

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records Management				
1	Records Mgmt	Ability to system support flexible records retention		
2	Records Mgmt	Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
3	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
4	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
5	Records Mgmt	Ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
6	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
7	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
8	Records Mgmt	Ability to support shared folders - e.g. enable permission for individuals to see other users' folders.		
9	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
10	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
11	Records Mgmt	External audit capability		
12	Records Mgmt	Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
		Availability of post box inventory, delivery and notification on-line controls		
E-MAIL				
1	E-mail	Basic e-mail functionality, including but not limited to send, receive, format, and attachment -	forward, bcc, resend, retract, delete, use of aliases, alert flags	
2	E-mail	Ability to create user defined e-mail groups or personal folders based on search criteria	Does the group expand and collapse when clicked on it	
3	E-mail	Ability to define rules for e-mail handling (incl category for junk email)	Describe the main rule handling capabilities -	
4	E-mail	Ability to add both personal signatures and notes	This should allow for images and multiple signatures	
5	E-mail	Ability to push contact lists and web links to mobile devices		
6	E-mail	Ability to retain e-mail (List per-user limit, if any)		
7	E-mail	Ability to copy, move, and store information to desktop or local storage	Copy between applications - does it retain formatting? Can items be dragged and dropped?	
8	E-mail	Ability to print stored information locally		
9	E-mail	Ability to scan or fax from multifunction devices to an e-mail address		
10	E-mail	and ability to access third party applications and address bookSMTP access		
11	E-mail	Allow remote printing to a Agency facility		
12	E-mail	Ability to send, assign and delegate tasks	Is there an offline mode of operation - how does one use it offline; is a connection to the internet mandatory; if not how does information get sync'd	
13	E-mail	Ability to utilize e-mail system remotely		
14	E-mail	Ability to delegate e-mail functionality to another staff member (i.e., proxy assignments, including mail/phone, appointments, reminder notes, tasks, etc.)		
15	E-mail	Ability to define proxy access limitations (e.g., Read/Write; Subscribe to Alarms and Appointments, Modify Options, Rules, and Folders)		
16	E-mail	Ability to retract and/or retrieve within Agency e-mail system	Can e-mail be deleted, retracted/recalled, How are retention rules handled for deletion	
17	E-mail	Ability to mark outgoing message for delivery verification		
18	E-mail	Ability to mark outgoing message for read receipt/verification	List all commands and functionalities - or provide any documentation available on this subject	
19	E-mail	Ability to script E-mail functions		
20	E-Mail	Ability to access E-mail via Single Sign On platform (including standards based LDAP)		
21	E-Mail	Ability to retract, delete from all mailboxes, resend email		
22	E-Mail	Ability to recover sessions lost due to connectivity issues or session time outs		
23	E-Mail	Ability to mark email as unread	List all flags that are available	
24	E-Mail	Capacity of X users for each shared resource	shared mailbox	
25	E-Mail	Capacity for attachment size of X mb and number of attachments of X	Describe configurability, say, at agency level	
26	E-Mail	Does the solution allow Server-based mail queuing?	No. of tries for sending an e-mail; can this be configured at Agency, group level and/or individual level	
27	E-Mail	Specify attachment file size limitations	e-mail body size limitations, are there any file types that cannot be sent; is that configurable?	
28	E-Mail	Does the solution preserve file format?	Will tables, graphs, images look distorted?	
29	E-Mail	Ability to insert appointments/ new email(s) on arrival on their screen without having the user to refresh/check the browser window every time		
30	E-Mail	Ability to recover screen shots / images directly from clipboard feature		
31	E-Mail	Ability to recover deleted emails	Describe how rules can be setup for this activity	
32	E-Mail	Can solution provide "Blast-Mail" capability?	Does it have an integrated listserv capability e.g. pager to the mail system and from there send it to a set of users	
33	E-Mail	Allow setup of "Out of Office" Assistance/message response		
34	E-Mail	Ability to create dynamic Rules and Alerts based on email attributes	Example of attributes are key words in the subject line, sender, content etc.	
35	E-Mail	Ability to search for email based on multiple specific criteria	Describe rule based searches available in the application	
36	E-Mail	Ability to specify granular permissions by user and role	Example: Some users can only view messages	
37	E-Mail	Backout/Migrate from one SaaS environment to another or to a non SaaS environment	Has anybody done it? Why?	
38	E-Mail	Ability to incorporate digital signature as part of the e-mail		
39	E-Mail	Ability to have offline clients		
40	E-Mail	Delay delivery of e-mail - or send e-mails at set time		
		Is the solution Browser agnostic; impact on version enhancements and backward compatibility;	Example: compatibility with IE 6, Firefox etc.	

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records Management				
1	Records Mgmt	Ability to system support flexible records retention Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
2	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
3	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
4	Records Mgmt	ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
5	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
6	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
7	Records Mgmt	Ability to support shared folders – e.g. enable permission for individuals to see other users' folders.		
8	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
9	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
10	Records Mgmt	External audit capability Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
11	Records Mgmt	Availability of post box inventory, delivery and notification on-line controls		
12	Records Mgmt			
41	E-Mail	Allow communication with external e-mail systems - whitelisting, blacklisting, shared contact list, shared calendar costs for distribution lists and other mailboxes not directly tied to an individual are counted as "users" for pricing purposes.		
42	E-Mail	Describe how time stamp is managed in terms of time zones and daylight savings time		
43	E-Mail	Ability to support Unified Messaging		
44	E-Mail	How is Unified Messaging integrated with Blackberry or similar smart devices		
45	E-Mail	Is Unified Messaging supported when connected remotely		
46	E-Mail			
CONTACT MANAGEMENT				
		including but not limited to last name, first name, middle initial, department, title, business address, contact log, notes, ph. nos (desk, mobile 1, mobile 2, home, emergency contact no., admin assistant)		
1	Contact Mgmt	Ability to synchronize contact information with desktop applications	Specify e-mail systems that your outputs/exports are compatible with	
2	Contact Mgmt	Ability to synchronize contact information with industry standard mobile devices		
3	Contact Mgmt	Ability to share contact lists - permissions for others to view / edit the contacts		
4	Contact Mgmt	Ability to export and import contacts in formats compatible with other email systems		
5	Contact Mgmt	Ability to sync contacts with multiple external e-mail systems		
6	Contact Mgmt	Ability to attach your contact information (like v card) to outgoing emails		
7	Contact Mgmt	Ability to have and manage multiple address books and ability to copy and paste from one to another		
8	Contact Mgmt	Supports Distribution Lists per individual and in Global/System-wide Address List		
9	Contact Mgmt	Ability to Sync with Active Directory/LDAP		
10	Contact Mgmt	Ability to export to print-ready format		
11	Contact Mgmt		Some new contacts may be added to the list; however, it may not be necessary to add all new contacts. Does the tool allow the user to choose which ones to add and which ones not to?	
12	Contact Mgmt	Ability to categorize contacts and automate additions to list form)		
13	Contact Mgmt			
CALENDAR				
1	Calendar	Basic calendaring functionality, including appointment, event, and sharing		
2	Calendar	Ability to view multiple calendars at the same time (both personal and global)		
3	Calendar	Ability to schedule resources, including but not limited to facilities, conference rooms, and equipment		
4	Calendar	Ability to manage resources by proxy (e.g. delegate calendar management, set "view-only" or "edit" rights) to another staff member		
5	Calendar	Ability to print calendars locally in standard formats (such as daily, weekly, monthly, Franklin format)		
6	Calendar	Ability to view/schedule from "free-busy" information with primary and external (third party) calendaring systems	Can the user accept a request from a third party system	
7	Calendar	Ability to view or hide appointment details appts across multiple days including periodicity and configurable date selections - how is this functionality integrated with third party systems and which third parties are supported		
8	Calendar	Ability to create, delegate and track task start, status and end dates		
9	Calendar		Specify if the rules for reminders can be configured at Agency, group, individual level	
10	Calendar	Ability to create customizable appointment reminders	Example: Some user should only view the calendar	
11	Calendar	Ability to specify granular permissions by user and role	Specify search and filter capabilities	
12	Calendar	Ability to search/filter calendar items/appointments		
13	Calendar	Ability to delete only future recurring appointments without affecting past occurrences		

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records Management				
1	Records Mgmt	Ability to system support flexible records retention		
2	Records Mgmt	Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
3	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
4	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
5	Records Mgmt	ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
6	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
7	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
8	Records Mgmt	Ability to support shared folders – e.g. enable permission for individuals to see other users' folders.		
9	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
10	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
11	Records Mgmt	External audit capability		
12	Records Mgmt	Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
14	Calendar	Availability of post box inventory, delivery and notification on-line controls		
14	Calendar	invitations		
E-DISCOVERY				
1	e-Discovery	Ability to search emails and attachments (live or archived) based on the following criteria:		
2	e-Discovery	Content		
3	e-Discovery	Sender and/or recipient		
4	e-Discovery	Date range		
5	e-Discovery	Metadata		
6	e-Discovery	Ability to store search results with any metadata	What metadata is available in general with regards to e-mail	
7	e-Discovery	Ability to add and delete from search results to create an e-Discovery set	In litigation situations, how does the vendor propose to hold, preserve, store and log such actions of email, attachments and metadata for an indefinite period of time?	
8	e-Discovery	Ability to export results in usable format (i.e. PDF, etc...)		
9	e-Discovery	Will SaaS data be more accessible for e-discovery by external 3rd parties?		
ARCHIVE AND BACK-UP				
1	Archive & backup	Ability to store and retrieve all live e-mail data for a minimum of 180 days: 90 days available to the user and 90 additional days available to System Administrators before data is automatically processed for long-term archive		
2	Archive & backup	Ability to archive data based on content, sender, recipient, and/or other metadata with different archival periods per Agency policy or legal requirements		
3	Archive & backup	Ability to retrieve or e-Discover archived data based on content, sender, recipient, and/or other metadata with different archival periods		
4	Archive & backup	Ability to view and perform all normal e-mail functions on archive by an e-mail administrator without having to restore		
5	Archive & backup	Ability to restore archived e-mail data to "live" status		
SECURITY				
1	Security	Ability to Encrypt end-to-end (in motion, at rest on disk and back up media, from email gateway to/from external email recipients)	Does vendor provide for encryption of e-mail designated by customer as confidential, sensitive or other protected information (message content and attachments, end-to-end transport, storage and back-up)? Does encryption application provide secured access to encrypted email content and attachments to a non-certificate end user/recipient of the email? Is there an authentication process for a non-certificate recipient? Does the vendor provide a secure portal for non-certificate users to communicate in an encrypted manner with the State (e.g. individual identifiable inquiries regarding sensitive or confidential issues with a state agency such as behavioral health, communicable disease, health care, unemployment services, vital records, etc)?	
2	Security	Ability to mark and control distribution of all communications and documents as Private, Sensitive and Confidential.	Does the solution turn on encryption for e-mail (transport, storage and back-up) and confidential documentation based on user request?	
3	Security	Availability of Isolated/dedicated data stores available?	classification/ categorization capabilities: If we move forward with this model, how is historical data going to be handled and how is future classification going to be handled; this pertains to compliance.	
4	Security	Availability of option to store data in-house at the state datacenters instead of the cloud	Can such classification be triggered by rules/configuration? management, supervisory at the agency level, customer data: does this make sense in the context of the cloud; concept of private cloud at state / agency level; what is the risk of cross contamination. What is the cost premium for isolation, if available? Will data be comingled with other agencies / customers?	

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records	Management			
1	Records Mgmt	Ability to system support flexible records retention Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
2	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
3	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
4	Records Mgmt	Ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
5	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
6	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
7	Records Mgmt	Ability to support shared folders - e.g. enable permission for individuals to see other users' folders.		
8	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
9	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
10	Records Mgmt	External audit capability Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
11	Records Mgmt	Availability of post box inventory, delivery and notification on-line controls		
12	Records Mgmt	Ability to ensure that the data on mobile devices (ex: BlackBerry's) is stored safely and more importantly can be wiped/deleted when an employee leaves the state - how is that going to be wiped out of backed up data - and adhere to rules surrounding e-mail when an employee leaves - to be made available by each agency	BES to be taken into test considerations as well, sync through exchange; how is access given to another person when an employee leaves for all his/her e-mails	
5	Security	MIS/Reporting to report compliance, risks and vulnerabilities to SISPO, Agency Executives and Risk Management for breach insurance purposes - What is the process for administering and monitoring this situation	Can the agency do the monitoring through a dashboard and / or be able to delegate that capability; Is it possible report on user access?	
6	Security	Availability of enterprise and local blocking/filtering of SPAM and malware		
7	Security	Availability of an option for multiple pass phrases/questions, 2 factor and biometric authentication		
8	Security	Policies, Standards and Practices and Federal initiatives, e.g HIPPA, NIST, PCI, FIPS, ISO & Generally Acceptable Priv Principles (GAPP). Does the vendor support any other Standards?	Through what portal would users connect to the SaaS solution?	
9	Security	Enterprise and local security and privacy policy management capabilities	Describe how the vendor actually manages security and breach notification	
10	Security	Browser filter controls for enterprise and local management	How is security controlled or addressed for multiple browsers/ Any specific browser version to be used / not used?	
11	Security	Ability to broadcast e-mail from non internet enabled appliance - currently this device would connect to an e-mail server and route the broadcast through that appliance		
12	Security	Do we only store and access non-confidential classified data?	recommendations based on experience with other government agencies	
13	Confidentiality	Ability to put sensitivity label information on data stores		
14	Confidentiality	Highly confidential email stores like Director's email, what is proposed and how to handle sensitive situations? Is it possible to setup trust levels?	Should all information be confidential by default - what does this mean from a user standpoint and administrator standpoint	
15	Security/Confidentiality	Ability to verify that data is destroyed in the cloud after the retention period has expired?		
16	Confidentiality	Some cloud providers mine the metadata for subsequent marketing (who, what, when accessed the data - is there a tracking mechanism). Is it possible to prevent clouding data mining with regular 3rd party verification of compliance? provider.	Describe your policy on data mining on customer/government data. Does the vendor use the data for any form of analysis or marketing?	
17	Confidentiality	Are legal ownership rights altered? Who owns the liability?		
18	Confidentiality	Describe all cost premium levels and features available at each level	Describe the costing model based on our requirements	
19	Confidentiality	Availability of option to store data in-house at the state datacenters and the cloud (hybrid/private options)		
20	Confidentiality	Where will the data be stored and are there any controls over where it is placed	How do you ensure that the State information is preserved and safeguarded if the State discontinues use of the vendor or discontinues use of a cloud solution? What validation and verification (e.g. 3rd party) methods are used by contractor to give proof that at end of contract all data is returned to the State or destroyed as authorized by the State?	
21	Confidentiality	In state transport, storage and disaster recovery capabilities only?		
22	Confidentiality	In USA transport, storage and disaster recovery capabilities only?		
23	Confidentiality	Other countries? - is there a separate Govt. Cloud and how does it work?'		
24	Confidentiality	Confidentiality - Is it possible to specify what data is stored into the cloud? Can any data be prevented from going to the cloud by mistake based on rules of prevention if a dual storage mode is indeed available?		
25	Confidentiality	Ability to have configurable Password timeout and ability to allow role based self-authentication for password re-set.		
26	Confidentiality	Ability to protect personal information from unauthorized access, use, or disclosure.		
27	Privacy			
28	Privacy			

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records	Management			
1	Records Mgmt	Ability to system support flexible records retention		
2	Records Mgmt	Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
3	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
4	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
5	Records Mgmt	Ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
6	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
7	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
8	Records Mgmt	Ability to support shared folders - e.g. enable permission for individuals to see other users' folders.		
9	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
10	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
11	Records Mgmt	External audit capability		
12	Records Mgmt	Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
29	Security/Privacy	Availability of post box inventory, delivery and notification on-line controls		
30	Security/Monitoring	Are any security features configurable based on context and in flight? Example: When data to be collected is classified as highly sensitive, additional security measures such as encrypting while in transit, at rest, or both, may be taken.	Describe the tracking mechanism in place for any e-mail to decipher if it is authentic and the number of changes it went through or tampering	
31	Security/Data Location	Data Lifecycle - What tooling is provided for document lifecycle management?		
32	Security/ sub contracting	Is the location of the data and the provider, being subject to laws where the data resides		
33	Security/ Access Rights	Does vendor subcontract of services to another provider? If so, are these vendors overseas, what services do they provide, and how do you ensure compliance?		
34	Security/ Access Rights	What access is given to the cloud provider's administrators (sensitive data)?		
35	Security/ Access Rights	What protection is available to the gov. agency?		
36	Security/ Access Rights	Can we audit Cloud admin privileges?		
37	Security/ Access Rights	What level of detail in logging can we expect for privileged / all activities?"		
38	Security/ Access Rights	Describe your policy and capabilities relating to federated identity management.		
39	Security/Incident Management	Can the solution be integrated with future Identity Access Management such as Claims Based Identity Management?"		
40	Security/Incident Management	How is security penetration testing done; is it performed by internal and external parties.		
41	Security/Incident Management	What mitigating strategies are used by the cloud provider to prevent breaches?		
42	Security/Incident Management	How does the vendor support the ability to perform investigations	What support will be provided by SaaS provider; what liability will be assumed	
43	Security/Incident Management	Logging and data comingled with multiple cloud customers; how does this work in Govt. cloud, if there is one		
44	Security/Incident Management	Do cloud providers provide adequate logging detail (who logged in, when, from where, what admin actions taken, what was accessed, per recorded/document read records)	Provide clarification on level of granularity available for logging	
45	Security/Incident Management	Ability to have the confidence that both security and privacy are being maintained predicates periodic monitoring, testing and evaluation of services.	How is this addressed? What monitoring can be done by the agency and what is done by the vendor? Describe the communication and process identification between the vendor and agency.	
46	Security/Incident Management	Incident Management - Maintain 24X7 Security Incident Management Team (SIM) to quickly and accurately assess and mitigate computer security incidents and privacy breaches involving Online Services, while communicating relevant information to customers.	Must provide 3rd party compliance verification on privacy and ITS standards including compliance with HIPAA, Health Information Technology standards!	
47	Security/Incident Management	What are the roles/responsibilities related to electronic discovery?	How much support is available from the vendor?	
48	Security/Incident Management	Incident Management - What is our (customer) ability to perform vulnerability management and reporting (self testing penetration - vulnerability testing) or is even allowed?		
49	Security/Operations Management	Governance and auditing and controls		
50	Security/Availability	What anti-spam capabilities are available?		
51	Security/Availability	What Anti-malware capabilities are available?"		
52	Security/Availability	Availability - all cloud providers have experienced outages - how will our business processes be impacted by future outages (and they will happen) ?		
53	Security/Availability	We do not have expectations of what is acceptable quality of service so how can we define Cloud SLA's?	Define your Application(s) performance/response times including SLAs for screen refresh times, login times, backup retrieval times, eDiscovery, outages for comparison	
54	Security/Availability	How long does a total restore take (per terabyte of data)?		
55	Security/Availability	Is testing of retained backups performed?		
56	Security/Availability	What redundancy is needed into the cloud? How do we calculate/manage		

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records	Management			
1	Records Mgmt	Ability to system support flexible records retention		
2	Records Mgmt	Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
3	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
4	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
5	Records Mgmt	Ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
6	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
7	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
8	Records Mgmt	Ability to support shared folders – e.g. enable permission for individuals to see other users' folders.		
9	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
10	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
11	Records Mgmt	External audit capability		
12	Records Mgmt	Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
57	Security/Availability	Availability of post box inventory, delivery and notification on-line controls		
58	Security/Physical Security	Network bandwidth - Provide details on infrastructure requirements to support a SaaS model for Data / e-mail delivery. How do your SLAs relate to this requirement?		
59	Security/Physical Security	Ability to restrict access by applying a lowest privilege policy, so that only essential personnel are authorized to manage customers applications and services.		
60	Security/Physical Security	Standard security protocols regarding identification, access tokens, and logging and surveillance of site entry clearly state what type of authentication is needed. In the case of access to highly sensitive assets, multifactor authentication is required.		
61	Security/Network	Password strength definition - is this controlled by vendor or customer? Also need to know if we can have variable strength (Weak, Fair, Strong, etc.) controls/capabilities in place?	How is this implemented in a SaaS environment?	
62	Security/encryption	is in place for the cloud environment. DNS clusters are continuously monitored for unauthorized software and DNS zone configuration changes as well as for other disruptive service events.	How will this be implemented by a SaaS vendor?	
63	Security/encryption	Assets are classified to determine the strength of security controls to apply. For example, assets classified as confidential is subject to encryption requirements for storage and for internal system and network transfers.	Describe this implementation in the SaaS environment	
64	Security/encryption	throughout development and operational practices: Security by Design, by Default, in Deployment, and in Communications.	Describe how this is implemented in a SaaS environment	
65	Security/Comment	All products meet the SDL cryptographic standards, which list the acceptable and unacceptable cryptographic algorithms. For example, keys longer than 128-bits are required for symmetric encryption. When using asymmetric algorithms, keys of 2,048 bits or longer are required.	Any comments?	
66	Security/Options	The SDL is and continues to be applied to the creation of applications to be hosted on SaaS infrastructure: The SDL process is development methodology agnostic and is fully integrated with the application development lifecycle from design to response, and is not a replacement for software development methodologies such as waterfall or Agile.	Agency incidents VS. vendor incidents - How is reporting and management done? What is time frame for reporting suspected and actual incidents to government agency? Will vendor and subcontractors be compliant with HITECH business associate requirements for breach identification and notification requirements?	
67	Security/Incident	Availability - What are the avenues available for migration to other cloud vendors or for pulling back into a private cloud?		
68	Security/Standards	Incident Management - How can we perform and follow-up on incidents?		
69	Security	validates the company has implemented the internationally recognized information security controls defined in this standard - relevance from the State's perspective to be discussed - which standard is followed and who verifies certification?	Describe your security governance program	
70	Security/Risk management	A Governance Program exists to ensure compliance with relevant standards and regulatory obligations for customers. Internal audit and privacy assessments occur throughout a given year.		
71	Security/Risk management	"A formal Security Risk Management Program is maintained to:		
72	Security/Risk management	Identify threats and vulnerabilities to the environment	How is risk calculated in a SaaS environment for security?	
73	Security/Risk management	Calculate risk C193	How is this going to be reported?	
74	Security/Risk management	Report risks across the SaaS environment	How is this determined in a SaaS environment?	
75	Security/Risk management	Address risks based on impact assessment and the associated business case		
75	Security/Risk management	Test remediation effectiveness and residual risk	How is this tested and how are the results shared?	

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records Management				
1	Records Mgmt	Ability to system support flexible records retention		
2	Records Mgmt	Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
3	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
4	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
5	Records Mgmt	Ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
6	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
7	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
8	Records Mgmt	Ability to support shared folders – e.g. enable permission for individuals to see other users' folders.		
9	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
10	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
11	Records Mgmt	External audit capability		
12	Records Mgmt	Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
		Availability of post box inventory, delivery and notification on-line controls		
76	Security/Risk management	encrypt messages containing confidential personal identifying information as defined by rule. The monitoring feature should also send a message to the individual who failed to encrypt the information and create a risk incident if the person continues to issue emails containing confidential PII without encryption.	Does vendor provide a log of bounce back, autoencrypt messages, and encryption failures by time, date, classification of information nature of confidential information), user ID and IP locations?	
77	Security/Risk management	Ability to notify of encryption failures, privacy breaches, critical infrastructure incidents/failures, data loss, contractual non-compliance, etc.		
78	Security/Governance/Assurance	What controls and metrics will be provided by the SaaS vendor?		
79	Security/Governance/Assurance	What certifications does the SaaS vendor maintain?		
80	Security/Governance/Assurance	What recourses are available if the contract is breached?		
81	Security/Governance/Assurance	What team skills are required to manage a SaaS architecture?		
82	Security/Governance/Assurance	What resources are required to update/upgrade team skills?		
83	Security/Governance/Assurance	Where is the risk management framework that documents security controls and business requirements?	Describe your process and methodology	
84	Security/Governance/Assurance	What 3rd party risks assessments are available on the cloud vendor?	Provide documentation	
85	Security/Governance/Assurance	What are the security policies of the cloud vendor?		
COLLABORATION				
1	Collaboration	Ability to share data and files store within the solution at the same time from different or separate Agency work locations		
2	Collaboration	Ability to collaborate with staff members that are telecommuting or otherwise away from a Agency facility		
3	Collaboration	Availability of a Wiki-type solution for collaboration that allows changes to be tracked by user		
4	Collaboration	Ability to maintain version control (i.e., who, when, what)		
SOLUTION ADMINISTRATION				
1	Administration	Ability, from the Administrative console, to: Fully manage all Agency accounts within the Agency network including but not limited to addition, deletion, manipulation and suspension		
2	Administration	Ability to access any/all email account's contents for investigative and discovery purposes.		
3	Administration	Fully manage SaaS identity and user accounts		
4	Administration	Control SPAM or provide anti-spam		
5	Administration	Control virus or provide anti-virus (including spyware)		
6	Administration	Apply content filter		
7	Administration	Ability to apply policies in managing solutions		
8	Administration	Review restricted e-mail		
9	Administration	View all calendars and appointments		
10	Administration	Print historical, statistical and usage reports locally		
11	Administration	Prioritize e-mail accounts		
12	Administration	Manage attachment size		
13	Administration	Setup mail routing		
14	Administration	Manage multiple separate Global Address Lists (GALs)		
15	Administration	Use "Whitelist", "Blacklist", and aliases		
16	Administration	Ability to manage optional solution as cited in Section II.B below		
17	Administration	Can users archive old emails to their desktops so that the storage costs can be kept down?		
18	Administration	Ability to use all domain names utilized within Agency as e-mail extensions		
19	Administration	Ability to synchronize e-mail identities with identities that are managed in our internal authentication directory		

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records Management				
1	Records Mgmt	Ability to system support flexible records retention		
2	Records Mgmt	Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
3	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
4	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
5	Records Mgmt	ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
6	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
7	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
8	Records Mgmt	Ability to support shared folders - e.g. enable permission for individuals to see other users' folders.		
9	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
10	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
11	Records Mgmt	External audit capability		
12	Records Mgmt	Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
20	Administration	Availability of post box inventory, delivery and notification on-line controls		
21	Administration	Ability to control Blackberry, Treo, iPhone and other such mobile/smart devices, including the ability to synchronize calendar, contacts, tasks, and e-mail (e.g., Blackberry Enterprise Server, etc.)		
22	Administration	Ability to integrate with Internal apps using e-mail - SMTP, IMAP, SOAP, POP3, etc.		
23	Administration	Ability to manage DNS ???		
24	Administration	current proprietary format to proposed solution after implementation		
25	Administration	Extent to which administration can be implemented in a distributed manner to different departments		
26	Administration	exception text string to eliminated the possibility of duplication (only target message bound for an external mail domain).		
27	Administration	Create a rule to block a specific group of e-mail users from sending messages to another set of user, but allow messages to be delivered to another set of users (bi-directional).		
28	Administration	Ability to do a number of tasks* with messages that have text strings contained in the header/subject/body/attachment parts of a message to specific group or user (in some cases using exceptions). *Tasks: Apply classification, Prepend text to a subject, Log an event, Redistribute to another address or group of addresses, Block or bounce a message back with a specific error code...		
29	Administration	Ability to control an outgoing message content to a certain format		
30	Administration	name template (force changes to all SMTP addresses on the fly)		
31	Administration	Ability to disable e-mail threading		
			allow/support wireless calendar, task, and contact transfers from the mailbox to the device or vice versa? Or does it work similar to BlackBerry Internet Service (BIS)? Will the BlackBerry device user be required to have BlackBerry Desktop Manager installed on PC to function? What carrier networks (e.g. Verizon, Sprint, AT&T etc.) is the solution compatible with?	
APPLICATION INTEGRATION / SYSTEM AUTOMATION				
1	Integration	Ability to relay system alerts and other automated email		
2	Integration	Does solution work with Cisco Unified Messenger;		
3	Integration	Explain level of integration		
4	Integration	Complexity of conversion process for existing state e-mail platforms and directories	what kind of data loss should be anticipated?	
5	Integration	API availability for integration with various programming languages; e.g. .NET, java, etc.		
6	Integration	Are event triggers to broadcast and receive e-mail available		
7	Integration	SQL server and Exchange are tightly coupled - how do we accomplish this coupling:		
8	Integration	access to send or receive e-mail using SMTP / IMAP / POP3 protocols		
9	Integration	Directory / LDAP integration services		
10	Integration	Address lookup through apps on multiple devices		
11	Integration	Integrated and anonymous authentication through apps; e.g. internet facing apps which send e-mail notifications that do not need authentication		
12	Integration	Calendar updates through applications		
13	Integration	Active Directory integration with address book and calendar and speed of updates; user provisioning and de-provisioning		
14	Integration	user password changes - synch when there is another application between the user and the e-mail environment; not all users have e-mail		
15	Integration	single sign on integration		
		currently the active directory tables are customizable to add additional user defined fields/attributes for applications to access and co-relate; e.g. EIN no. added to active directory to facilitate fetches of other address information		

IMPORTANT QUESTIONS REGARDING CLOUD COMPUTING FOR GOVERNMENT LEADERSHIP, IT, RM AND VENDORS
 (Taken from the AZ Government Information Technology Agency (GITA) RFI)

Category	Application Area	Level One Description	Level Two Description	RESPONDENT COMMENTS
Records Management				
1	Records Mgmt	Ability to system support flexible records retention Ability to support records retention for required period of time, including destruction when obsolete and permanent preservation? (ARS §41-1347.B) Note, this typically requires the ability to categorize into folders by topic/function.		
2	Records Mgmt	Ability to support for destruction holds; manually and rules based (Federal Rules of Evidence, Arizona Rules of Evidence)		
3	Records Mgmt	Ability to report on destruction of records? ARS 41-1346 (A) (8)		
4	Records Mgmt	ability to export messages and all metadata, whether internal or external to the messages? (Lake v. Phoenix; Armstrong v. Executive Office of the President)		
5	Records Mgmt	Ability to migrate messages to other e-mail systems - Is the export format currently defined and supported in a public document?		
6	Records Mgmt	Ability to export archival messages in a format that can be accepted into the Archives. If a proprietary format, will Archives be given specifications to ingest the records? (ARS 39-101(A))		
7	Records Mgmt	Ability to support shared folders – e.g. enable permission for individuals to see other users' folders.		
8	Records Mgmt	Ability to demonstrate the authenticity and reliability of the records.	What standards and methods are used? How can an agency certify records kept outside its system?	
9	Records Mgmt	Availability of audit features and reporting. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	The ability for state or 3rd party contractors to monitor/audit vendor's compliance with security and privacy terms and conditions. Which standards are used? Should the state have dedicated staff with administrative access to ensure compliance with state requirements?	
10	Records Mgmt	External audit capability Ability to support public records request inventory management capabilities for e-mail and documents that supports compliance with statutes		
11	Records Mgmt	Availability of post box inventory, delivery and notification on-line controls		
12	Records Mgmt	default e-mail client capability - e.g. if an e-mail link is clicked, what e-mail interface opens		
16	Integration			
DISASTER RECOVERY				
1	Disaster Recovery	Within how much time has service been restored when interrupted?	Describe restoration times if it dependent on type of interruption	
2		On-line disaster recovery restoration for e-mail and documents for at least 3 years.		
3		Data loss prevention control via a portal tool that monitors and blocks improper use of PII and confidential information (in-bound and out-bound).		
MISCELLANEOUS				
1	TCO	TCO (setup, ongoing yearly maintenance, storage, administration)		
2	Training	Describe the Admin and End User Training provided		