Prioritized Approach Milestones for PCI DSS v.3.2.1 r1

PCI DSS Requirements v3.2.1	Milestone	Status *Please enter "yes" if fully compliant with the requirement*	If status is "N/A", please explain why requirement is Not Applicable	If status is "No", please complete the following		
				Stage of Implementation	Estimated Date for Completion of Milestone	Comments
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1	No		Planning	August 30, 2024	Update / develop network diagrams for all CDE systems including Envibe and the telephony network. Diagrams must include wireless networks and the CDE network components. Decommisioning of the Aquatic Centre will partially address this requirement by removing it from scope.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	2	No		Planning	April 30, 2025	Document the required ports and protocols in use for all CDE systems including the Envibe network and Contact Centre. Document security features required to protect unencrypted telephony calls. Decommisioning of the Aquatic Centre will partially address this requirement by removing it from scope.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	3	No		Planning	April 30, 2025	Document security features required to protect unencrypted telephony calls.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	2	No		Planning	April 30, 2025	Document security features required to protect unencrypted
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	3	No		Planning	April 30, 2025	Review the configuration of the telephony servers
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	2	No		Planning	April 30, 2025	Undate the PCI scope and inventory documentation to include Contact Centre workstations acting as telephony endpoints.

9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.	2	**No**		**Planning**	June 30, 2024	Review the list of EFTPOS terminal devices and ensure that all required information is accurate. Consider implementing a process to review the list on a quarterly or annual basis.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	2	**No**		**Planning**	September 30, 2024	Work with the ASV scan provider to enable scanning of in scope IP addresses to provide a passing scan report. Specifically firewalls protecting CDE components, telephony components exposed to the internet and remote access services managed by City of Adelaide.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	2	**No**		**Planning**	April 30, 2025	Investigate options for removing the telephony system from the PCI scope. Consider options such as DTMF clamping, segmentation of the telephony system, online only payments or call back on an analogue PSTN / mobile phone.
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	6	**No**		**Planning**	March 31, 2024	Review and update the security policy suite of documents at least annually.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	2	**No**		**Planning**	March 31, 2024	Document the roles and responsibilities for development and distribution of incident response processes and procedures.
12.8.1 Maintain a list of service providers including a description of the service provided.	2	**No**		**Planning**	June 30, 2024	Review the management of service providers and ensure documentation of in scope service providers includes details of the services provided.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	2	**No**		**Planning**	June 30, 2024	Educate new procurement personnel on the requirement to monitor service provider compliance status.

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**2**	**No**		**Planning**	June 30, 2024	Document the requirements each service provider is responsible for maintaining on CofA's behalf. Service providers should include at least JP Media, Infor, Advam, MiClub, Envibe, Microsoft, Duncan Solutions and Designa.