shall either cease its use of the sub-processor to process the Confidential Information or notify the Client that it may terminate that portion of the Services that require the use of the sub-processor in accordance with the terms set forth in the agreement pursuant to which such Services are provided.
9. Preventing unauthorized access to Confidential Information through the use, as appropriate, of physical and logical entry controls, secure areas for data processing, procedures for monitoring the use of data processing facilities, built-in system audit trails, use of secure passwords, network intrusion detection technology, encryption and authentication technology, secure log-on procedures, and virus protection, monitoring compliance with its policies and standards related to data protection on an ongoing basis. In particular, McKinsey has implemented and complies with, as appropriate and without limitation:
- a. Physical access control measures designed to prevent unauthorized access to data processing systems such as entry controls including the legitimization of authorized persons (e.g., access ID cards, card readers, alarm systems, burglar alarms, video surveillance and exterior security);
 - b. Denial-of-use control measures designed to prevent unauthorized use of data protection systems by technical (keyword/password protection) and organizational measures concerning user identification and authentication (e.g., automatically enforced password complexity, automatic disabling and change requirements, firewalls);
 - c. Requirements-driven authorization scheme and access rights, and monitoring and logging of system access to permit access to data processing systems to only persons with appropriate access rights;
 - d. Data transmission control measures to restrict Confidential Information from being read, copied, modified or removed without authorization during electronic transmission, transport or storage on data media, and transfer and receipt records. In particular, McKinsey's information security program shall be designed to facilitate the encryption "in transit" of Confidential Information over public networks to protect the security of the transmission.
 - e. Penetration tests conducted on McKinsey's IT systems and applications;
 - f. When subcontracting Services involving the processing of Confidential Information, McKinsey shall execute formal agreements with each subcontractor that requires the subcontractor to implement security controls no less stringent than those set forth here and in the attached agreement;
 - g. Measures to protect Confidential Information from accidental destruction or loss including, as appropriate and without limitation, data backup, retention and secure destruction policies, secure

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

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.

August 2, 2023

CONFIDENTIAL

June 15, 2023

CONFIDENTIAL

2024 GENERAL RATE APPLICATION
Part IX – EXP Appendix 23b - ConfidentialMcKinsey
& Company

SCHEDULE – E

Standard Contractual Clauses

The relevant standard contractual clauses as linked below and executed for McKinsey & Company, Inc. United States on behalf of itself and its affiliates (together "McKinsey") are, as applicable for the respective transfer of personal data, deemed automatically incorporated into the relevant services agreement (the "agreement") by virtue of reference to this page and execution of the agreement by McKinsey and the respective counterparty (the "Client").

1. The following standard contractual clauses shall apply in the event that the Client transfers personal data in the absence of an adequacy decision of the competent authority (i) that is subject to the General Data Protection Regulation (2016/679) to McKinsey outside of the European Economic Area or that is subject to the Swiss Federal Act on Data Protection to McKinsey outside of Switzerland, in either case where such transfer occurs before September 27th, 2021; OR (ii) that is subject to the United Kingdom ("UK") General Data Protection Regulation (as implemented by the European Union (Withdrawal) Act 2018) ("UK GDPR") to McKinsey outside of the UK prior to the implementation of an alternate set of standard contractual clauses approved by the UK Government; OR (iii) where the parties otherwise agree or is otherwise required by applicable law to be governed by such standard contractual clauses:
 - Standard contractual clauses as implemented by the Commission Decision (2010/87/EU) of February 5th, 2010 on 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, as applicable to McKinsey's services as set forth in the agreement and available at solutions.mckinsey.com/msd/service-providers/docs/2010-sccs.pdf.

2. The following standard contractual clauses shall apply in the event that the Client transfers personal data in the absence of an adequacy decision of the competent authority (i) that is subject to the General Data Protection Regulation (2016/679) to McKinsey outside of the European Economic Area or that is subject to the Swiss Federal Act on Data Protection to McKinsey outside of Switzerland, in either case where such transfer occurs on or after September 27th, 2021; OR (ii) where the parties otherwise agree or is otherwise required by applicable law to be governed by such standard contractual clauses:
 - Standard Contractual Clauses as implemented by the Commission Implementing Decision (EU) 2021/914 of June 4th, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council – MODULE TWO: Transfer controller to processor –as applicable to McKinsey's services as set forth in the agreement and available at solutions.mckinsey.com/msd/service-providers/docs/2021-sccs.pdf.

This document may be updated from time to time by McKinsey to reflect the promulgation of additional or amended standard contractual clauses or similar approved transfer mechanisms promulgated by data protection authorities and required to effectuate the lawful transfer of personal data in collection with the applicable agreements.



TO: ALL MANITOBA PUBLIC INSURANCE SUPPLIERS

The following Tax-Exempt Certificate will appear on all our purchase orders, work orders, agreements and contracts:

PLEASE NOTE:
GOVERNMENT OF MANITOBA
GST/HST Registration Number:
R122001191

It is hereby certified that the goods and/or services described herein are being purchased with Crown funds on behalf of the Government of Manitoba and are exempt from the Goods and Services Tax and Harmonized Sales Tax.

Suppliers are not to include GST/HST in quoted prices or invoices

As indicated on the Certificate, suppliers are not to include GST/HST for goods and services provided to the Corporation. This will facilitate processing of your invoices and prompt payment.

Please note that the GST/HST Registration number on the certificate is Manitoba Public Insurance's registration number.

The use of the Tax-Exempt Certificate does not affect your right to claim input tax credits on your purchases relating directly to your sales to Manitoba Public Insurance.