ADB

Technical Assistance Consultant's Report

Project Number: 47192-001
September 2015

Regional: Consolidated View and Analysis of Survey Responses on e-Government Procurement System (Data Retention, Disaster Recovery, Third Party Audit and Anti-virus Scan)

Prepared by Dr. Ramanathan Somasundaram
India

For the Asian Development Bank

This consultant's report does not necessarily reflect the views of ADB or the Government concerned, and ADB and the Government cannot be held liable for its contents.

Asian Development Bank

DISCLAIMER

The views expressed in this report are those of the author and do not necessarily reflect the views and policies of the Asian Development Bank (ADB) or its Board of Governors or the governments they represent.

ADB does not guarantee the accuracy of the data included in this publication and accepts no responsibility for any consequence of their use.

By making any designation of or reference to a particular territory or geographic area, or by using the term “country” in this document, ADB does not intend to make any judgments as to the legal or other status of any territory or area.

ADB encourages printing or copying information exclusively for personal and non-commercial use with proper acknowledgement of ADB. Users are restricted from reselling, redistributing, or creating derivative works for commercial purposes without the express, written consent of ADB.

This report has been prepared only based on the survey responses. No other primary or secondary research was conducted for better understanding of the responses. Hence, findings reported in this document are accurate to the extent the survey responses are accurate.

This report is prepared as per survey responses submitted by country representatives in 2014. Hence, developments subsequent to that time period are not reflected in this report.

ABOUT THE AUTHOR

Dr. Ramanathan Somasundaram is a Consultant for the Asian Development Bank with more than 10 years of experience in conceptualization, implementation and assessment of e-Government Procurement systems.

ABBREVIATIONS

ADB	–	Asian Development Bank
CWRD	–	Central and West Asia Department
e-GP	–	electronic government procurement
EARD	–	East Asia Department
DC	–	Data Centre
DMC	–	developing member country
DR	–	disaster recovery
ISO	–	International Organization for Standardization
OWASP	–	Open Web Application Security Project
PARD	–	Pacific Department
PMU	–	project management unit
RPO	–	Recovery Point Objective
RTO	–	Recovery Time Objective
SAAS	–	Software As A Service
SARD	–	South Asia Department
SERD	–	Southeast Asia Department
TA	–	technical assistance

NOTE

In this report, "$" refers to US dollars

CONTENTS

FIGURES

I. INTRODUCTION

1. The Asian Development Bank (ADB) commissioned a survey in the second half of 2014 to learn about the current status of e-GP implementation in its Developing Member Countries (DMC). A survey questionnaire was sent out to a total of 40 countries of which 29 responded. This survey is a follow-up to a survey conducted earlier in 2011. The latest survey questionnaire is more close ended and sought detailed information about certain key aspects of e-Government Procurement (e-GP) system implementation experience such as the methodology adopted to ensure secrecy of commercial bids, business model and Disaster Recovery (DR) set-up.

2. The survey questionnaire is comprised of 4 sections viz.:
   - (i) Eco-system readiness
   - (ii) e-GP implementation plan
   - (iii) e-GP implementation experience &
   - (iv) e-GP on Software As A Service (SAAS) model

3. Section C of the questionnaire sought details of up to 3 e-GP installations if a country had more than one installation. India and Nepal have provided details of 3 e-GP installations in their respective countries. Thus, this survey has gathered information about 33 e-GP installations.

4. The survey responses are analysed such that certain key output requirements of the TA are addressed as given below:
   - (i) Comparative view of the different approaches adopted for implementation of e-GP system is provided
   - (ii) Interest of countries in using e-GP system is analyzed
   - (iii) Discussion points on key aspects of e-GP implementation are identified such as business model, 3rd party audit and the use of digital signatures. Public procurement professionals could discuss these issues in an online web forum &
   - (iv) Potential for knowledge exchange amongst the surveyed countries is identified. Public procurement specialists and e-GP specialists could share certain details about their implementation such as a draft of the e-GP legal provisions, system malfunction policy and transition management plan in an online-wiki type of knowledge base. e-GP implementing agencies could re-use the material available in this wiki knowledge base instead of reinventing / recreating this knowledge afresh. This wiki-site would be an excellent knowledge base for e-GP specialists, researchers, students and other interested stakeholders.

5. The analysis and reporting of the survey responses is done subject-wise. The responses pertaining to a subject are analysed to learn about the status quo and view of the respondents. Key findings from this analysis are interpreted where required. Each subject report has the following key sections:
   - (i) Subject(s) explained
   - (ii) Survey data explained
   - (iii) Key findings
   - (iv) Discussion points &
   - (v) Knowledge areas

6. All the subject analyses will be compiled and summarized for preparation of a detailed report on the survey findings.

7. As few of the respondents expressed concern in publicly sharing their responses, only holistic and regional level analyses are done. References to individual countries are avoided as much as possible in the report.

II. SUBJECTS EXPLAINED

8. The countries which already implemented e-GP system were asked to provide information about the following in Section C-9 (Data Retention, Disaster Recovery, Third Party Audit and Anti-Virus Scan) of the questionnaire:

(i) Data retention
(ii) Third party audit of e-GP system
(iii) Disaster Recovery (DR) set-up, Recovery Point Objective (RPO) and Recovery Time Objective (RTO)
(iv) Virus scanning

A. Data Retention

9. Government agencies tend to discontinue maintenance of manual records as adoption of e-GP becomes the norm. Information about procurement transactions will get stored automatically when the transactions are processed online in e-GP system. A copy of the tender documents, bids submitted in response to tenders and bid evaluation details will get automatically recorded in e-GP system. Purchasing officials and suppliers can view and access such transactional data from the e-GP portal from anywhere using the Internet. Besides the data uploaded by users, e-GP system will need to record and maintain detailed audit logs as well.

10. A very large number of documents get uploaded in e-GP system viz.:

(i) Government officials upload file attachments to explain in detail the procurement undertaken &
(ii) Suppliers upload documentary evidences and their proposal details as file attachments.

11. The quantum of data processed in e-GP system tends to grow in size as the volume of procurement processed in e-GP system increases. Certain e-GP systems have TeraBytes of data.

12. The duration for which the procurement data shall be retained varies from one procurement agency to another. Typically, Government agencies require maintenance of procurement data for at least 5 years. As per the Multi-lateral Development Bank guidelines, *"EGP systems and information security shall ensure that secure records are kept of every process, procedure, transmission, receipt, transaction in terms of the content, executing individual and authorizations, time and date. These records shall be kept for at least two years after the closing date of the Loan Agreement and be made available for audit on request."*

13. e-GP systems tend to get transitioned once every 7-8 years or an even lesser period. The data stored in the transitioned out e-GP system has to be duly transitioned into the newly implemented e-GP system. Alternatively, a version of the transitioned out e-GP system will have to be kept operational continuously to read the data processed in that system. It is emphasized here that data herein refers not only to the transactional data but also the audit logs. Procurement agencies have to take due care to ensure that procurement data processed in an e-GP system is available at least until expiry of the data retention period.

14. A decision has to be taken on whether old data has to be stored for online access or if it can be archived in back-up devices. A procedure has to be put in place to retrieve the archived

data from back-up devices. If the data were to be stored for online access for a long period or perennially, the e-GP system has to be duly designed to handle large chunks of data without causing performance issues.

B. Third Party Audit

15. e-GP is a Government to Business (G2B) system, wherein sensitive procurement valued at millions of dollars is transacted. It is important that such a mission critical system is kept secured and works reliably. The agencies implementing e-GP system typically take efforts to ensure compliance to well established security guidelines such as ISO 27001 and Open Web Application Security Project (OWASP). An indicative list of subjects covered under ISO 27001 is specified below:

(i) Equipment security
(ii) Information backup
(iii) Controls against malicious code
(iv) Network security
(v) Monitoring set-up such as audit logging
(vi) User access management
(vii) Network access control
(viii) Operating system access control
(ix) Sensitive data exposure &
(x) Missing function level access control

16. A best practice is to hire a 3rd party agency to verify compliance of e-GP system to security guidelines developed in line with International best practices. Such a security audit ideally has to be done once at the outset as pre-requisite for Go-live of e-GP system, which ideally has to be followed by periodic audits conducted at regular intervals. In periodic audit, a 3rd party audit agency will at regular intervals (e.g. bi-annually) verify system security such as verification of server configurations, deployment of latest patches and upgrades and compliance to the latest OWASP guidelines.

17. The Multi-lateral Development Bank’s (MDB) e-Tendering guideline states that the assessed e-GP system shall have *“no outstanding audit issues that represent material risk to the integrity or security of any project”*.

18. A third party audit can also be engaged to test the load handling capabilities of an e-GP system. The load processed in an e-GP system will be less in the pilot phase and will peak with increased adoption of the system. A couple of examples to measure load in e-GP system are listed below:

(i) Concurrent number of users connected to the system
(ii) Concurrent connects to the Application server &
(iii) Capacity of application and database server to handle X number of transactions in an hour

19. The audit agency will be engaged to simulate the envisaged peak load in a test environment. This simulation will seek to verify whether the system has the capacity to handle the envisaged peak load. Some breakages could occur during this simulation, root cause for which will be investigated by the e-GP application service provider and suitable remedial actions taken. Thus, the e-GP software will be optimized to handle the envisaged peak loads.

C. Disaster Recovery

20. e-GP is increasingly being established as a unified platform for a country or a State or a group of government agencies. Further, use of a unified e-GP system is mandated in many countries. An e-GP system used to process all procurement in a country is a mission critical infrastructure. This infrastructure shall function reliably and unexpected shutdown if any shall be limited. Hence, the live production set-up should preferably have a Disaster Recovery set-up with 1:1 replica or at least 50% of the Data Centre (DC) set-up.

21. The Disaster Recovery (DR) set-up shall be kept up to date and fully in sync with the data centre set-up ready for switch over when needed.

22. Two key concepts to note about Disaster Recovery are:

(i) Recovery Point Objective (RPO): It is a measure of the maximum data loss prescribed for a system. A system designed with a RPO of 4 hours will result in a maximum data loss of 4 hours. In other words, data will be backed up every 4 hours. Refer illustration below:

(a) The latest data backup taken on: 03rd of September 2015 at 1600 hours

(b) Time for next scheduled data backup: 03rd of September 2015 at 2000 hours

(c) Unexpected system shutdown: 03rd of September 2015 at 1930 hours

(d) Data loss: 3 hours and 30 minutes

(ii) Recovery Time Objective (RTO): It refers to the time required to restore the latest back-up and resume operations after a disaster has struck (i.e.) presumably from the Disaster Recovery site. A system designed with a RTO of 6 hours can be brought back online within 6 hours of the disaster. Refer illustration below:

(a) Disaster happened on: 03rd of September 2015 at 1600 hours

(b) System brought back online by: 03rd of September 2015 at 2200 hours

23. RPO and RTO should be kept as minimal as possible.

24. e-GP data in some cases are segregated and stored in database and in file system both of which have to be backed up and restored to achieve the targeted RPO and RTO.

25. DC-DR drill has to be conducted on a periodic basis (e.g. once in a quarter) to verify whether:

(i) The data is correctly backed up in the DR site &

(ii) The application deployment in DR is in sync with that of the DC

26. The system owner may decide to completely switch over from the DC to DR site and run the application directly from the DR site for a while. The DR site should be a 1:1 replica of DC if such switch over has to be executed.

D. Anti-virus Scan

27. Both suppliers and government users upload a large number of file attachments in e-GP system. These files are uploaded over the Internet from client machines which are beyond the control of e-GP application service provider. Some client machines may have installed up-to-date Anti-virus software and many others might not have installed Anti-virus software.
The following problems may occur if virus file gets uploaded in e-GP system:

(i) The virus file uploaded by a bidder cannot be downloaded and read by purchasing officials either due to corruption of the file or as the file got quarantined by Anti-virus software installed in the client machine used to open the file

(ii) The virus file affects all other files uploaded in the e-GP server causing damage to the system as a whole

28. The e-GP system should ideally scan uploaded files for virus signatures, reject virus file and inform the party uploading the file about the virus; all of which in real-time. Thus, only virus free files will be uploaded in the system and user will be intimated about the reason for rejection of file. This requirement is defined in MDB's e-Tendering guideline as follows: *Bids/proposals submitted online shall be virus scanned by the Contracting Authority before being uploaded and accepted into the online bid box, and where this causes a bid to be rejected the bidder/consultant shall be notified immediately.*

29. There are certain operational challenges in implementing real time virus scanning of files viz.:

(i) Bid submission is a time bound activity wherein suppliers are required to submit bids within a certain prescribed time. A large number of tenders will close in a certain time of the day (e.g. 1600 hours) or a certain time in the year (e.g. year-end). The load in the system will be at its peak around the bid submission time. Real-time virus scanning will introduce latency especially during peak loads causing performance issues in the e-GP software.

(ii) The definition of virus signatures differs from one Anti-virus solution to another. The Anti-virus solution implemented in e-GP software could wrongly reject an uploaded file as virus whereas a different Anti-virus solution might treat the same file as normal. A bidder which could not submit its bid due to this wrong rejection will complain about the e-GP system.

(iii) The solution for real-time virus scanning of files can be expensive as compared to virus scanning of files subsequent to upload

30. e-GP Application Service Providers (ASP) have implemented certain work around to protect e-GP system from virus attack as given below:

(i) Restrict upload of only certain file types such as .docx, .xls and .pdf

(ii) Disallow upload of executable files such as .exe, .msi, .jar and .bat

(iii) Quarantine a virus file subsequent to uploading of the file &

(iv) Store files in binary format where virus will be rendered inactive. Binary components of a file will be put together on the fly in response to a request by the e-GP application software.

31. In points (iii) and (iv) listed above, the onus will be on the user to upload virus free files.

III. SURVEY DATA ANALYSIS

A. Data Retention

32. A total of 18 responses were received in response to the question on the duration for which data is kept in the production environment. Region wise break-up of the responses is listed below:

(i) South Asia (SARD) – 6 responses
(ii) South East (SERD) – 5 responses
(iii) Pacific (PARD) – Nil response
(iv) Central & West Asia (CWRD) – 6 responses &
(v) East Asia (EARD) – 1 response

33. The survey results show that 72.22% of the 18 respondents retain data in the production system for more than 5 years or forever. About 1/4th of the respondents retain the data for less than 5 years. Refer to the figure below for a pictorial view of the survey responses on the data retention period.

34. All respondents in the SARD region retained data in the production environment for more than 5 years or forever. In SERD & CWRD regions, data retention period is distributed across the board. All the respondents retain data at least for a period of 1 year.

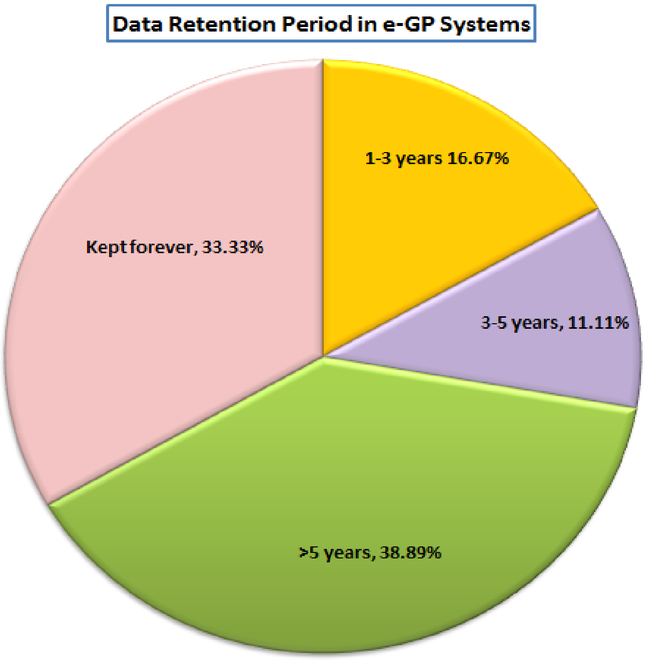


Figure 1: Data retention period in e-GP systems

Duration	CWRD		EARD		SARD		SERD	
	No.	%	No.	%	No.	%	No.	%
1yr	0	0.00%	0	0.00%	0	0.00%	0	0.00%
1-3 yrs	2	33.33%	1	100.00%	0	0.00%	0	0.00%
3-5 yrs	0	0.00%	0	0.00%	0	0.00%	2	40.00%
> 5 yrs	2	33.33%	0	0.00%	4	66.67%	1	20.00%
Kept forever	2	33.33%	0	0.00%	2	33.33%	2	40.00%
TOTAL	6	100.00%	1	100.00%	6	100.00%	5	100.00%

Figure 2: Region wise break-up of responses on data retention period

B. Third Party Audit

35. A total of 17 responses were received in response to the questions on:

(i) Whether e-GP system is subjected to 3rd party audit and

(ii) If audit conducted is:

(a) An one time system acceptance audit or

(b) One time system acceptance audit followed by periodic audits

36. Region wise break-up of the responses is listed below:

(i) SARD – 7 responses

(ii) SERD – 5 responses

(iii) PARD – Nil response

(iv) CWRD – 5 responses &

(v) EARD –Nil response

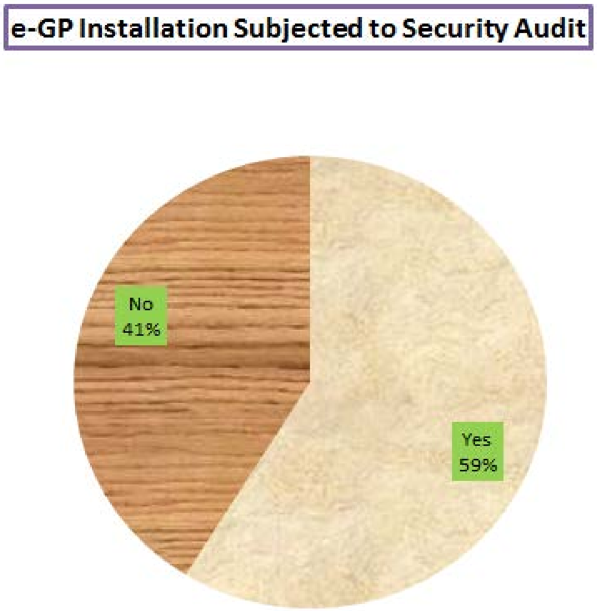


Figure 3: e-GP installation subjected to security audit

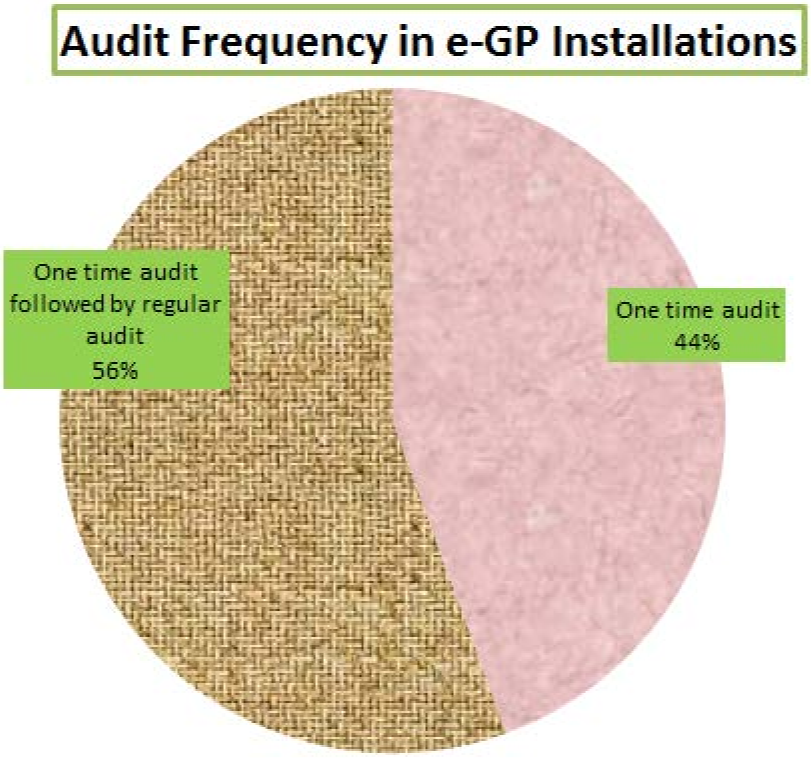
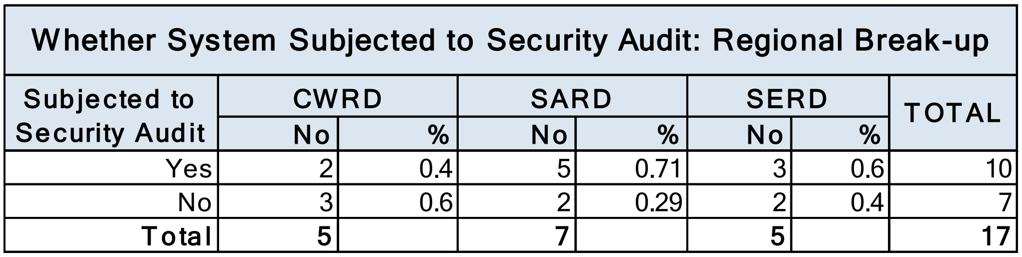


Figure 4: Audit frequency in e-GP installations

37. 10 out of the 17 respondents (i.e. 59%) stated that their system is subjected to security audit. The remaining 41% e-GP systems were not subjected to security audit.

38. Only 9 responses were received to the question on whether one time acceptance audit is followed by periodic audits. Out of the 9 systems subjected to security audit, 4 were subjected to a one-time acceptance audit followed by periodic audits and only acceptance audit was performed in the remaining 5 systems (i.e. 56:44 ratio).

39. SARD region tops the list with 71% of e-GP systems subjected to security audit, followed by SERD at 60% and CWRD at 40%. Refer to the table below:

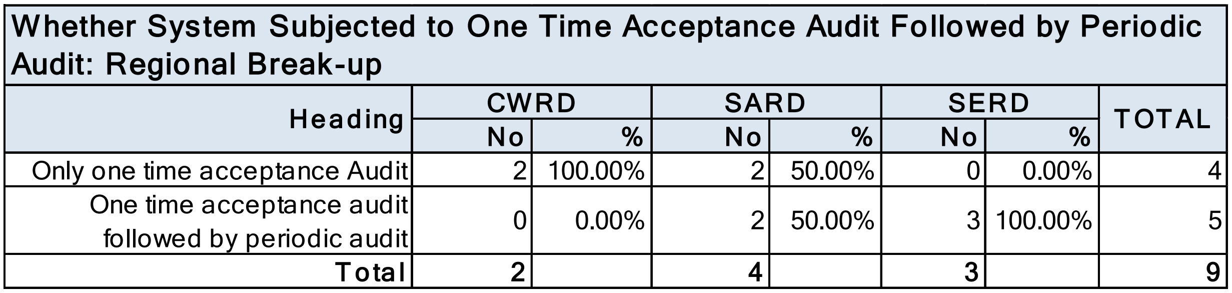


Whether System Subjected to Security Audit: Regional Break-up

Subjected to Security Audit	CWRD		SARD		SERD		TOTAL
	No	%	No	%	No	%	
Yes	2	0.4	5	0.71	3	0.6	10
No	3	0.6	2	0.29	2	0.4	7
Total	**5**		**7**		**5**		**17**

Figure 5: Whether system subjected to security audit (Regional break-up)

40. All the 3 systems from SERD region were subjected to one time acceptance audit followed by periodic audits. The systems in CWRD region are not subjected to periodic audits.

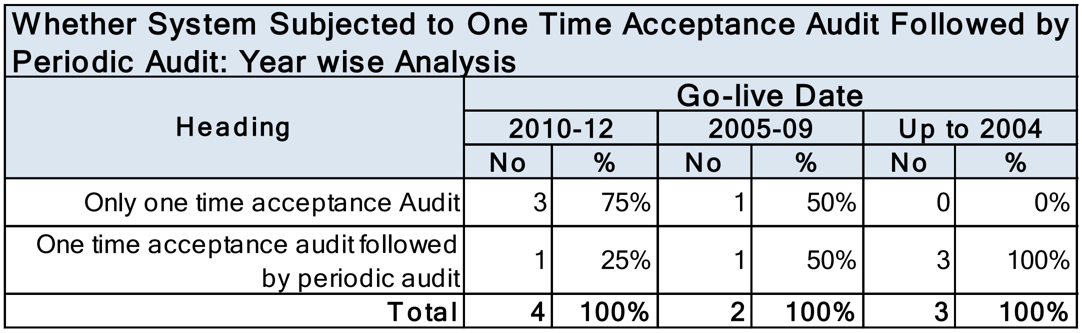


Whether System Subjected to One Time Acceptance Audit Followed by Periodic Audit: Regional Break-up

Heading	CWRD		SARD		SERD		TOTAL
	No	%	No	%	No	%	
Only one time acceptance Audit	2	100.00%	2	50.00%	0	0.00%	4
One time acceptance audit followed by periodic audit	0	0.00%	2	50.00%	3	100.00%	5
Total	**2**		**4**		**3**		**9**

Figure 6: One time acceptance audit followed by periodic audit (Regional break-up)

41. All e-GP systems which went live on or before 2004 have been subjected to a one time audit followed by periodic audits. Only 1/3rd of the systems which went live more recently (i.e. 2010-12) have been subjected to periodic audits. Refer to the table below for details.



Whether System Subjected to One Time Acceptance Audit Followed by Periodic Audit: Year wise Analysis

Heading	Go-live Date					
	2010-12		2005-09		Up to 2004	
	No	%	No	%	No	%
Only one time acceptance Audit	3	75%	1	50%	0	0%
One time acceptance audit followed by periodic audit	1	25%	1	50%	3	100%
Total	**4**	**100%**	**2**	**100%**	**3**	**100%**

Figure 7: One time acceptance audit followed by periodic audit (Year-wise analysis)

C. Disaster Recovery

42. A total of 19 responses were received for the question on whether Disaster Recovery (DR) is set-up for e-GP. Region-wise break-up of the responses is listed below:

(i) SARD – 7 responses
(ii) SERD – 5 responses
(iii) PARD – Nil response
(iv) CWRD – 6 responses &
(v) EARD –1 response

43. Out of the 19 responses received, DR is set-up for 12 e-GP systems (i.e. 63%). All the 6 e-GP systems in CWRD region and 1 e-GP system in EARD region have established DR set-up. SARD ranks the lowest wherein only 2 out of the 7 e-GP systems have established DR.

44. All the 3 e-GP systems established on or before 2004 have established DR. About 3/4th of the systems established recently reported setting up of DR.

45. Refer to the tables below for region-wise and year-wise analysis.

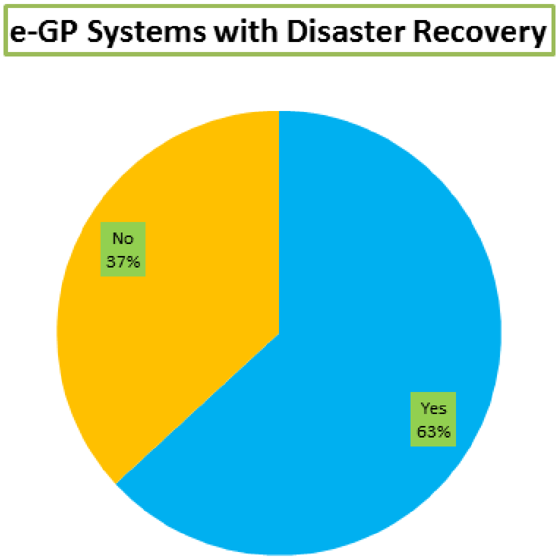


Figure 8: e-GP Systems with Disaster Recovery

Disaster Recovery for e-GP: Region wise Analysis								
Response	CWRD		EARD		SARD		SERD	
	Number	%	Number	%	Number	%	Number	%
Yes	6	100.00%	1	100.00%	2	28.57%	3	60.00%
No	0	0	0	0	5	71.43%	2	40.00%
Total	6	100%	1	100%	7	100%	5	100%

Figure 9: Disaster Recovery for e-GP (Region wise Analysis)

Disaster Recovery for e-GP System: Year wise Analysis								
Response	Go-live Date							
	2010-12		2005-09		Up to 2004		Not Specified	
	Number	%	Number	%	Number	%	Number	%
Yes	7	78%	2	50%	3	100%	0	0%
No	2	22%	2	50%	0	0%	3	100%
Total	9	100%	4	100%	3	100%	3	100%

Figure 10: Disaster Recovery for e-GP System (Year wise Analysis)

46. The question on Recovery Point Objective received 17 responses, region wise break-up of which is given below:

(i) SARD – 6 responses
(ii) SERD – 5 responses
(iii) PARD – Nil response
(iv) CWRD – 5 responses &
(v) EARD – 1 response

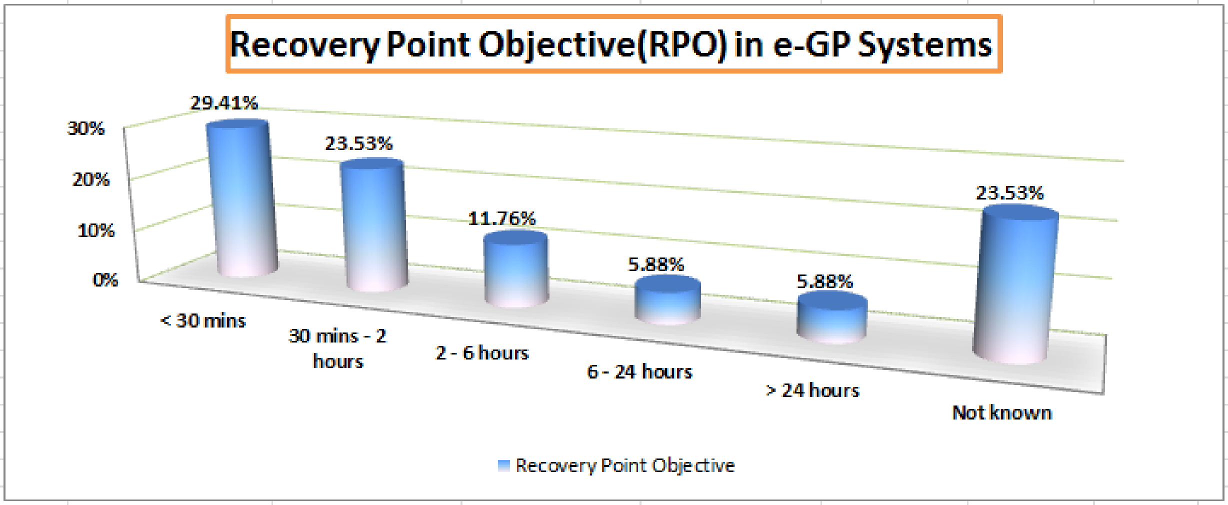
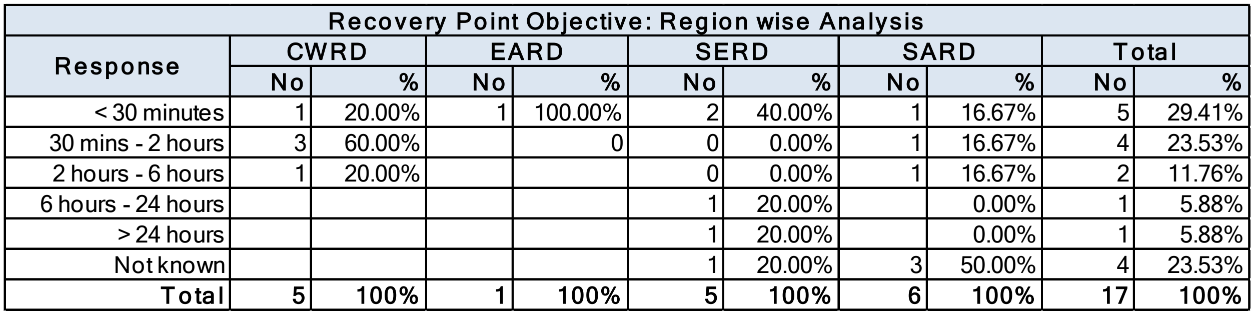


Figure 11: Recovery Point Objective in e-GP systems

47. The respondents were asked to select one of the following RPO:

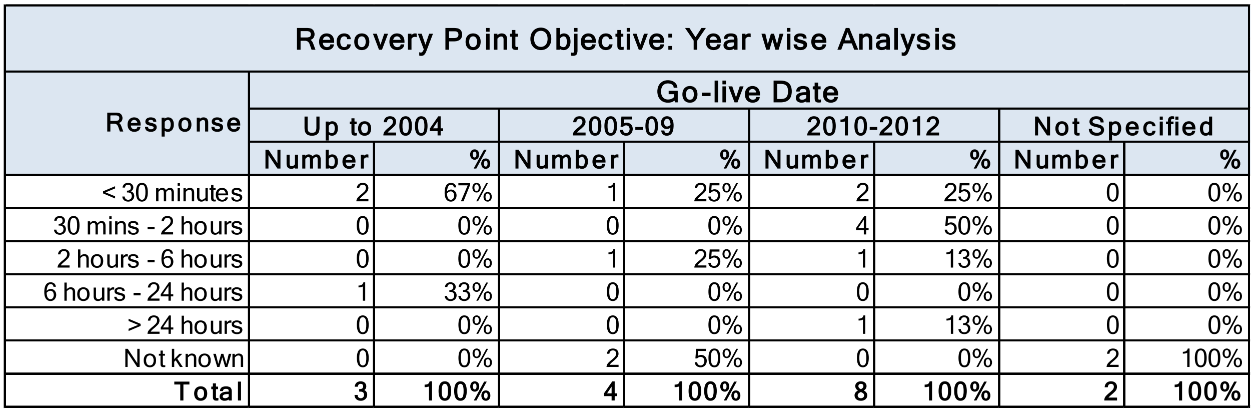
(i) Less than 30 minutes
(ii) 30 minutes – 2 hours
(iii) 2 hours – 6 hours
(iv) 6 hours – 24 hours
(v) More than 24 hours
(vi) Not known

48. The RPO is less than 30 minutes in about 1/3rd of e-GP systems and RPO of 30 minutes – 2 hours is maintained in 23% of e-GP systems. About a quarter of the respondents did not know about RPO. The remaining 1/4th of the responses was spread amongst 2-6 hours, 6-24 hours and more than 24 hours.



Recovery Point Objective: Region wise Analysis										
Response	CWRD		EARD		SERD		SARD		Total	
	No	%	No	%	No	%	No	%	No	%
< 30 minutes	1	20.00%	1	100.00%	2	40.00%	1	16.67%	5	29.41%
30 mins - 2 hours	3	60.00%		0	0	0.00%	1	16.67%	4	23.53%
2 hours - 6 hours	1	20.00%			0	0.00%	1	16.67%	2	11.76%
6 hours - 24 hours					1	20.00%		0.00%	1	5.88%
> 24 hours					1	20.00%		0.00%	1	5.88%
Not known					1	20.00%	3	50.00%	4	23.53%
Total	5	100%	1	100%	5	100%	6	100%	17	100%

Figure 12: Recovery Point Objective (Region wise Analysis)



Recovery Point Objective: Year wise Analysis

Response	Go-live Date							
	Up to 2004		2005-09		2010-2012		Not Specified	
	Number	%	Number	%	Number	%	Number	%
< 30 minutes	2	67%	1	25%	2	25%	0	0%
30 mins - 2 hours	0	0%	0	0%	4	50%	0	0%
2 hours - 6 hours	0	0%	1	25%	1	13%	0	0%
6 hours - 24 hours	1	33%	0	0%	0	0%	0	0%
> 24 hours	0	0%	0	0%	1	13%	0	0%
Not known	0	0%	2	50%	0	0%	2	100%
Total	**3**	**100%**	**4**	**100%**	**8**	**100%**	**2**	**100%**

Figure 13: Recovery Point Objective (Year wise analysis)

49. 4/5th of the e-GP systems in CWRD region maintain RPO of less than 2 hours. The only one e-GP system in EARD maintains RPO of less than 30 minutes. RPO in e-GP systems located in SERD and SARD regions is spread out across the range and not skewed towards RPO of less than 2 hours as in CWRD.

50. The question on Recovery Time Objective (RTO) received 16 responses, region wise break-up of which is given below:

(i) SARD – 6 responses
(ii) SERD – 5 responses
(iii) PARD – Nil response
(iv) CWRD – 4 responses &
(v) EARD – 1 response

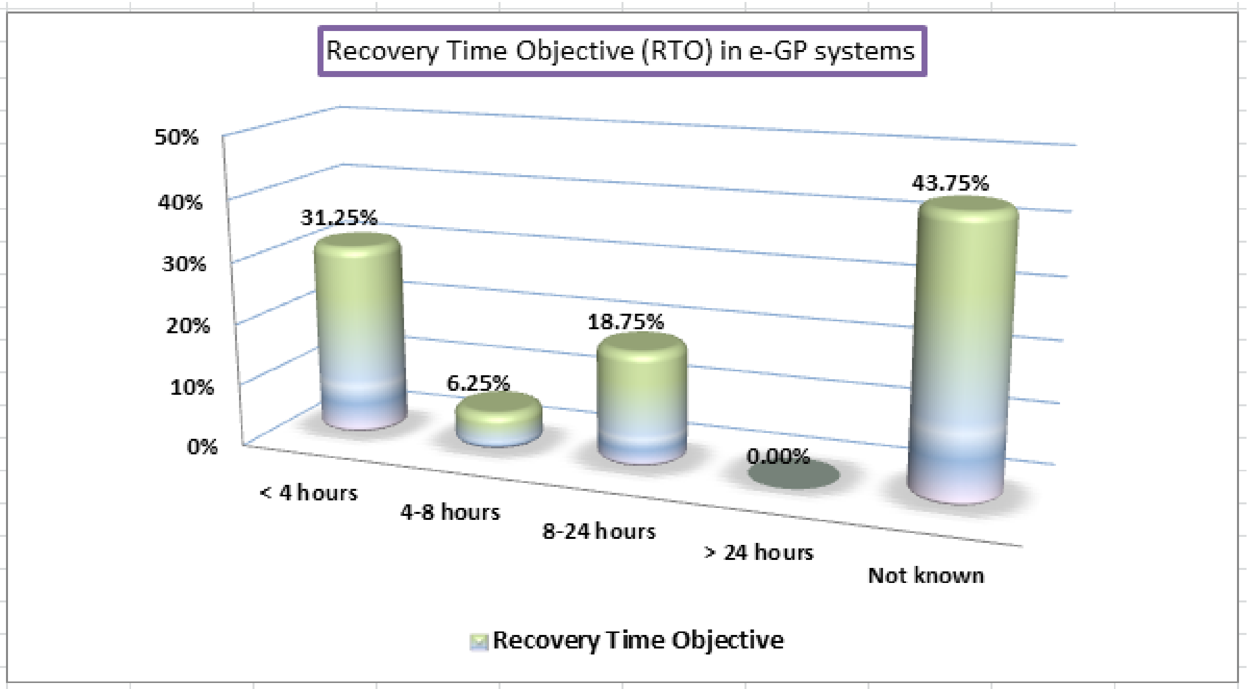
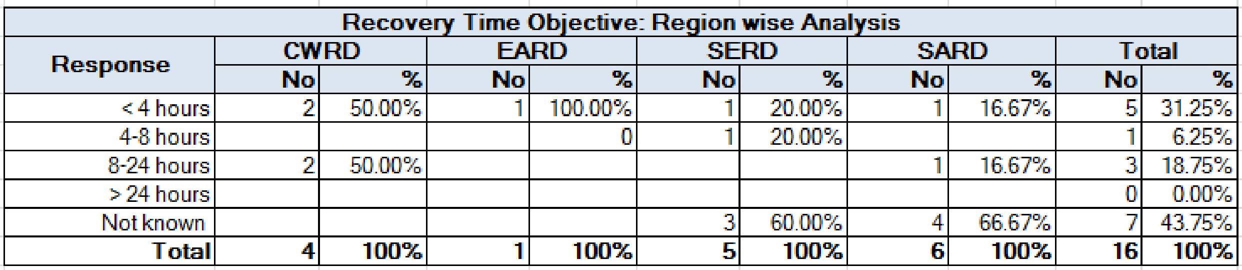


Figure 14: Recovery Time Objective (RTO) in e-GP systems

51. The respondents were asked to select one of the following RTO:
(i) Less than 4 hours
(ii) 4 hours – 8 hours
(iii) 8 hours – 24 hours
(iv) More than 24 hours &
(v) Not known

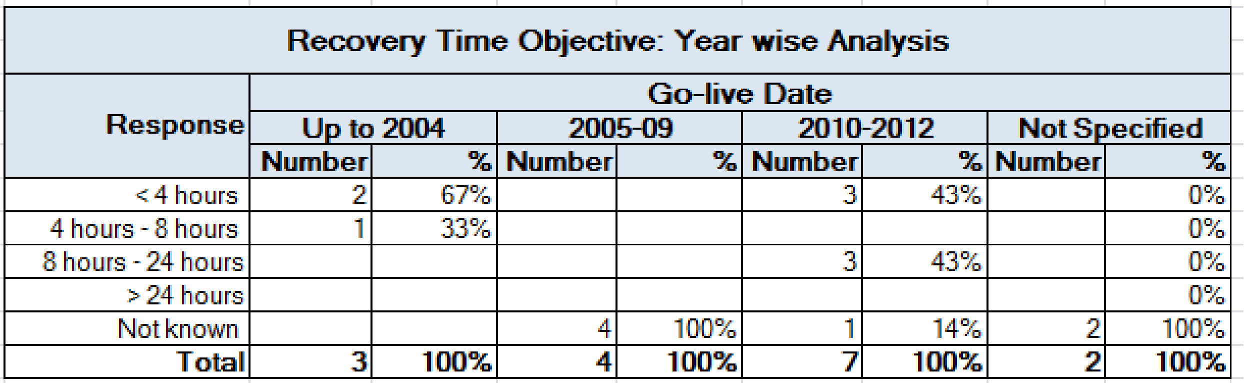
52. RTO of less than 4 hours is maintained in about 1/3rd of the e-GP systems and 7 out of the 16 respondents did not know the RTO.



Recovery Time Objective: Region wise Analysis										
Response	CWRD		EARD		SERD		SARD		Total	
	No	%	No	%	No	%	No	%	No	%
< 4 hours	2	50.00%	1	100.00%	1	20.00%	1	16.67%	5	31.25%
4-8 hours				0	1	20.00%			1	6.25%
8-24 hours	2	50.00%					1	16.67%	3	18.75%
> 24 hours									0	0.00%
Not known					3	60.00%	4	66.67%	7	43.75%
Total	**4**	**100%**	**1**	**100%**	**5**	**100%**	**6**	**100%**	**16**	**100%**

Figure 15: Recovery Time Objective (Region wise Analysis)

53. All the 4 responses from CWRD region claimed RTO of less than 24 hours and the 1 response from EARD has RTO of less than 4 hours. Majority of the respondents from SERD and SARD regions did not know about RTO.



Recovery Time Objective: Year wise Analysis								
Response	Go-live Date							
	Up to 2004		2005-09		2010-2012		Not Specified	
	Number	%	Number	%	Number	%	Number	%
< 4 hours	2	67%			3	43%		0%
4 hours - 8 hours	1	33%						0%
8 hours - 24 hours					3	43%		0%
> 24 hours								0%
Not known			4	100%	1	14%	2	100%
Total	**3**	**100%**	**4**	**100%**	**7**	**100%**	**2**	**100%**

Figure 16: Recovery Time Objective (Year wise Analysis)

54. All the e-GP systems established over a decade have RTO of less than 8 hours. The systems established between 2010 and 2012 have RTO varying from less than 4 hours and between 8 and 24 hours.

55. e-GP systems in CWRD region have taken the initiative to implement DR and kept the RPO and RTO levels in the lower range.

D. Anti-virus Scan

56. The question on Anti-virus scan received 18 responses, region wise break-up of which is given below:

(i) SARD – 6 responses
(ii) SERD – 5 responses
(iii) PARD – Nil response
(iv) CWRD – 6 responses &
(v) EARD – 1 response

57. Anti-virus scan is implemented in 11 out of 18 e-GP systems. There is no discernible region wise difference in the ratio of e-GP systems which implemented Anti-virus scan. Refer to the Table below for regional break-up of the responses.

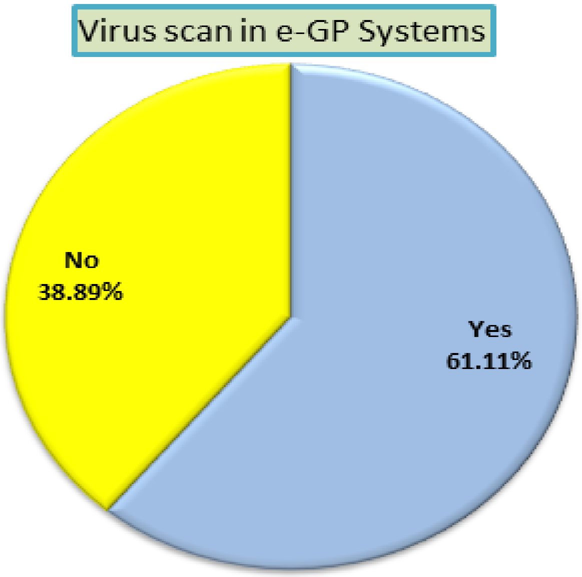
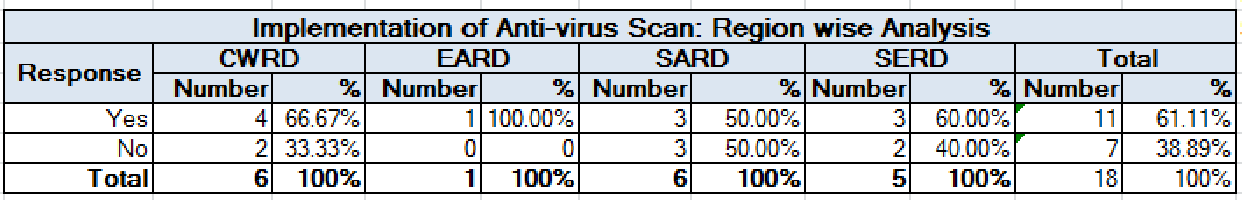


Figure 17: Virus scan in e-GP system



Implementation of Anti-virus Scan: Region wise Analysis										
Response	CWRD		EARD		SARD		SERD		Total	
	Number	%	Number	%	Number	%	Number	%	Number	%
Yes	4	66.67%	1	100.00%	3	50.00%	3	60.00%	11	61.11%
No	2	33.33%	0	0	3	50.00%	2	40.00%	7	38.89%
Total	**6**	**100%**	**1**	**100%**	**6**	**100%**	**5**	**100%**	18	100%

Figure 18: Implementation of Anti-virus Scan (Region-wise Analysis)

E. Key Findings

(i) SARD region tops the list with 71% of e-GP systems subjected to security audit, followed by SERD at 60% and CWRD at 40%
(ii) All e-GP systems which went live on or before 2004 have been subjected to a one time audit followed by periodic audits. Only 1/3rd of the systems which went live more recently (i.e. 2010-12) have been subjected to periodic audits
(iii) All the 6 e-GP systems in CWRD region and 1 e-GP system in EARD region have established DR set-up. SARD ranks the lowest wherein only 2 out of the 7 e-GP systems have established DR.
(iv) All the 3 e-GP systems established on or before 2004 have established DR
(v) The RPO is less than 30 minutes in about 1/3rd of e-GP systems and RPO of 30 minutes – 2 hours is maintained in 23% of e-GP systems. About a quarter of the respondents did not know about RPO
(vi) RTO of less than 4 hours is maintained in about 1/3rd of the e-GP systems and 7 out of the 16 respondents (43.75%) did not know the RTO
(vii) e-GP systems in CWRD region have taken the initiative to implement DR and kept the RPO and RTO levels in the lower range
(viii) Anti-virus scan is implemented in 11 out of 18 (61.11%) e-GP systems

IV. DISCUSSION POINTS

58. The setting up of an online forum is envisaged as a key output under the TA-8520 funding this research. In light of the study findings, the respondents could interact online or face-to-face in a workshop environment the following indicative discussion areas pertaining to Data Retention, Disaster Recovery, 3rd Party Audit and Anti-virus scan are listed herein:

(i) Audit of e-GP systems by a 3rd party is a key requirement to verify compliance and security and integrity requirements. As per the survey, 10 out of the 17 e-GP systems have been subjected to 3rd party audit. However, periodic audit is done only in 4 e-GP systems. In light of the above:

(a) What should be the broad functional scope for 3rd party audit?

(b) When should the one time acceptance audit of e-GP system be conducted? Should it be done as pre-requisite before the first live transaction or as pre-requisite for clearance of pilot stage?

(c) What should be the frequency of periodic audit? For example, can the periodic audit be done once every 6 months?

(d) What should be the broad scope of work for periodic audit?

(ii) A Disaster Recovery (DR) set-up is required for an e-GP system especially when its adoption is mandated by the Government. As per the survey, DR is set-up in 12 out of 19 e-GP systems (i.e. 63%) and all the 3 e-GP systems established on or before 2004 have established DR. In this background:

(a) When should a DR be set-up for e-GP system? Should it be done as pre-requisite before the first live transaction or as pre-requisite for clearance of pilot stage or well into the project stabilization phase?

(b) Should the Government set-up DR as 100% replica of Data Centre or would a DR at 50% capacity be adequate?

(c) How frequently should Data Centre (DC) – Disaster Recovery (DR) drill be conducted? What should be the objective and scope of work for the DC – DR drill?

(iii) About a 1/3rd of the respondents maintained RPO of less than 30 minutes and RTO of less than 4 hours. A similar or even higher percentage of respondents did not know RPO and RTO for their e-GP systems. Given which:

(a) What should be the ideal RPO and RTO for e-GP system?

(b) What would be the best approach to back-up file attachments uploaded in e-GP system (i.e.) especially considering that files loaded into a well-established e-GP system can be in TeraBytes? For example, should the back-up be taken in tapes or should there be disk level replication?

(iv) Anti-virus scan is implemented in 11 out of 18 e–GP systems. It is not known whether files are subjected to virus scan in real-time and what is done to the files found to have virus infected either during the real time scan or subsequent to storing the file. The survey did not enquire whether real-time scanning of files for virus signatures introduces latency in file upload. In this regard:

(a) Experience of e-GP service provider in implementation of virus scanning in real time

i. Whether real-time scanning of files introduced latency in file upload?

ii. Is such scanning implemented to restrict upload of only certain file extensions or disallow upload of file extensions or individually verify files for a large number of virus signatures?

V. AREAS FOR KNOWLEDGE EXCHANGE

59. The development of a wiki-type knowledge base is envisaged under TA-8520. Such knowledge base would be relevant primarily for e-GP practitioners, researchers and academia. The e-GP practitioners could share details about some of the concepts they have already worked out. All members of the e-GP community could study the worked out details and suitably customize them to address their country specific requirements. The ADB under this TA will provide a facility for knowledge sharing amongst e-GP practitioners. This section lists down a set of details which e-GP practitioners could share with the community in relation to Data retention, 3rd party audit of e-GP system, Disaster Recovery (DR) set-up, Recovery Point Objective and Recovery Time Objective & Virus scanning:

(i) Data retention plan and / or data archival policy
(ii) Terms of Reference or a sample Request for Proposal for selection of 3rd party audit agency
(iii) Data backup policy
(iv) Data Centre – Disaster Recovery drill plan &
(v) Virus scanning approach

VI. ANNEXURE

A. List of Respondents

S.no.	Respondent Details	Region
South Asia (SARD)		
1	Nepal - Dolidar	SARD
2	Nepal - Irrigation	SARD
3	Nepal - GEPSON	SARD
4	Bhutan	SARD
5	India - Maharashtra	SARD
6	India - Karnataka	SARD
7	India - Gujarat	SARD
8	Bangladesh	SARD
9	Srilanka	SARD
South East Asia (SERD)		
10	Indonesia	SERD
11	Malaysia	SERD
12	Vietnam	SERD
13	Lao PDR	SERD
14	Thailand	SERD
15	Philippines	SERD
Central & West Asia (CWRD)		
16	Uzbekistan	CWRD
17	Afghanistan	CWRD
18	Kazakhstan	CWRD
19	Georgia	CWRD
20	Kyrgyz Republic	CWRD
21	Tajikistan	CWRD
22	Armenia	CWRD
23	Azerbaijan	CWRD
Pacific (PARD)		
24	Cook Islands	PARD
25	Vanuatu	PARD
26	Tuvalu	PARD
27	Tonga	PARD
28	Samoa	PARD
29	Papua New Guinea	PARD
30	Solomon Islands	PARD
31	Timor Lieste	PARD
32	Fiji	PARD
East Asia (EARD)		
33	Mongolia	EARD

B. List of e-GP Systems with Disaster Recovery (DR) set-up

S.no.	Respondent Details	Go live
South Asia Region (SARD)		
1	India - Karnataka	2007
2	India - Gujarat	2004
South East Asia (SERD)		
3	Malaysia	2000
4	Vietnam	2009
5	Philippines	2000
Central & West Asia (CWRD)		
6	Uzbekistan	2011
7	Kazakhstan	2010
8	Georgia	2010
9	Kyrgyz Republic	2011
10	Tajikistan	2011
11	Armenia	2011
East Asia (EARD)		
12	Mongolia	2012

C. List of e-GP Systems with Recovery Point Objective (RPO) of < 30 minutes

S.no.	Respondent Details	Go live
South Asia Region (SARD)		
1	India – Gujarat	2004
South East Asia (SERD)		
2	Indonesia	2008
3	Philippines	2000
Central & West Asia (CWRD)		
4	Uzbekistan	2011
East Asia (EARD)		
5	Mongolia	2012

D. List of e-GP Systems with Recovery Time Objective (RTO) of < 4 hours

S.no.	Respondent Details	Go live
South Asia Region (SARD)		
1	India – Gujarat	2004
South East Asia (SERD)		
2	Philippines	2000
Central & West Asia (CWRD)		
3	Kyrgyz Republic	2011
4	Armenia	2011
East Asia (EARD)		
5	Mongolia	2012

E. List of e-GP Systems subjected to Anti-virus scan

S.no.	Respondent Details	Go live
South Asia Region (SARD)		
1	Nepal – GEPSON	2007
2	Bhutan	
3	India – Gujarat	2004
South East Asia (SERD)		
4	Indonesia	2008
5	Malaysia	2000
6	Philippines	2000
Central & West Asia (CWRD)		
7	Uzbekistan	2011
8	Kazakhstan	2010
9	Tajikistan	2011
10	Armenia	2011
East Asia (EARD)		
11	Mongolia	2012

F. List of e-GP Systems subjected to 3rd party audit

S.no.	Respondent Details	Go live
South Asia Region (SARD)		
1	Nepal – Irrigation	
2	Nepal – GEPSON	2007
3	India – Maharashtra	2011
4	India – Karnataka	2007
5	India – Gujarat	2004
South East Asia (SERD)		
6	Malaysia	2000
7	Thailand	2010
8	Philippines	2000
Central & West Asia (CWRD)		
9	Uzbekistan	2011
10	Kazakhstan	2010

G. List of e-GP Systems subjected to one time system acceptance audit

S.no.	Respondent Details	Go live
South Asia Region (SARD)		
1	Nepal – GEPSON	2007
2	India – Maharashtra	2011
Central & West Asia (CWRD)		
3	Uzbekistan	2011
4	Kazakhstan	2010

H. List of e-GP Systems subjected to one time acceptance audit followed by regular periodic audits

S.no.	Respondent Details	Go live
South Asia Region (SARD)		
1	India – Karnataka	2007
2	India – Gujarat	2004
South East Asia (SERD)		
3	Malaysia	
4	Thailand	2010
5	Philippines	2000