ACT Government Provider Capability Questionnaire

Introduction

This questionnaire is for completion by service providers. You have been provided with this questionnaire as a Service Provider/Vendor to provide information to support a Security Assessment of an ICT System/Solution.

This questionnaire contains four sections, each in a different worksheet:
1. General Questions for All Providers
2. Solution Specific Questions for All Providers
3. General Questions for Cloud Service Providers
4. Cloud Solution Specific Questions

Provide your organisation’s responses in an editable format only and return with supporting documents to the business area contact who sent you this questionnaire and CC cyber.security@act.gov.au.

Your response will be considered in confidence. However, if sensitive information is included contact us to arrange a secure transfer method.

If you require assistance in completing this questionnaire, contact the Cyber Security Team on +61 02 6205 5196 during our core business hours of Monday – Friday, 9:00am to 5:00pm AEST.

ACT Government Business Area:	<Please advise name of business area you are working with>
Vendor:	<Please provide name of principal vendor providing solution>
Name of solution:	<Please provide name of solution>

Section 1. General Questions for All Providers

The following questions are for all providers and ask about your business, terms and conditions, certifications and audits etc.

Subsection		Question		Response
1.1.	Provider Profile	1.1.1.	Where is your head office registered?	97 Bankers Road, Bywong, NSW 2621
		1.1.2.	Which countries do you deliver services from?	Australia
1.2.	Terms of Service	1.2.1.	Does the provider allow the ACT Government to negotiate Terms of Service (ToS) or must they accept a standard Terms of Service (ToS)?	Yes.
		1.2.1.1.	If no, provide a copy (or link) of the provider's standard Terms of Service.	
1.3.	Certifications and Audits	1.3.1.	List any relevant security certifications, the certifying authority, and certification numbers.	
		1.3.2.	Please provide any third-party audit reports you are willing to share.	
1.4.	Environments	1.4.1.	List all proposed environments including Development, Test, and Production:	Schedule 2.2(a)(xi) [redacted]
		1.4.2.	Do you use or request the use of Production data in non-Production environments?	[redacted]
		1.4.2.1.	If yes, list the implemented security and privacy controls for protection of Production data in these environments:	[redacted]
		1.4.3.	Which (if any) environments will your staff (including subcontractors, third parties etc.) have access to?	[redacted]
		1.4.3.1.	How will this access occur (i.e., remote access? Supervised?)	[redacted]

Section 2. Solution Specific Questions for All Providers

The following questions are for all providers and ask about the solution you are providing to ACT Government. Please answer these questions in the context of this solution.

Subsection	Question	Response
2.1. Logging and Auditing	2.1.1. Describe the logging and auditing of systems, solutions, or infrastructure (including networks) that handle ACT Government information. Please include information about what operations are logged (i.e., create, change, view, delete, access right changes etc.):	eVACS® (the provided solution) is a standalone, closed (embedded) system allowing the activation of a very specific set of functions via menus. The system has no users, uses a highly cutdown Linux OS (no administrative GUI, no powertools, no logons) to help manage the very restricted operations to setup and conduct the voting and counting for a Legislative Assembly Election. When operating, eVACS® consists of an isolated (physically secured) single Election Server (ES), up to 20 (isolated, physically secured) Polling Place Servers (PPS) and (typically) 10-20 Voting Clients (VC) connected to each PPS via ethernet LAN only. All servers contain only eVACS® functionality. Standard Linux OS system logging is active on all servers and clients which captures most (if not all) events/actions. eVACS® is only active for elections, including casual vacancies.
	2.1.2. Can audit logs be exported from the solution and if so, in what formats?	No. System logs are store on each server, but currently there is no menu item provided to export such logs. However, each PPS provides a separate log of cancelled votes and particular voting-errors. These logs are ultimately exported as part of server report.
	2.1.3. How long are audit logs retained by the solution if not exported?	Forever.
	2.1.4. Do you maintain any manual audit logs for the solution?	No.
2.2. Authentication Options	2.2.1. Does the service support federated single sign-on using SAML 2.0, OAuth 2.0, or OpenID.Connect?	No.
	2.2.1.1. If not, list other available options for single-sign on or state “not available” and detail available authentication options, including any capacity for multi-factor authentication.	
	2.2.2. Does the service support integration with Customer Identity Management Systems such as Microsoft B2C, Salesforce Identity or other third-party solutions?	No.
	2.2.3. How will users be provisioned, managed, and de-provisioned?	Other than (selected) administrators, the only users of eVACS® are electors who, once authenticated outside the eVACS® system, are provided with a unique eVACS®-generated QR code which the elector must scan at an eVACS® voting client in order to create and submit a vote. The only 'commands' available to an elector are displayed (on a touchscreen) and can only be activated by button selection + mouse-click. There is no keyboard, but a visually impaired voter is provided with a keypad that only allows the equivalent of command selection + mouse click. Various messages guide the elector in producing a submitable vote (consisting of a set of sequentially ordered preferences). Once the elector is satisfied with his/her vote, it can be submitted, which is achieved when the elector scans the QR code again. No other QR code can be scanned for vote submission. Once the elector has submitted his/her vote, the QR code cannot be re-used.

2.3.	Mobile Options	2.3.1.	Does your solution support access via a mobile application?	No. No bluetooth or wifi either!
		2.3.1.1.	If yes, detail security mechanisms employed by the application - for example, any Mobile Device/Application Management integration capability, data encryption, PIN code/biometric or other application lock functionality, any other mechanisms to secure access to and data within the application.	
2.4.	Personnel	2.4.1.	Describe the personnel vetting and pre-employment checks applied to all staff (whether directly employed or contracted through a supplier) with any access to systems, solutions, or infrastructure containing ACT Government information:	Schedule 2.2(a)(xi) [redacted]
		2.4.2.	Describe any administrative access your staff, third parties, subcontractors etc. will have to the solution:	[redacted]
		2.4.3.	Describe the personnel vetting and pre-employment checks applied to staff with administrative access to the solution:	[redacted]
		2.4.4.	Describe the cyber-security training your staff receive:	[redacted]
		2.4.5.	Are duties segregated between staff (i.e., testers and developers have specifically defined roles and responsibilities with little or no overlap)	[redacted]
2.5.	Network Overview	2.5.1.	Show all network nodes involved in the delivery and maintenance of the service, the nature of the connectivity and description of information flow between nodes. If possible, estimate the total monthly information transfer volume and peak transfer rate for interfaces traversing the ACT Government firewall. This information may be provided through another medium such as design documentation.	See the attached diagram labelled 'eVACS Layout'. Please note that transfer activities occur (essentially) once every 4 years (when conducting Legislative Assembly Election). In 2020, there were ~273,000 electors who voted, of which ~71% (~194,000) used eVACS®. The latter volume of votes was transferred from 20 polling places to the ES over a period of 3 weeks using Veracrypt-encrypted USBs with independent passwords. Please see attached file named 'eVACS_Layout_2020.png'
2.6.	Encryption and Key Management	2.6.1.	Describe the encryption used to protect ACT Government information	
		2.6.1.1.	In transit:	Schedule 2.2(a)(xi) [redacted]
		2.6.1.2.	At rest:	[redacted]
		2.6.1.3.	In use:	[redacted]

		2.6.2.	Describe your key management methodology:	Schedule 2.2(a)(xi)
		2.6.3.	Which encryption protocols and algorithms are enforced?	We use only those protocols and algorithms recommended by ASD.
		2.6.3.1.	Have you explicitly denied obsolete encryption methods / obsolete earlier versions of encryption (i.e., TLS 1.1 and below)?	The VC-PPS connections use the TLS 1.2 protocol and HTTPS to ensure that VCs are connected to the right PPS. This is the only type of network connection in eVACS®.
2.7.	Integration	2.7.1.	If the solution will integrate with ACT Government systems, describe technical options available for these integrations:	N/A because eVACS® is a standalone, closed (embedded) system with very restricted functions activated from menus and requiring very restricted input (types). It does not integrate with any other system.
		2.7.1.1.	Describe the data that will be exchanged	N/A.
		2.7.1.2.	If methods for protection of data in transit differ from question 2.6.1. detail them here:	N/A.
2.8.	Third Party Service Providers	2.8.1.	List all third parties involved in providing your service (including suppliers and subcontractors) and detail:	Software Improvements Pty Ltd. (SI) Stratum ICT Pty Ltd. (SICT) SI and SICT have formed a joint venture company named Digital Elections (DE). As far as Elections ACT is concerned, Digital Elections will be the prime In the future.
		2.8.1.1.	their roles in the delivery and maintenance of the service	Currently, SI is prime contractor and SICT is subcontracted for specific development. SI is responsible for delivering the service. There is no official maintenance contract, but there is an agreement to review and upgrade system components as and if necessary for each election.
		2.8.1.2.	the locations their services are delivered from (with special attention to any overseas supplier, technician, or support function with any access to any infrastructure, software, or services containing ACT Government information)	SI office. The service is delivered in the form of a bootable USB that contains all relevant software (including cutdown Linux OS) which can only be setup and used with dedicated hardware (ES, PPSs and VCs).
		2.8.1.3.	the location of their head office	97 Bankers Road, Bywong, NSW 2621.
		2.8.2.	How will the ACT Government be consulted if these third parties change?	As in the past, Elections ACT will be fully informed of any changes that occur with SI (and in the future, DE). Elections ACT have previously stated their concerns regarding ongoing support and availability of the capabilities SI (DE) offers. In fact DE was set up in answer to those concerns.
2.9.	Technology Stack	2.9.1.	Show the standards, technologies, and platform products used in the delivery and support of the solution. Include version numbers of key technologies including Web Servers, Operating Systems, Database Systems and Middleware. This information may be provided through another medium such as design documentation.	We base most of our development on a combination of the Software Engineering Body of Knowledge (SEBoK 3.0 / SWEBok-IEEE) and also the relevant IEEE Standards for Software Engineering which (together) provide description of all the various phases of development. We are well-versed in requirements elicitation, analysis and specification, as well as the modelling of requirements and subsequent design and architecture. Also, we are well-versed in structured and object-oriented development as well as web system development including in the cloud, and relational database development. Wherever possible we use open source products including CentOS Linux 7, Java 11, Ada 2012, VirtualBox 7, PostGreSQL 10-15, VeraCrypt for eVACS®.

2.10.	Secure Coding and Penetration Testing	2.10.1.	To what standards is the service coded, reviewed and tested?	Schedule 2.2(a)(xi)
		2.10.2.	Does the provider engage an independent third party to penetration test the service?	Only in the sense that the system code is openly available to those genuine third parties who wish to undertake independent work to try and show points of system failure.
		2.10.3.	Please provide any penetration test reports you are willing to share.	N/A.
		2.10.4.	Does the provider allow ACT Government to perform its own vulnerability assessment of the service?	Absolutely, yes! See 2.11.1.3 for more information.
2.11.	Patch / Change / Vulnerability Policies	2.11.1.	Provide a link to or copy of your:	
		2.11.1.1.	Patch management policy:	N/A
		2.11.1.2.	Change management policy:	eVACS® is not a large system. Infrequent change requests typically originate from Elections ACT during (preliminary) UAT. Small changes are dealt with immediately and the system is updated using 'git' to record changes. The update is sent to Elections ACT to verify the change has been done to satisfy their (detailed) requirements.
		2.11.1.3.	Vulnerability management policy:	We regard the act of identifying system vulnerabilities as a very important activity in order to ensure that discovered vulnerabilities are dealt with appropriately as part of the system structure and behaviour. SI has adapted a safety-critical system technique named HAZOPS (HAZard OPerarability Study) to identify, analyse and determine ways to mitigate system security vulnerabilities. Elections ACT has the necessary documentation to explain the HAZOPS technique applied to eVACS® and also (now) knows how to use the technique effectively. The technique has also been used for a separate, internet-based Overseas Electronic Voting system.
		2.11.2.	If any of the above are unavailable, provide descriptions of your relevant processes, or equivalent documents:	Permission to provide particular, or full, information on the HAZOPS for eVACS® must be gained from Elections ACT.

	2.11.3.	Do you have automated tools for:	
	2.11.3.1.	Patch management?	No.
	2.11.3.2.	Vulnerability management?	No.

Section 3. General Questions for Cloud Service Providers

The following questions are for Cloud Service Providers and request cloud-specific information about your business, information ownership, privacy etc. If you are not delivering a cloud service to ACT Government you do not need to answer these questions.

Subsection		Question		Response
3.1.	Information Ownership	3.1.1.	Does the ACT Government retain legal ownership of the information, or does it belong to you as the service provider?	
		3.1.2.	Do you intend to use this information for research, marketing or other purposes?	
		3.1.3.	How will the ACT Government be consulted if our data is to be shared with third parties beyond the provider?	
		3.1.4.	Will it be considered an asset for sale by liquidators if your organisation declares bankruptcy?	
		3.1.5.	Please provide a link to or copy of your Terms of Service (if available):	
3.2.	Information Transfer	3.2.1.	What are the procedures, policies, costs and/or penalties that apply should the ACT Government request migration to a different provider or to our own hosting platform?	
3.3.	Information Sovereignty	3.3.1.	List the legal jurisdictions and/or countries other than Australia that ACT Government information will be:	
		3.3.1.1.	Stored in:	
		3.3.1.2.	Processed in:	
		3.3.1.3.	Transmitted to:	
		3.3.1.4.	Transmitted through:	
		3.3.2.	Is the ACT Government allowed to specify the locations where our information can and cannot be stored, processed, and/or transmitted?	
		3.3.3.	Under what circumstances will ACT Government information be shared with external entities (e.g., governments, law enforcement and regulatory agencies, etc.)?	
		3.3.4.	How does the provider handle requests for ACT Government information?	
3.4.	Privacy	3.4.1.	Please provide a link to or copy of your Privacy Policy (if available):	
		3.4.2.	Is your Privacy Policy compliant with:	
		3.4.2.1.	The *Information Privacy Act 2014* (ACT) including its Territory Privacy Principles?	
		3.4.2.2.	The *Privacy Act 1988* (Commonwealth)?	
3.5.	Storage Sanitisation	3.5.1.	On termination of services, equipment failure, or equipment disposal, how will you sanitise physical devices used to store ACT Government information?	
		3.5.2.	Is storage and backup media destroyed when faulty or end-of-life?	

		3.5.2.1.	What destruction methods are used?	
3.6.	Security Incident Detection and Response	3.6.1.	Provide a link to or copy of your security incident response plan (or equivalent):	
		3.6.1.1.	If unavailable, describe your methodology, processes, plans and/or procedures to detect and respond to security incidents.	
		3.6.2.	In the event of a security incident will you supply ACT Government with information to conduct a forensic audit?	
		3.6.3.	Describe the incident response and resolution timeframes for the solution:	
3.7.	Backup and Disaster Recovery	3.7.1.	Provide a link to or copy of your disaster recovery and backup strategy:	
		3.7.1.1.	If unavailable describe your backup strategy and outline the disaster recovery approach for a major incident, for example loss of a data centre.	
3.8.	Support	3.8.1.	Provide a link to or copy of your support policy:	
		3.8.2.	Provide any details about available support not provided in responses to previous questions:	
3.9.	Additional Information	3.9.1.	Provide any additional information you would like us to know about the security and management of your organisation and/or solution:	

Section 4. Cloud Solution Specific Questions

The following questions are for Cloud Service Providers and ask about the cloud service you are providing to ACT Government. Please answer these questions in the context of this cloud service.

Subsection		Question		Response
4.1.	Infrastructure Sharing Overview	4.1.1.	List any of the service's physical or virtual infrastructure that is shared with any other customers: *Examples include network, security, storage, compute, support resources etc.*	
		4.1.2.	List methods used to segregate ACT Government information from other tenants:	
4.2.	Data Centres	4.2.1.	Describe the data centres housing any systems, solutions, or infrastructure containing ACT Government information:	
		4.2.2.	Provide any relevant certifications from the certifying authority, or link to where certification of data centres can be verified:	
		4.2.3.	List any audits of the data centres conducted by reputable third parties that can be shared with ACT Government:	
4.3.	Service Availability	4.3.1.	Describe the service's:	
		4.3.1.1.	Targeted service availability ("uptime guarantee") including how this is achieved:	
		4.3.1.2.	Recovery Time Objective:	
		4.3.1.3.	Recovery Point Objective(s):	
		4.3.1.4.	Schedule of planned outages (if any):	
		4.3.2.	Describe any relevant business continuity methods used to maintain the service:	