

NZ Transport Agency
Review of the effectiveness of
controls to manage third party
access to personal information
held on the Motor Vehicle
Register

August 2017

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



Building a better
working world

Contents

1. Executive summary	2
Summary of findings and remediation actions	3
2. Findings and associated risks	9
3. Appendix A: Objectives, Scope and Approach.....	16
4. Appendix B: Third party access channels to MVR	18
5. Appendix C: Third Party Organisations interviewed	19
6. Appendix D: Rating system	20
7. Appendix E: Purpose of report and restrictions on its use	21

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

1. Executive summary

Definitions

The following definitions are used within this report:

Third parties - individuals, organisations, industry bodies or portal access providers that request access to MVR data via Section 241 of the Land Transport Act 1998, where the end to end access processes is requested and fulfilled by NZTA.

Portal access providers - these are a sub-group of the third parties, who are able to grant access to MVR data via their portal (e.g. InfoLog, Carjam, TradeMe).

Subscribers - individuals or organisations who obtain access to MVR data via portal access providers.

Context

The motor vehicle register (the "register" or "MVR") holds information about motor vehicles and the individuals responsible for such vehicles. The NZ Transport Agency (NZTA) has responsibilities as the 'Registrar' to maintain the register of motor vehicles, including the release of information held on the register. According to the Land Transport Act 1998, the register can be accessed internally by NZTA and government departments and agencies, as well as externally by individuals and organisations. Access can include the vehicle registration and vehicle information but also personal information (names, addresses) of current and historic registered persons or motor vehicles.

NZTA aims to improve their user access management processes for authorised access to personal information under section 241 of the Land Transport Act 1998 (which covers authorised access to name and address details in MVR). NZTA's mandate as the 'Registrar' is to maintain the register of motor vehicles, including the release of information held on the register. They also strive to meet regulatory requirements, including the requirements of the Data Privacy Act 1993. Third party authorisation under section 241 for access to personal information in the Register is considered a critical process and operation within NZTA. 241 access has in the recent past been granted based on 'class' authorisations, which were introduced by the Ministry of Transportation. If a third party organisation that belongs to a certain approved class (e.g. a vehicle trader), applied for access to MVR vehicle information, access to names and addresses was granted in addition by default.

Currently, authorised access is to some extent still granted based on class authorisation and a deadline of 31 October 2017 has been set for an entire cut over to the new application process. Most recently, NZTA has designed changes to this process to improve efficiency, which have not as yet been implemented.

NZTA has contracted Ernst & Young ("EY") to conduct a health check assessment of the design and operation of section 241 processes, focusing on the user access management process for third parties, NZTA administration of access to MVR and third parties' use of personal information from MVR.

Objectives

This objective of this review is to assess that the processes and controls in place to govern, manage and control third party access to personal information in MVR are designed and operating effectively.

Scope

The scope of this review was to assess the processes and controls in place to manage third party access to personal information held on the register, including:

1. Processes and controls to grant third party access to personal information in MVR to individuals and / or organisations through authorised access applications under section 241.
2. IT security controls in place for the MVR system as they relate to 241 access.

(A detailed overview of the scope and approach can be found in Appendix A).

This review has been performed through interviews with NZTA personnel, third parties and through the review of documentation provided by NZTA.

Overall assessment conclusion

In this conclusion we share the risk context and our key findings.

MVR contains the name and address of registered persons, which is personal information, protected by the Land Transport Act 1998 as well as the Privacy Act 1993. With the volume of transactions exceeding 10 million a year, MVR is in high demand for New Zealand business and many Government organisations (including law enforcement). The risk profile of the application, based on the level of information stored within MVR, can be seen as low profile, even though the integrity and availability of this information is critical to many of the third parties. During the years of operation, we are not aware of a major incident that has become public, which reflects some degree of reliability of the service.

Our key findings from this review are:

1. The processes, especially for reviewing and assessing third party applications for 241 access, are inherently capable to comply with the Land Transport Act 1998, Section 241.
2. The changes to the design to improve the 241 application approval processes are well balanced and have the potential to increase efficiency without compromising compliance.
3. Meeting the 31st October deadline for ceasing class authorisation may be challenging.
4. Opportunities for improvements exist in the overall governance of MVR and implementing and documenting the end to end 241 access management process.

Based on the findings, our overall assessment of the effectiveness of the control environment is 'Partially Effective' based on NZTA's internal ratings standard (refer to Appendix D).

Rating	Description
Partially Effective	The controls are adequate but manage only a portion of the risk. Management attention is required to implement new or improve existing controls. Multiple moderate findings and/or a low number of high findings have been identified.

Summary of findings and remediation actions

We identified a number of gaps in the management and operation of the user access lifecycle related to 241 access. These gaps relate to the following three categories:

1. Governance over the 241 access processes and operations.
2. Compliance with regulatory requirements.
3. Access and security management operations.

We have identified twelve findings and grouped them across these three categories. Based on NZTA's internal methodology for rating risks (Refer to Appendix D), we identified 2 high, 9 medium and 1 low finding.

Our key findings in these areas are summarised below.

Category	Finding	Risk Rating
Governance over the access processes and operations	<p>1) Our assessment found that the impact for decommissioning the class authorisations has not been properly documented and effectively communicated, for example:</p> <ul style="list-style-type: none"> ▶ There are approximately 4000 third parties and subscribers whose access (under the class authorisation) is due to expire on 31 October 2017 as NZTA plans to discontinue class based approvals. There is a plan on how this is to be addressed but there is a lack of ownership of the plan and reduced confidence in NZTA's ability to meet this deadline. ▶ Portal Access Providers (e.g. InfoLog, Carjam, TradeMe) are uncertain how they will be required to validate 241 access approval from 31 October 2017 before granting access and how to deal with current access that has not gone through the 241 application process. <p>The risk implication is that the 31 October 2017 deadline may not be met, that third party and subscriber access may expire without clear visibility that this will happen, and that portal access providers may be granting unauthorised access or not removing expired access. This could lead to disgruntled third parties and could have a negative reputational impact on NZTA.</p>	High
	<p>2) Our assessment found that Governance responsibilities for MVR have not been defined, specifically identification of the data owner and who is responsible and accountable for the 241 access management processes and operations, including resourcing.</p> <p>The risk implication is that the execution of the end to end processes has an insufficient level of guidance and oversight potentially resulting in inappropriate access and use of MVR data.</p>	High

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Category	Finding	Risk Rating
	<p>3) Our assessment found insufficient internal documentation.</p> <ul style="list-style-type: none"> ▶ The documentation governing the 241 access management process does not cover the end to end process (including granting, updating, reviewing, monitoring and removing access). ▶ The access management documentation covers the key steps in the 241 access process for granting access but does not cover how the process should be executed (for example the first step in the process is “check documents and ensure that all questions have been answered completely”, there is no further guidance on how correctness can be assessed). ▶ The process design of third party access management for MVR does not appear to have been clearly assessed from a risk and controls perspective. <p>The risk implication is that third party and subscriber access to MVR data may be granted inappropriately or that authorised access is used by third parties for purposes that have not been approved. Inappropriate access may also be granted to NZTA employees, which could result in the misuse of MVR data. There is also a risk that access management processes take longer than necessary, resulting in reduced service levels or disruption of services provided to third parties.</p>	Medium
Compliance with regulatory requirements	<p>4) Our assessment did not find evidence of non-compliance with the Land Transport Act 1998. NZTA inherited the class authorisation concept for MVR from the Ministry of Transportation and NZTA is intended to move away from this. We found the following:</p> <ul style="list-style-type: none"> ▶ The application questionnaire completed by third parties for 241 access, does not consistently have a reasonable level of information to enable NZTA to properly evaluate the validity of the applicant’s business case and their processes in place to protect personal information. ▶ Individual re-assessments of applications have not consistently been performed every five years, even though 241 access for individuals and organisations covered by certain approved classes was authorised for a timescale that exceeds five years. ▶ Applicants are indicating that they are not being informed within a reasonable timeframe of the access decisions (application assessments are taking many months with a number of examples taking longer than 6 months). <p>The risk implication of these findings is that NZTA may approve access which does not meet the requirements of the Land Transport Act 1998, Section 241. NZTA have to ensure ongoing compliance with the Land Transport Act 1998, Section 241, to avoid potential reputational damage and legal action.</p>	Medium

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Category	Finding	Risk Rating
	<p>5) Our assessment has identified opportunities for strengthening privacy controls.</p> <ul style="list-style-type: none"> ▶ Formal contracts are not in place with third parties who are granted Section 241 access to MVR. A letter is sent to third parties upon access approval, which contains terms and conditions, these do not include the requirement to comply with the Privacy Act 1993. ▶ A documented plan is not in place for identifying and managing personal information breaches. ▶ Personal information of opted-out registered persons are exposed to third parties. <p>The risk implication is that NZTA or other third parties (including organisations, portal access providers and industry bodies) may not be complying with the Privacy Act 1993 and may not be able to identify, contain, investigate and report on breaches when they occur. Non-compliance with the Privacy Act 1993 could result in potential reputational damage and legal action.</p>	Medium
Access and security management operations	<p>6) Our assessment found that there are minimal clearly defined procedures in place for:</p> <ul style="list-style-type: none"> ▶ Managing end to end access (including granting, updating, reviewing and removing access). ▶ Monitoring 241 access to identify suspicious activity. <p>The risk implication of these findings is that third parties use their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected. This could also lead to non-compliance with the Privacy Act 1993 which could result in potential reputational damage and legal action.</p>	Medium
	<p>7) Our assessment found that under the current class authorisations, there is an incomplete view of the number of individuals and third parties (including organisations, portal access providers and industry bodies) with access to personal information from MVR.</p> <p>The risk implication is that third parties misuse their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected.</p>	Medium
	<p>8) Our assessment found that NZTA has no transparency or control around how access to MVR is granted through the different portal access providers (e.g. InfoLog, Carjam, TradeMe). Portal access providers can grant access up to the maximum level of access they have received by NZTA. There is no standardised access scheme or model in place. The portals are able to set and grant access levels based on their own discretion.</p> <p>The risk implication is that third parties use their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected.</p>	Medium

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Category	Finding	Risk Rating
	<p>9) Data usage: Our assessment found that there is limited verification by NZTA over how the third parties are using and protecting MVR data or if they are complying with NZTA's terms and conditions. Some third parties are required to provide annual audit reports on access to MVR, however these are not reviewed by NZTA and the criteria for requiring audit reports have not been clearly defined.</p> <p>The risk implication is that third parties (including organisations, portal access providers and industry bodies) use their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected.</p>	Medium
	<p>10) Data handling/extraction: Our assessment found that NZTA has limited oversight or control over what third parties are doing with the personal information extracted from MVR, where the data is being stored or how it is being used and protected. There is an indication that queries are being made to MVR to replicate the data.</p> <p>The risk implication is that third parties (including organisations, portal access providers and industry bodies) use their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected.</p> <p>This could lead to non-compliance with the Privacy Act 1993, which could result in potential reputational damage and legal actions.</p>	Medium
	<p>11) Our assessment found that privileged access (which enables a user to grant access to MVR) is granted to NZTA staff that are not part of the access management team and do not required this level of access.</p> <p>The risk implication is that access is granted to NZTA employees inappropriately resulting in unauthorised access and misuse of data in MVR. This is a common issues that we see in many organisations and is simple to address through implementing privileged access rules and consistently following them.</p>	Medium
	<p>12) Our assessment found that requirements for information security, including password settings, are not documented and are applied inconsistently.</p> <p>The risk implication is inappropriate configuration of systems, which could lead to information being more easily compromised.</p>	Low

We recommend that NZTA evaluates the risks and impact of postponing the 31 October 2017 deadline for decommissioning the class authorisations. Prior to communicating a revised deadline, a clearly defined strategy and reliable action plan needs to be defined, to avoid further extensions of the class authorisations. We suggest the following next steps:

1. Agree governance responsibilities.
2. Complete an impact assessment for implementing the new 241 access process.
3. Define the future state.
4. Develop a roadmap, including the activities NZTA needs to perform to get to the future state, including,
 - a. Process and technology changes required (both internally and by third parties)
5. Based on the roadmap, derive a detailed plan for a reasonably planned, resourced, paced and conservatively risk-balanced delivery (including timeline, costs, and resources).
6. Develop a communication plan (internally and to third parties).

Thorough execution of this approach is likely to set NZTA up for the future to more reasonably mitigate the risks of non-compliance, unauthorised access and disruption to services. It should also significantly enable NZTA to develop and execute a realistic, achievable and risk managed plan for implementing an efficient 241 end to end access process.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

2. Findings and associated risks

Note to reader: This section provides more details related to the findings above and will benefit the responsible operations teams.

Please refer to Appendix D for a description of the risk ratings.

Category	Finding(s)	Potential risk(s)	Risk Rating
Governance	<p>F1 - Our assessment found that the impact for decommissioning the class authorisations has not been sufficiently documented and effectively communicated.</p> <p>There are approximately 4000 third parties and subscribers whose access (under the class authorisation) is planned to expire on 31 October 2017 as NZTA plans to discontinue class based approvals. There is a plan on how this is to be addressed but there is a lack of ownership of the plan and reduced confidence in NZTA's ability to meet this deadline.</p> <p>Portal Access Providers (e.g. InfoLog, Carjam, TradeMe) are uncertain how they will be required to validate 241 access approval from 31 October 2017 before granting access and how to deal with current access that has not gone through the 241 application process.</p>	<p>The risk implication is that the 31 October deadline may not be met, that third party access may expire without clear visibility from the third parties that this will happen, and that portal access providers may be granting unauthorised access or not removing expired access. This could lead to disgruntle third parties and could have a negative reputational impact on NZTA.</p>	High
Governance	<p>F2 - Our assessment found that governance responsibilities for MVR have not been defined, specifically identification of the data owner and who is responsible and accountable for the 241 access management processes and operations.</p> <p>We noted that roles and responsibilities for owners of MVR data and processes related to third party access to MVR have not been clearly defined. In consequence, a number of departments and stakeholders are engaged and involved, and knowledge is spread across a few individuals within the organisation.</p>	<p>As accountability and responsibility is not clearly defined there is a higher risk that processes are not standardised, documented or performed appropriately resulting in inappropriate access and use of MVR data.</p>	High

Category	Finding(s)	Potential risk(s)	Risk Rating
Governance	<p>F3 - Our assessment identified a lack of internal documentation</p> <p>Current processes</p> <p>The documentation governing the 241 access management process does not cover the end to end process (including granting, updating, reviewing, monitoring and removing access).</p> <p>We observed the following gaps in documentation:</p> <ul style="list-style-type: none"> ▶ The access management documentation covers the key steps in the 241 access process but does not cover how the process should be executed (for example the first step in the process is "check documents and ensure that all questions have been answered correctly", there is no further guidance on how correctness can be assessed). ▶ The process for granting NZTA employees with privileged access to MVR is not clearly defined. As a result privileged access may be inappropriately assigned (refer to F11). NZTA has not defined guidelines/requirements for third parties to comply with when assigning privileged access (e.g. user administration) to their users. ▶ Even though there are individual assessments per application, a holistic risk and controls assessment has not been performed to identify and assess risks resulting from processes, procedures and operations of third party access to MVR. <p>Newly designed changes to 241 process</p> <p>The documentation on the newly designed changes for Section 241 access process does not cover the end to end process. The documentation contains the revised five step process for approving Section 241 authorisation but does not cover granting, updating, reviewing, monitoring and removing access.</p> <p>There may be technology changes requires as a result of the changes to the process. These have not been documented.</p>	<p>There is a higher risk that third party access to MVR is granted inappropriately, e.g. granting access to unauthorised users or granting the wrong access levels.</p> <p>There is a higher risk that third parties use their authorised access to MVR data for purposes that have not been approved.</p> <p>There is a higher risk that unauthorised access is granted to NZTA employees resulting in unauthorised access and misuse of information.</p> <p>As processes are not clearly defined there is a higher risk that access management processes take longer than necessary resulting in reduced service levels or disruption of services provided to third parties.</p>	Medium

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Category	Finding(s)	Potential risk(s)	Risk Rating
Compliance	<p>F4 - Our assessment found no evidence of non-compliance with the Land Transport Act 1998. However the current processes are not fully meeting the intent of the Land Transport Act 1998 Section 241.</p> <p>NZTA inherited the class authorisation concept for MVR from the Ministry of Transportation and NZTA is intended to move away from this. We found the following:</p> <ul style="list-style-type: none"> ▶ The application questionnaire completed by third parties for 241 access, does not consistently have a reasonable level of information to enable NZTA to properly evaluate the validity of the applicant's business case and their processes in place to protect personal information. ▶ Individual re-assessments of applications have not consistently been performed every five years, even though 241 access for individuals and organisations covered by certain approved classes was authorised for a timescale that exceeds five years. ▶ Applicants are indicating that they are not being informed within a reasonable timeframe of the access decisions (application assessments are taking many months with a number of examples taking longer than 6 months). 	<p>The risk implication of these findings is that the Agency may approve access which does not meet the requirements of the Land Transport Act 1998, Section 24. NZTA and third parties (e.g. Access Portal Providers) have to ensure ongoing compliance with the Land Transport Act 1998, Section 241, to avoid potential reputational damage and legal action.</p>	Medium

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Category	Finding(s)	Potential risk(s)	Risk Rating
Compliance	<p>F5 - Our assessment has identified opportunities for strengthening privacy controls.</p> <p>Formal contracts are not in place with third parties who are granted Section 241 access to MVR. A letter is sent to third parties upon access approval, which contains terms and conditions, these do not include the requirement to comply with the Privacy Act 1993.</p> <p>There is no defined plan for identifying and managing breaches to personal information. Data breaches in the past have not been detected internally. There have not been investigations into the breaches to assess the root cause and whether remediation actions are adequate and complete.</p> <p>MVR data including personal information is stored indefinitely by some third parties. There is no specific requirement by NZTA which prohibits third parties from downloading and storing data indefinitely.</p> <p>Personal information of opted-out registered persons are exposed to third parties.</p>	<p>The risk implication of this is that NZTA or other third parties (including organisations, portal access providers and industry bodies) might not be able to manage compliance with the Privacy Act 1993 or identify, contain, investigate and report on breaches when they occur. Non-compliance with the Privacy Act 1993 could result in potential reputational damage and legal actions.</p>	HighMedium
Operations	<p>F6 - Our assessment found there are no identifiable specific procedures in place for:</p> <ul style="list-style-type: none"> ▶ Managing end to end access (including granting, updating, reviewing and removing access). ▶ Monitoring 241 access to identify suspicious activity. <p>Access operations are executed to the best knowledge of the individuals performing the activities. Standardised procedures and a clear understanding of responsibilities and activities, especially with regards to updating, reviewing, monitoring and removing access could not be identified.</p>	<p>There is a higher risk that third parties (including organisations, portal access providers and industry bodies) use their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected.</p> <p>This could also lead to a decreased level of-compliance with the Privacy Act 1993 which could result in potential reputational damage and legal actions.</p>	Medium

Category	Finding(s)	Potential risk(s)	Risk Rating
Operations	<p>F7 - Our assessment found that under the current class authorisations there is an incomplete view of the number of individuals and third parties (including organisations, portal access providers and industry bodies) with access to personal information from MVR.</p> <p>NZTA was not able to advise on the total number of third parties that have been authorised for 241 access due to 'class authorisations' approach to granting access. There is not standard approach to granting access across the portal access providers.</p>	<p>There is a higher risk that third parties (including organisations, portal access providers and industry bodies) use their authorised access to MVR data inappropriately (i.e. not for its intended purposes).</p>	Medium
Governance	<p>F8 - Our assessment found that NZTA has limited transparency or control around how access to MVR is granted through the different portal access providers (e.g. InfoLog, Carjam, TradeMe). There is no standardise access scheme or model in place. The portals are able to set and grant access levels based on their own discretion.</p> <p>NZTA has four different 241 access levels implemented for granting access to Motochek. There is no transparent guidance for how NZTA should provision these access levels, e.g. when to grant access to personal information of individuals who have opted-out.</p> <p>There is no clear guidance for portal access providers that have the ability to access opted-out information around how this level of access should be granted to other third parties. We noted one portal access provider with access to opted-out and historical information and the ability to grant this access to other third parties. Generally, portal access providers can only grant access up to the maximum level of access they have received by NZTA.</p> <p>End user credentials are not validated by the public Application Programming Interface (API) when accessing data through third party portal access providers (i.e. access to MVR via third parties cannot be tied to a specific individual or organisation).</p> <p>Some third parties have multiple or shared user IDs.</p>	<p>There is a higher risk that third parties (including organisations, portal access providers and industry bodies) use their authorised access to MVR data inappropriately (i.e. not for its intended purposes).</p> <p>Without clearly defined guidance for managing personal information there is a higher risk that NZTA and its third parties will not be able to manage compliance with the Privacy Act 1993. Non-compliance with the Privacy Act 1993 could result in potential reputational damage and legal actions..</p>	Medium

Category	Finding(s)	Potential risk(s)	Risk Rating
Operations	<p>F9 - Data usage: Our assessment found there is no verification by NZTA over how the third parties are using and protecting MVR data or if they are complying with NZTA's terms and conditions. Some third parties are required to provide annual audit reports on access to MVR, however these are not reviewed by NZTA and the criteria for requiring audit reports have not been clearly defined.</p> <p>During the review we noted:</p> <ul style="list-style-type: none"> ▶ There is no defined process in place to monitor the access activities of third parties such as access patterns/statistics of access to identify suspicious activities. ▶ There is no process in place to perform compliance monitoring or audit of third parties (refer to F6). A number of third parties have to provide NZTA with an annual compliance and usage report. There is no standard report provided to third parties to complete and there no evidence that the received reports are reviewed or actioned by NZTA. ▶ Some of the portal access providers have the technical capability to log user access to MVR, but this is not being utilised by NZTA for auditing purposes. 	<p>Without clearly defined processes to monitor access activities there is a higher risk that inappropriate access usage will go undetected.</p>	Medium
Operations	<p>F10 - Data handling/extraction: Our assessment found that NZTA has no oversight or control over what third parties are doing with the personal information extracted from MVR, where the data is being stored or how it is being used and protected. There is an indication that queries are being made to MVR to replicate the data.</p> <p>MVR data, including personal information, is stored indefinitely by some third parties. There is no requirement by NZTA which entitles or prohibits third parties from downloading and storing data indefinitely.</p>	<p>There is a higher risk that third parties (including organisations, portal access providers and industry bodies) use their authorised access to MVR data inappropriately (i.e. not for its intended purposes).</p> <p>This could lead to a decreased level of-compliance with the Privacy Act 1993 which could result in potential reputational damage and legal actions.</p>	Medium

Category	Finding(s)	Potential risk(s)	Risk Rating
Operations	<p>F11 - Privileged access (which enables a user to grant access to MVR) is granted to NZTA staff that are not part of the access management team and do not required this level of access.</p> <p>The access management team is responsible for granting access to third parties based on the rights contained within the email received from the Customer Response Team (CRT) team. We confirmed that a total of 6 people should have privileged access roles to manage user access There are more than 6 individuals with this privileged access.</p> <p>NZTA was unable to provide process for granting privilege user access as well as privilege user listings at the time of this review.</p>	<p>A higher risk has already materialised, that access is granted to NZTA employees inappropriately resulting in unauthorised access and misuse of information.</p>	Medium
Operations	<p>F12 - Requirements for information security, including passwords settings are not documented and applied inconsistently.</p> <p>NZTA could not provide an Information Security policy or policy that outlines what the requirements are for safeguarding the information. Passwords for access to Active Directory (which is required to gain internal access to MVR) do not meet the New Zealand Information Security Manual (NZISM) standards.</p> <p>Password settings are configured differently across the Portal Service Providers including Motochek.</p>	<p>Lack of formal information security policies including password polices should increases the higher risk of inappropriate configuration of systems to protect information. This also increases the risk of not meeting the minimum technical security standards for good system hygiene as detailed in the New Zealand Information Security Manual.</p>	Low

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

3. Appendix A: Objectives, Scope and Approach

Objectives

This overall objective of this review is to assess whether the processes and controls in place to govern, manage and control third party access to personal information on the motor vehicle register are designed and operating effectively. An action plan will be developed to address any process and/or control weaknesses identified.

Scope

The Transport Agency is the Registrar of the motor vehicle register with regard to the holding and releasing (as applicable) of personal information held on the register to third parties. The scope of this review is to assess the processes and controls in place to manage third party access to personal information held on the register. This includes the following processes and controls:

1. Processes and controls to grant third party access to personal information in the motor vehicle register to individuals and / or organisations through authorised access applications under section 241, specifically:
 - a. The process by which applications are submitted.
 - b. The process by which NZTA assesses, approves (or rejects), and responds to these applications, including consultation with the Privacy Commissioner, the Chief Ombudsman, and the Commissioner of Police.
 - c. The process by which NZTA grants relevant user access, the contractual requirements provided to relevant organisations, and the guidance provided to these users (both organisations and the relevant staff members) regarding their obligations with respect to the Land Transport Act 1998 and Privacy Act 1993.
 - d. User access management processes for those NZTA staff user profiles that have access to grant authorised access applications to the MVR, including appropriateness of individuals that have such access at the time of the review.
 - e. The user access profile design within MVR for authorised access applications - specifically whether this design excludes access to the following information: personal information for those persons who have 'opted out' of having their information released; and personal information for persons who were previously registered in respect of motor vehicles.
 - f. The process by which NZTA identifies the need for and removes third party user access in cases of authorised access being revoked and / or the termination of employment for third party staff members with MVR access.
 - g. Processes for the ongoing monitoring and management of third party access to personal information from the motor vehicle register, including the process to identify and respond to notifications of unauthorised access, and processes to gain assurance that third parties comply with the requirements and guidance provided by NZTA (refer c above).
 - h. The newly designed processes for group and class authorisations, and specifically whether these address the issues previously identified by NZTA.
 - i. Visit up to 20 third parties (to be confirmed) to:
 - ▶ Interview key personnel to understand how they have implemented the NZTA MVR access requirements
 - ▶ Observe how access to the MVR system and information is managed.
2. IT security controls in place for the MVR system, specifically:
 - a. System configuration - password settings and sign on procedures,
 - b. Privileged access- administration and monitoring, and
 - c. Remote access - the mechanism by which third parties access MVR and how this is secured.

The review will:

- ▶ Assess the current processes for managing third party access to personal information held on the motor vehicle register, specifically access requested under section 241 (authorised access) of the Land Transport Act 1998 (EY),
- ▶ Identify key risks, including legislative compliance risks, to the effective management and control of third party access to personal information EY),
- ▶ Identify and document the controls in place to manage third party access to personal information and to detect unauthorised access to such information (EY),
- ▶ Assess whether the changes made to the group and class authorisations processes and controls are designed effectively (EY),
- ▶ Assess the design and operating effectiveness of the controls identified (operating effectiveness testing of group and class authorisations will be out of scope) (EY),
- ▶ Identify gaps and weaknesses in the current controls (EY), and
- ▶ Identify actions to address the gaps identified, including immediately actionable changes (NZTA, with feedback provided by EY as to whether the actions address the risk).

Approach

The MVR third party access assessment conducted by:

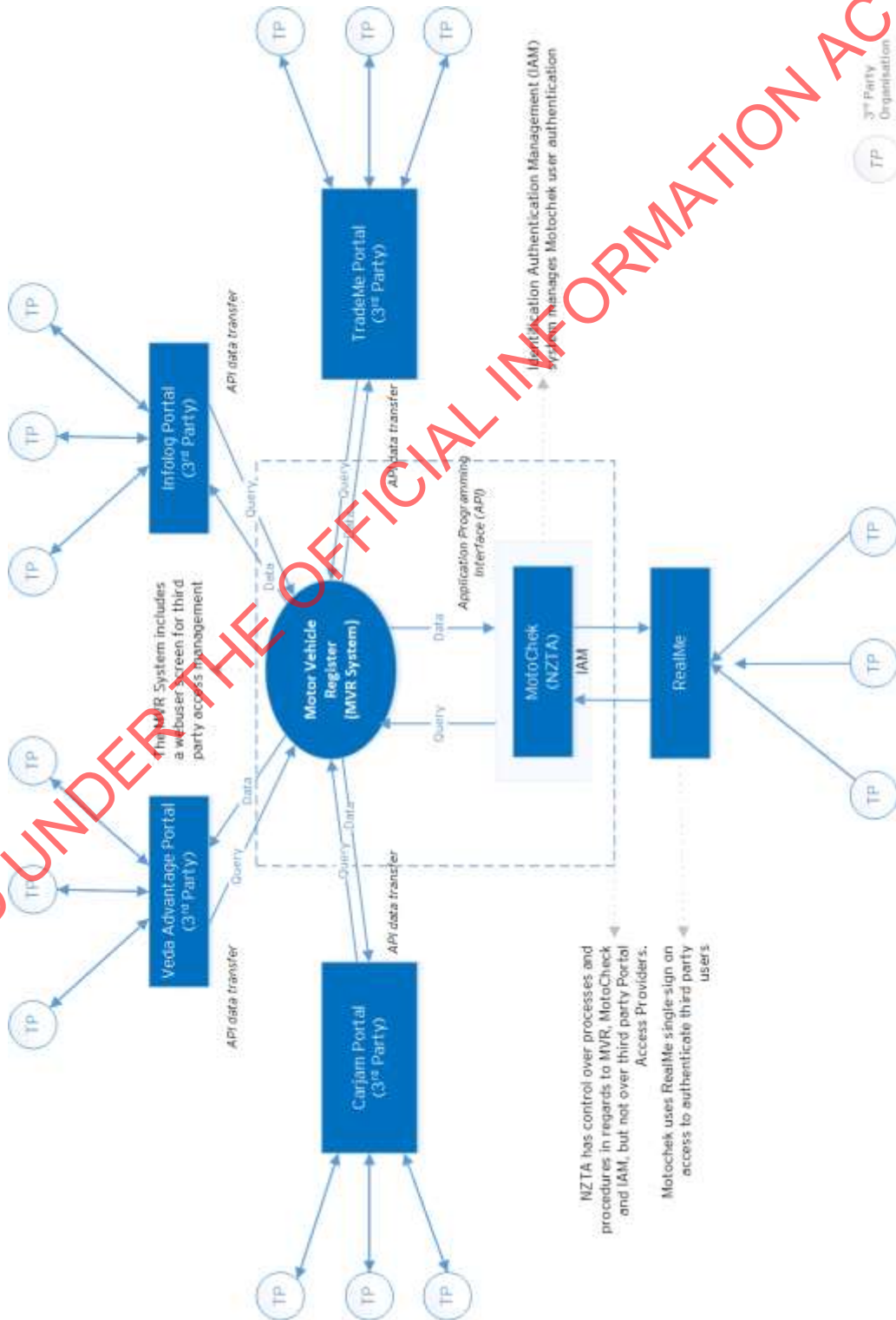
- ▶ Understanding the existing process for granting Section 241 authorisation access.
- ▶ Interviewing NZTA business process owners and selected third parties to understand the processes relating to the above scope and objectives.
- ▶ Documenting the processes and validation of existing process documentation.
- ▶ Confirming our understanding of the processes with business process owners.
- ▶ Identifying key controls within the process; and testing the controls for design and operating effectiveness
- ▶ Identifying key controls to manage the identified
- ▶ Collating our findings, review the work performed and summarise results.

Arranging a closing meeting with you to discuss the preliminary results. Most of these results will have been socialised with business process owners as they are identified during the assessment.

As outlined in the body of the report, we have proposed remediation actions that, once implemented, should strengthen the existing processes. Details of high, moderate and low observations from the assessment are contained in the Findings and Observations section of this report.

4. Appendix B: Third party access channels to MVR

The diagram below shows the connectivity between MVR and selected Portal Access Providers (including NZTA's Motochek). It also shows the wider eco-system with the thirds party channels for accessing MVR for personal information of registered persons.



5. Appendix C: Third Party Organisations interviewed

#	Organisations	Business	Contact Persons
1	InfoLog	Portal Access Provider	Murray Towers
2	Carjam	Portal Access Provider	Paul Osborne
3	Gasoline Alley Services	Petrol station	Kylie Baudet Andrew Bowie
4	Motor Vehicle Trade Association	Association	Greig Epps Tony Everett
5	Toyota	Vehicle manufacturer and distributor	Kerrin Soderberg
6	Equifax	Portal Access Provider	Michael Amyes
7	NZ Private Fire Service	Emergency response and security	Paul Stanley
8	TradeMe	E-Commerce	Georgina Leslie
9	Bartle Group	Towing and hauling services	Rebecca Morgan
10	Club Auto Insurance	Insurance	Brandon Bailey
11	Sages Holdings	Motor Vehicle Trader	Peter Gormly
12	Lemon Check	Portal Access Provider	Chris Wenzlick
13	Thompson & Toresen Investigations Limited	Private Investigator	Daniel Toresen
14	Gull New Zealand Limited	Fuel Supplier	Melanie Day
15	Financial Services Federation (FSF)	Industry Body	Lyn McMorran
16	Wilson Parking	Parking Enforcement	Matt Ransom

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

6. Appendix D: Rating system

The following rating system has been used to identify the significance of the findings.

Risk Ranking Matrix					
	Insignificant	Minor	Moderate	Severe	Extreme
Almost certain	Low	Medium	High	Critical	Critical
Likely	Low	Medium	High	Critical	Critical
Possible	Low	Medium	Medium	High	Critical
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Low	High

The following rating system has been used to identify the overall effectiveness of

Effectiveness of Control Environment	Descriptions
Strong	The controls are in place and are working very well. The controls are being performed in the manner for which they are designed to mitigate the risk. Either none or a small number of low findings, and either no or minimal scope for improvement has been identified.
Effective	The controls are good and the majority of the risk is managed. But there is room for some improvement to increase the effectiveness of these controls or reduce the risk of the control failing. Multiple low findings and/or a single moderate finding has been identified.
Partially Effective	The controls are adequate but manage only a portion of the risk. Management attention is required to implement new or improve existing controls. Multiple moderate findings and/or a low number of high findings have been identified.
Not Effective	The controls are either not effective or non-existent. Urgent attention and management review are required to implement new controls. A large number of high findings have been identified and/or a critical finding has been identified.

7. Appendix E: Purpose of report and restrictions on its use

Our Report may be relied upon by NZTA for the purpose set out in the Scope section only pursuant to the terms of the accepted CSO and corresponding Variations signed 8 May 2017. We disclaim all responsibility to any other party for any loss or liability that the other party may suffer or incur arising from or relating to or in any way connected with the contents of our report, the provision of our report to the other party or the reliance upon our report by the other party.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit ey.com.

© 2017 Ernst & Young, New Zealand.
All Rights Reserved.

This communication provides general information which is current at the time of production. The information contained in this communication does not constitute advice and should not be relied on as such. Professional advice should be sought prior to any action being taken in reliance on any of the information. Ernst & Young disclaims all responsibility and liability (including, without limitation, for any direct or indirect or consequential costs, loss or damage or loss of profits) arising from anything done or omitted to be done by any party in reliance, whether wholly or partially, on any of the information. Any party that relies on the information does so at its own risk.

ey.com

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982