Submission No 8

EXAMINATION OF THE AUDITOR-GENERAL'S PERFORMANCE AUDIT REPORTS DECEMBER 2014 - JUNE 2015

Organisation: Transport for NSW

Name: Mr Tim Reardon

Position: Secretary

Date Received: 22 August 2016

Security of Critical IT Infrastructure

Remediation Status

Recommendation		Accepted or Rejected	Actions to be taken	Due Date	Status (completed, on track, delayed) and Comment	Responsibility (Section of agency responsible for implementation)
1	Extending the ISMS to oversee the security of the complete traffic management environment, including operational level risks.	Accepted	The TfNSW ISMS is being prepared for re-certification prior to 30 June 2015 which will cover the components maintained by Group IT. SAI Global has been selected in December 2014 to conduct the re-certification and will commence in January 2015.	Jul-15	**Completed** ISMS scope for TfNSW (Group IT) has been finalised and documented. The TfNSW ISMS is now certified to ISO 27001:2013 standard. The scope only coveres the activities of IT Service Delivery of TfNSW.	Group IT – Principal Manager, Security Policy (Gijo Varghese)
			The TMC ISMS is being reviewed for re-certification in 2015. It will cover the SCATS system, Central Manager and regions under TMC control.	Jul-15	**Completed** The TMC ISMS was sucessfully re-certified in June 2015 to the updated ISO: 27001, 2013 version	TMC – Principal Manager, TMC Systems (Ray Treuer)
			The RMS ISMS scope will be extended to include the traffic light environment	Jul-15	**Completed** The extension of the ISMS will heavily leverage the achievements already delivered by TMC, TfNSW and RMS. The Management Structure of the ISMS includes representation from each of the accountable parties. The ISMS extension to include the Traffic Light Environment has now been established, and has been independently audited (July 2016), as required by the standard. It was not a requirement that this ISMS extension be formally certified. However, we have determined that certification is the most effective method of showing maturity and obtaining formal independent assurance. Hence, following on from the recent audit, the recommendation (by the certification auditors) for certification will also be completed in July 2016.	RMS – Security and Technology Risk Manager (Frank Davies)
2	Developing a comprehensive security plan for the whole environment.	Accepted	TMC is reviewing the ISMS for components under their control and will develop a Security Plan, as part of the ISMS re-certification process	Jul-15	**Completed** An end to end diagram of the Scats Traffic Management environment has been developed, and the TfNSW, RMS and TMC responsibilities identifed.The TMC ISMS scope was updated prior to re-certification, and the components under TMC control, assessed and appropriate controls are in place.	TMC – Principal Manager, TMC Systems (Ray Treuer)
			TfNSW is reviewing the ISMS for components under their control and and will develop a Security Plan, as part of the ISMS re-certification process	Jul-15	**Completed** TfNSW Group IT ISMS scope has been finalised in ISMS framework manual. The scope includes services delivered by IT Service Delivery to TMC.	Group IT – Principal Manager, Security Policy (Gijo Varghese)
			A comprehensive security plan will be developed for the RMS environment.	Sep-15	**Completed** As part of the formalisation of the ISMS, a Security Management Plan and associated risk management activities have been implemented. The ISMS was formally independently audited, and recommended for certification in July 2016.	RMS – Security and Technology Risk Manager (Frank Davies)

Recommendation		Accepted or Rejected	Actions to be taken	Due Date	Status (completed, on track, delayed) and Comment	Responsibility (Section of agency responsible for implementation)
3	Improving the identification, assessment and recording of security risks.	Accepted	TMC will align risk management practices with TfNSW Enterprise Risk Management (TERM) framework.	Jul-15	**Completed** The TMC ISMS Risk register was rewritten using the TfNSW Enterprise Risk Management (TERM) framework	TMC – Principal Manager, System Operations (Ray Treuer)
			ISMS will align Group IT risk management processses. Group IT have adopted the TfNSW Enterprise Risk Management (TERM) framework for the identification and assessment of risk, and it will be reflected in the improved Risk Register.	Jul-15	**Completed** Group IT has established a Transport Cluster Technology (TCT) Security and Risk (S&R) Committee. This committee will provide oversight on risk management practices including identification and recording of operational IT risks across the Transport Cluster. TMC is a key participant of the TCT S&R Committee. Additionally, IT Security and Risk team has provided TMC with an IT risk template and is assisting TMC to adopt TfNSW Enterprise Risk Management (TERM) framework.	TfNSW Senior Responsible Officer (SRO) for Digital Security (David Colquitt)
			Operational risks will be tracked and managed as part of the RMS ISMS.	Sep-15	**Completed** Operational Risk Management has been achieved and managed as part of the management controls environment implemented within the Process Control Environment for the Traffic Light Environment. Risk Management is a key control requirement for certification of an ISMS. All risks are reviewed and discussed by the ISMS Committee, and acceptability of the risk and the associated risk treatment plans is agreed. Residual risk is considered as part of the formal review process.	RMS – Security and Technology Risk Manager (Frank Davies)
4	Revising the assessment of risk to better reflect current controls, rather than planned but yet to be implemented controls, and clarify the risk levels that can be tolerated.	Accepted	See Recommendation 3.			N/A
5	Improve logging and monitoring of security related events regarding access to applications, operating systems and network access.	Accepted	Relevant security and system logs will be feed to a central security monitoring tool	Jul-15	**Completed** Security and system logs are fed into the tool being deployed by the enterprise Security Monitoring and Assessment project.	TMC – Principal Manager, TMC Systems (Ray Treuer)
			A Security Monitoring & Assessment project was endorsed by the Transport Custer Technology Steering Committee on 2 October 2014. The SMA project will introduce significant improvements to security monitoring capabilities across the cluster. As part of implementation, relevant traffic management systems will be integrated into the SMA project.	Dec-15	**Completed** Security tools have bveen deployed and handed over to TMC. TMC is now responsible for business as usual (BAU) management. Group IT will monitor, assist and provide continuous improvement to the platform.	Principal Manager, IT Risk and Security (Nataliya Stephenson)
6	Introduce a formalised procedure and approach to the assessment of security alerts	Accepted	Regional servers will be checked to ensure they are configured to check for antivirus updates daily and to receive them as needed.	Completed	**Completed** All regional servers receive virus definition updates automatically when they are released by software supplier.	TMC – Principal Manager, System Operations (Ray Treuer)

Recommendation		Accepted or Rejected	Actions to be taken	Due Date	Status (completed, on track, delayed) and Comment	Responsibility (Section of agency responsible for implementation)
	and the recording of risk management decisions in response to these alerts. This should include assessing the commodity application and control system vendor software vulnerability notices and		A Security Monitoring & Assessment project was endorsed by the Transport Custer Technology Steering Committee on 2 October 2014. The SMA project will introduce significant improvements to security monitoring capabilities across the cluster. As part of implementation, relevant traffic management systems will be integrated into the SMA project.	SMA - July 2015 NGIS – July 2017	**Completed** Security tools have bveen deployed and handed over to TMC. TMC is now responsible for business as usual (BAU) management. Group IT will monitor, assist and provide continuous improvement to the platform.	Principal Manager, IT Risk and Security (Nataliya Stephenson)
7	Implement the Top 4 ASD mitigation guidelines and consider implementing the remainder of the ASD top 35.	Accepted	See Recommendation 6.			
8	Improve security zoning to better protect the system from potential threats.	Accepted	Security zoning model will be reviewed and improved. Relevant security controls will also be reviewed and enhanced.	Jul-15	**Completed** Security zoning enhanced and security controls tightened.	TMC – Principal Manager, TMC Systems (Ray Treuer)
9	Improving the access control mechanism for traffic control software including social media and IT system administration utilities (TfNSW/RMS)	Accepted	1st stage - Exceptions noted in the audit was addressed immediately. 2nd stage - All vulnerabilities identified through penetration testing will be remediated by 2015 quarter 4.	1st stage – Dec 2014 2nd stage – Q4 2015	**Completed** Recommendation implemented at time of audit and final resolution completed in 2015.	RMS - Manager, Traffic Systems Applications (Steven Shaw)
10	Ensuring and maintaining adequate technical skills through ongoing training for all staff requiring admin user access (TfNSW/RMS)	Accepted	A computer based training Security Awareness package is currently being piloted across TfNSW and will be available for use by all staff in March 2015. Starting FY15-16, it will be mandatory for all Transport staff to complete the CBT annually. An Information Security Handling Standard and Information Security Handling Procedure are being developed as part of the ISMS. The standard will be published by 30 June 2015 and the draft procedure will be available by 30 June 2015.	Jul-15	**Completed** The Learning Management System (LMS) environment for Information Security Awareness Training is now deployed and ready to use. TMC staffs have been registered for the training and it is their management's responsibility to ensure they complete the awareness training.	Group IT – Principal Manager, Security Policy (Gijo Varghese)
			TMC Systems staff to receive updated security briefing from TfNSW. Staff training address through staff personnel development plans.	Jul-15	**Completed** Security training provided to all Systems staff.	TMC – Principal Manager, TMC Systems (Ray Treuer)
11	Assessing the software vulnerabilities notices and action or record the risk management decisions. (TfNSW/RMS)	Accepted	See Recommendation 6.			

Recommendation		Accepted or Rejected	Actions to be taken	Due Date	Status (completed, on track, delayed) and Comment	Responsibility (Section of agency responsible for implementation)
12	Developing and conducting a program to perform vulnerability assessments and security penetration tests, at least annually, to verify the security of the key components and networks used to access TMC systems and associated workstations. (TfNSW/RMS).	Accepted	RMS will engage an external independent company to do penetration testing on a periodic basis.	Jul-15	**Completed** SCATS (Sydney Coordinated Adaptive Traffic System) Software testing complete and ongoing.	RMS - Manager Traffic System Applications (Steven Shaw)
13	Assess the risk of the vulnerabilities identified in the security penetration test and develop an appropriate action plan (TfNSW/RMS).	Accepted	See Recommendation 12.			N/A
14	Developing a program to improve locks on traffic signal boxes as a part of a periodic maintenance program (RMS)	Accepted	RMS is working with the other Australian States and Territories to finalise a design that will incorpoate the audit recommendation.	Jul-15	**Delayed** RMS has provided a solution to roll out keyed locks at all intersection's controller cabinets and will progress during 2016/17 now that funding has been confirmed Contract maintenance providers will install these locks over the next two financial years	RMS - Manager Traffic System Applications (Steven Shaw) Date to
15	Expediting initiatives to replace outdated software. (TfNSW/RMS)	Accepted	Outdated software associated with critical positions will be replaced.	Jul-15	**Completed** All outdated software in critical operations areas have been replaced and upgraded.	TMC – Principal Manager, TMC Systems (Ray Treuer)
16	By July 2015, develop a program of testing the disaster recovery capability following the delivery of the TMC IT disaster recovery project (TfNSW/RMS)		Disaster recovery, standby servers for the SCATS system are in place. Schedule disaster recovery tests for a SCATS region.		**Completed** The SCATS disaster recovery region testing is included in the annual disaster recovery test plan.	TMC – Principal Manager, TMC Systems (Ray Treuer)
17	By January 2015, ensure a program of ongoing training is in place to provide relevant staff with the knowledge to respond to a real or suspected security incident (TfNSW/RMS).	Accepted	See Recommendation 10.			

Recommendation		Accepted or Rejected	Actions to be taken	Due Date	Status (completed, on track, delayed) and Comment	Responsibility (Section of agency responsible for implementation)
18	By July 2015, ensure a tested IT disaster recovery plan is in place that meets the maximum acceptable outage timeframes should a disaster occur (TfNSW/RMS).		Test SCATS system backups for data integrity, and failover a SCATS region server and run for 24hours on one of the standby servers.		**Completed** The disaster recovery plan for a SCATS region has been tested. A live region was failed over to a standby region and operated for 24 hours. A SCATS reion backup has been restored and checked that the data was valid.	TMC – Principal Manager, TMC Systems (Ray Treuer)