OFFICE OF THE AUDITOR GENERAL IT AUDIT REPORT 2017/18 PUBLIC PROCUREMENT MONITORING OFFICE (PPMO) ELECTRONIC GOVERNMENT PROCUREMENT (E-GP)

December 2018

Contents

List of Tables

Executive Summary

This IT audit covers the Public Procurement Monitoring Office's software package, Electronic Government Procurement (e-GP). This a bespoke software package to enhance transparency in public procurement. A list of Acronyms used in the report is set out at Appendix 1 : List of Acronyms and a Glossary of Terms is set out at Appendix 2: Glossary.

The IT audit provides limited assurance over controls in the environment. Assurance is limited to commonly accepted key IT controls; this is due to the large number of IT controls in an IT environment, some of which require specialist experience to review e.g. technical configurations of a firewall. The audit covers both the network on which the software resides; its hardware and software and specific application controls over e-GP itself. The audit also provided some review of compliance with Directives issued by the Government of Nepal.

The audit was conducted by reviewing controls built into IT governance, change management, logical access security, physical security and compliance with Directives. A complete list of issues identified is in the action plan timetable at Appendix 3- Action Plan Timetable –e-GP. The most urgent issues are summarized below into strategic, operational and administrative categories; those that we consider to be where management action is required most urgently are highlighted in bold.

Strategic Controls

The nature of the strategic issues we have identified indicate that the Department of Customs Board needs strengthening to improve its oversight of IT and the IT control environment; this will include the Board approving budget to allow the IT Department to be sufficiently resourced. We found that:

- **E-GP functionality is only being used where it is compulsory**; this reduces transparency in the public procurement process and requires management review to establish whether the use of e-GP at all stages of public procurement above the thresholds set needs to be compulsory;

- **third party assurance has been sought by PPMO but recommendations have not been acted on**; Deloitte on behalf of the World Bank produced a high quality review of e-GP, there were significant recommendations; very little has been resolved, it is now almost 6 months after the report has been released;

- **key IT policies had not been drafted or approved**; policies ensure that legal, management and best practice requirements are formalized and available to guide the actions of employees in the business. The Public Procurement Monitoring Office must ensure that key policies are drafted and approved by them to ensure that day to day running of the business does not breach legal requirements and that Board and management requirements are followed;

- **there is no Business Continuity Plan or Disaster Recovery Plan**; these plans are essential to maintain public services in the event of unforeseen disaster and must be tested regularly once designed;

- **that there is no strategic or annual IT plan.** To ensure the Boards strategic objectives for IT are met an IT strategic plan should be set by the Board and delivered operationally by an annual IT plan which includes e-GP; actions should be allocated to a named individual, deadline set and progress should be monitored and reported to the IT Director and periodically the Board; and

- **that there are no Service Level Agreements (SLA's) with third parties or forums to meet third parties regularly;** SLA's and third party forums help senior management to identify and regulate strategic, operational and administrative concerns of users and to communicate PPMO concerns to users.

Operational Controls

The operational issues we identified are most likely to stem from the lack of Board level requirement for third party assurance over the IT environment; this has allowed operational practices to remain without constructive challenge. We found that:

- **there is no anti virus software applied to the Public Procurement Monitoring Office network**; the IT Department told us that this is due to the consideration that the Linux security feature is sufficient. We consider that this is a high-risk strategy and that the Linux security features are not sufficient.

- **that the IT Department is short staffed and key roles filled by outsourced staff**; this is of concern as it raises several risks for the Department including lack of knowledge transfer, loss of key skills within the organization and potentially a lower level of accountability where staff are not internally contracted; this is particularly an issue where there are no staff or where key administrator roles are outsourced;

- **that there are significant issues with internet connectivity**; it is appreciated not all factors causing this will be in managements control the reasons for this should be reviewed;
- there was some evidence of multiple technical and business process flow failings which may indicate wider systemic failings;

- **that there is no e-GP training plan and training has not been delivered** in the latest annual cycle;

- **there was no password policy and password rules not been set**;

- **there was no log in / log out policy** with a 15 minute idle time for log out; automatic log-out depends on user needs, without a policy it is unclear that management have considered whether this is reasonable or not;

- **that there was no firewall policy**, when this is combined with no penetration testing it is a source of significant concern;

- **there is no system to ensure security logs are regularly reviewed** and acted on; and

- **that there was insufficient evidence for the audit team that upgrades or patching to E-GP have been performed as expected.**

Administrative Controls

The missing IT administrative controls indicate that there are insufficient requirements to provide management information regarding IT controls regularly to IT senior management or the Board. We found that:

- **helpdesk calls are not recorded nor is a regular report on matters arising compiled** for management to identify and resolve common themes on a timely basis; this is a key control in an IT environment;

- **that IT asset register information is insufficient to manage IT assets;** this is a particular risk to budgeting for IT and also for aging and replacement of IT assets;

- **warranty information is insufficient to manage warranties**; it can be a major IT risk to allow warranties to run out without renewing them or replacing the assets which the warranty covered; and

- **there were examples of server rooms being unlocked;** weaknesses in physical security; particularly the server room, can lead to significant damage being done to a network,
-

1. Introduction and Scope

1.1 Introduction

This IT audit report has been prepared in order to make an assessment of legitimacy and application status of Electronic Government Procurement (e-GP), being used by Public Procurement Monitoring Office, in the fiscal year 2017/18 (2074/75).

The report is based upon the field work conducted by DFID (PFMA-2) consultants in co-operation with OAG Staffs and observations noted during the fieldwork performed during 2nd Oct, 2018 to 14th October, 2018.

This audit covers information technology machinaries used in the offices operating under Public Procurement Monitoring Office and especially the softwares being used by those offices, which are as follows:

- Public Procurement Monitoring Office
- Police Head Quarter
- Armed Police Force
- Department of Roads
- Department of Irrigation
- Divisional Road Offices - Biratnagar and Nepalgunj

1.2 Audit Scope

For this, it is essential to make study on National Electronic Governance Master Plan and its implementation, andexamine the accuracy, completeness, regularity of information technology software and certification methods being used by entities.This audit report has been prepared to study and analyse on the subject matters pursuant to make an assessment on controls system, credibility of available information and security system.

- Use of technology
- Information and technology infrastructure
- Human resource managemen
- Effectiveness of software
- Secrecy of information system
- Impartiality and integrity of information..

1.3 Audit Objectives

The main purpose of this IT audit is to give assurance on adequacy of software, control mechanism, credibility of information provided and security system by examining the information technology security and control arrangements. While setting above objectives for the purpose of the IT audit, attempts will be made to give assurance on all or some of aspects of the subject matters mentioned below:

- Appropriateness of Used System,
- Reliability of Data,
- Use of Technology,
- IT Infrastructure,
- Human Resource Management,
- Effectiveness of Software,
- Efficiency of Utilize System,
- Confidentiality of Information System,
- Impartiality,
- Compliance
- Integrity

1.4 Electronic Government Procurement (e-GP) System : Public Procurement Monitoring Office has been established on 2007 August 20 (2064/05/03)as an important entity for monitoring whether or not methods or procedures prescribed by the Public Procurement Act, 2007 (2063) and Rules 2007 (2064) have been followed appropriate manner. Public Procurement Monitoring Office has developed single portal based Electronic Government Procurement (e-GP) with an objective to make procurement procedures open, transparent, objective and credible by mitigating unhealthy competition in public procurement procedures. All electronic tender related activities have been conducted through this system by adding features the like-online assessment, contract agreement, contract management, electronic payment in the system and integrating all procurement system in Public Procurement Management Information System (PPMIS) along with systematic, scientific and data security. Section 14(2) of the Public Procurement Act 2007 has made provision for keeping tender notices in the websites of Public Procurement Monitoring Office and concerned entity, and Rule 146 of the Rules has made provision for requiring the operations of procurement activities by registering entities' electronic procurement system in the portal. The scope of this e-system extends from the publication of tender notice to bid evaluation relating to purchase goods and services and publication of notice for letter on intend

1.5 Policy and legal provisions related to actions of Information Technology Environment:

1.5.1 Legal Provision :Electronic Transaction Act 2063, Electronic Transaction Rules 2064, Public Procurement Act 2007 (2063), Public Procurement Rules 2007 (2064), National Electronic Governance Master Plan, Directives relating to Website Construction and Management of Government Entities 2068, Nepal Government Enterprise Architecture (GEA) Infrastructure Architecture, Information and Communication Technology Policy 2074, Information and Communication (Management and Operations) Directives 2071, Fourteenth Three Year Plan (2016/17 - 2018/19) and Budget Speech 2017/18 etc.

1.5.2 Policy Provision : Directives relating to Website Construction and Management of Government Entities 2068, Information and Communication (Management and Operations) Directives 2071, Information and Communication Technology Policy 2072, Electronic

Procurement System Operations Guidelines 2073 (Technical Guidelines), Electronic Procurement System Operation Handbook 2074 etc.

1.6 Audit Methodology

The following procedures will be followed for the execution of this audit:

1.6.1 Information Collection: In course of understanding entities, acknowledgements will be made as regards to entities' activities, software being used, reporting arrangements etc. and information will be collected relating work operations and general financial transactions operations.

1.6.2 Conducting the IT Audit: To carry out audit on the basis of approved audit plan, the audit team will be deputed in audits along with the preparation of audit programmes, necessary tools and check-lists in accordance with the ICT Audit Guide of the office of Auditor General.

1.6.3 Reporting: Preliminary audit report will be provided to the concerned office, Department and Ministry after the completion of this audit. Necessary time will be granted as per law to submit replies to queries mentioned in such audit report provided. Final reports will be issued by considering/incorporating the replies received within specified timeframe. Audit recommendations will be included in such reports as possible. Significant observations of preliminary and final reports will be included in annual report of the Auditor General.

1.6.4 Audit Follow-up: The responsibility of implementing the recommendations provided by the IT audit is of the concerned office, department and ministry. Pursuant to implementation of audit recommendations, necessary follow-up audit will be carried out in the offices where such audits are carried out.

1.6.5Audit Tools: For the purpose of this audit, documents relating to audit of entities and study/ discussion of records and observations and examination of software will be taken as the main audit tool.

1.6.6Audit Methodology: In order to carry out this audit, the reference of declarations made by International Organization of Supreme Audit Institutions (INTOSAI) and Asian Organization of Supreme Audit Institutions (ASOSAI) will be taken. An appropriate audit methodology will be followed by identifying the risk areas after making study on IT environment of the entities to be audited. An assurance will be made by obtaining electronic data from the concerned entities, and information collection andanalysis will be made by making discussion with employees involved in IT, office headsand other officials, and examining IT questionnaires and data.

1.6.7Audit Limitation: This audit may have inherent limitations due to audit scope, sample selection, human errors, lack of technical knowledge, complexity and uncertainity of system, use of professional judgement, lack of time, non- receipt of timely information, non-detection of errors or frauds etc.

2. Summary of Observations:

2.1 Planning and Policy

2.1.1 Governance

i. **Criteria:** Check and review the Governance Arrangements for ICT. We need to confirm that IT management or management with ICT responsibilities are involved at a sufficiently senior level. Meeting minutes should be obtained and any reports to those charged with governance relevant to ICT, review and record significant issues.

ii. Audit Observation: We observed that presently there is no separate ICT steering Committee. The work to be done by steering committee is being done as per the decision of secretary of PPMO. Technical committee has been formed recently. No meeting has been held till date. The committee suggests to make any changes/ updates in the system. Technical committee was constituted on 9th Aswin 2075. Composition consists of : Head of Planning and IT Division- Coordinator; Director-IT Member; Director Planning Member; Director Grievance re-addressal- Member; Director Monitoring (Goods)-Member; Director Monitoring (Works and Consulting) Member; Member Secretary- Computer Engineer; Staffs of related Public Entity to be invited. Committee has been recently formed and no meeting till date has been held. Committee is responsible for defining new business requirements and feature enhancement of E-GP.

Also, no regular meetings are held with the significant third parties to discuss the problems/ issues faced by them in the functioning of E-GP.

iii. Risk: Technical committee may not address all the E-GP related issues. The scope of technical committee is limited to feature enhancement of E-GP. The vulnerability issues in the system and their solutions may remain un discussed and not informed to the related authorities.

iv. Impact: Non availability of separate committee to address all the issues of E-GP may hamper the service capacity of E-GP. Also, the objective of implementation of E-GP will not be achieved if the users are not provided with the regular support.

v. Recommendation: It is recommended to form a ICT steering committee or add on the scope of work of the existing Technical Committee. Regular meetings (monthly) shall be held with the significant third parties to discuss the problems/ issues faced by them in the functioning of E-GP.

vi. Management Response:

2.1.2 Policy

i. **Criteria:** The organization should maintain a number of IT Policies including but not limited to: security policy (including access control); business continuity and disaster recovery; confidentiality of data; third party usage policy; Hardware Policy; Software Policy; Incident Response, Media Destruction and Retention, Back Up, Remote Access, Change; Management, Acceptable Use; ICT Training Policy.

ii. Audit Observation: It has been observed that the policy documents have not been approved by the management. The policies and procedures are not documented in regard to Information Security. The following policies are available in draft phase yet to be approved by the management. PPMO only has its annual budget plan both for hardware and software items.

a. Information Technology Policy
b. Security Policy
c. Business Continuity Plan
d. Disaster Recovery Plan
e. Hardware Policy
f. Software Policy
g. Policy for confidentiality of Data
h. Backup Policy
i. Remote Access Policy
j. Change Management Policy
k. ICT Training Policy
l. Third Party Usage Policy

iii. Risk: Due to non-availability of documented policies and procedures, no governance shall be available for the operation of E-GP. No guidance shall be available if any incident occurs also no single individual shall be liable in absence of clear methodology.

iv. Impact: Non availability of policies, procedures and processes leads to non-achievement of the effectiveness and efficiency of regulatory compliance efforts. It may lead of loss of opportunities to improve business performance.

v. Observation: It is recommended to draft, finalize and approve the following policy documents at the earliest so that a clear picture can be drawn to assign the responsibilities to the concerned personnel.

a. Information Technology Policy
b. Security Policy
c. Business Continuity Plan
d. Disaster Recovery Plan
e. Hardware Policy
f. Software Policy
g. Policy for confidentiality of Data
h. Backup Policy
i. Remote Access Policy

j. Change Management Policy
k. ICT Training Policy
l. Third Party Usage Policy

vi. Management Response:

2.1.3 Strategy

i. Criteria: The client should have an actively managed annual IT plan in place.

ii. Audit Observation: PPMO has a draft 5 year strategic IT plan. It is yet to be approved and implemented.

iii. Risk: A strategic plan acts as a road map and a long term approach to achieve the organizational goals and objectives. Due to non-availability of documented strategic plan and IT plan, the vision of E-GP cannot be clarified.

iv. Impact: E-GP system is expected to act as a one stop portal for various activities of public procurement life cycle including registration of bidders, procurement planning, e-tendering, on-line evaluation, contract management, etc. Lack of annual strategy plan shall lead to failure to make an analysis about whether the objectives of every year has been met or not.

v. Recommendation: It is recommended to prepare a annual strategy plan for E-GP clearing citing out the hardware/ software additions/ up gradations to be made during the year, feature enhancements to be made, trainings/ supports to be given to the users, ways to make the users aware about full utilization of E-GP and its benefits, etc.

vi. Management Response:

2.1.4 Third Party Assurance

i. Criteria: Management should obtain independent certifications, accreditation and assurance (e.g. Internal Audit) that IT processes and operations are maintained and monitored. Procedures should be in place to ensure that any improvement recommendations raised are acted upon.

ii. Audit Observation: It has been observed that PPMO had conducted internal audit of E-GP from DOIT (Department of Information Technology) in the year 2016 and thereafter it has hired third party Deloitte Touche Tohmatsu India LLP ("DTTILLP") through World Bank to conduct to conduct IT audit. The final submission of the report was done on 24th April, 2018. The report also covered penetration tests done by DTTILLP in E-GP. We have obtained the copy of reports from both DOIT and DTTILLP. We have not been provided with the status of recommendation provided both by DOIT and DTTILLP. The recommendations made are in line with the Audit objectives and are directly and specifically related to E-GP. The status report of recommendations made by DTTILLP is as follows:

Table 1: Third Party Assurance Report (April 2018)

S.no	Recommendations Made	Status of Compliance	Remarks
1	It is recommended that e-GP system's IT/Information security Policy covering the following domains should be drafted, finalized, approved and implemented:	Not Complied	Policy is in draft phase
	IS Policy Management		
	Access Control		
	Change and Patch Management		
	Network Security		
	Asset Management		
	Information and Data Classification		
	Incident Management		
	Cryptographic Controls Key Management		
	Physical and Environment Security		
2	It is recommended to document and implement the following: • Process of User revocation/ modification in case of job change/ transfer/ separation. • Automatic disabling the inactive users in e-GP system after a particular period. Eg 12 months	**Partially Complied**	• **Done** • **Not Done**
3	It is recommended to perform the following:	Not Complied	
	Define a process for performing user access review on a periodic basis, at least quarterly and take necessary action, as required.		Not Done
	PE/Bank/Bidder admin's should be asked to validate, whether all the current users are required or not, and access should be revoked, if required by PPMO IT Team.		Not Done
	Access to privileged users like system administrators, super users should be reviewed and approved every quarter by the IT Head		Not Done
4	Upgrade the Network Management Tool (NagiOS) to the latest version i.e. 4.3.4	Not Complied	Not done since a separate monitoring tool Cacti is being used
i.	Define resource utilization threshold for the system availability, memory usage, disk space usage and service metrics.	Not Complied	Not Done
ii.	Configure the NagiOS maps, so team can have a node view of the current host/ service running.	Not Complied	Not Done
iii.	Integrate it with a Ticketing tool to generate automatic escalation e-mail alerts to the PPMO It team.	Not Complied	Not Done
5	It is recommended that PPMO should be outsourcing their IT Operations to a third party, with the onsite model with clear	**Partially Complied**	**Done**

S.no	Recommendations Made	Status of Compliance	Remarks
	assignment of authority and responsibility over e-GP operations and ensuring segregation of duties.		
i.	Further, PPMO should consider developing in-house capability by hiring domain experts for development, database and network and security perspective, who can support and perform governance activities. Above hiring could be contractual/permanent in nature as per the PPMO/Nepal govt. policy.		**Not Specified**
ii.	It is recommended that PPMO should consider hiring a few technical IT resources for providing L1 support as a part of the Helpdesk team.		**Not Done**
6	It is recommended that SLA document which clearly defines and measures for the critical performance parameters for e.g. Service uptime, resolution time, response time, etc. should be available with the PPMO team. In case of absence of such a document, the SLA document should be created for the outsourced party/vendor and regular monitoring (weekly/fortnightly) should be done for the SLA compliance. Additionally, penalty terms must be explicitly mentioned for any type of SLA breach.	**Not Complied**	**There is a contract between PPMO and DG Market but no SLA is there.**
7	It is recommended to: Define and document a formal backup and restoration policy Define a Backup plan/schedule along with frequency and responsibility and implement for all servers and infrastructure related to e-GP system Perform monitoring of backups regularly to ensure that failed backups are identified and backup is re-run Perform Restoration testing on a periodic basis SAN storage should be monitored for the raw storage statistics and report should be shared with the IT Manager/Head on a regular basis	**Not Complied**	**Not Done**
8	It is recommended that the PPMO management should have a formal BCP policy approved and implemented. Contingency plans should be developed for potential threats other than technology failures such as, but not	**Not Complied**	**Not Done**

S.no	Recommendations Made	Status of Compliance	Remarks
	limited to: 1. Natural Calamities 2. External Threats 3. Human Error 4. Non-Compliance 5. Capacity Utilization It is recommended to perform a risk assessment for the mentioned threat scenarios and prepare a contingency plan for each scenario. Such plans should be updated (as and when required) or at least annually to keep them relevant during any incident of business service disruption.		
9	⍰ Assess the potential threats for e-GP environment and develop DR plan for the same, covering the following - Natural Disaster (Fire, Flood etc.), Cyber Attack (DDoS, Brute force attack etc.), Sabotage (Curfew etc.), Internet outage, Power outage , Random failure of critical system ⍰ Document and obtain approval for a plan, response and recovery procedures ⍰ Establish incident response team with necessary responsibility, authority and competence to manage an incident and maintain information security; develop mitigation steps for information security controls that cannot be maintained during an adverse situation.	**Not Complied**	**Establishment of DR is in planning phase.** **Not Done** **Not Done**
10	It is recommended that the IT Operations team should prepare a HA testing schedule which is approved by the PPMO Management and perform testing as per the schedule, ideally frequency should be quarterly.	**Not Complied**	**Not Done**
11	It is recommended to: ⍰ Implement a syslog server ⍰ Analyze security logs (on a regular basis); and analysis reports should be shared with PPMO IT Head, for review ⍰ A real time log monitoring system (e.g. SIEM tool) should be implemented for the real time security incident monitoring and escalation	**Not Complied**	**Not Done**
12	It is recommended to maintain a detailed asset tracker, capturing asset details, ownership, change in ownership etc.	**Not Complied**	**Not Done**

S.no	Recommendations Made	Status of Compliance	Remarks
	Further, the asset register should be reviewed and updated on a regular basis.		
13	It is recommended to effectively manage the licenses to strengthen system security and increase operational efficiency in order to prevent potential litigation costs associated with software misuse / violation of software licenses. Tracking and Managing Software licenses manually (using excel / database file) or via some automated tool like: □ IBM Licence User Management (LUM) □ Microsoft Software Asset Manager (SAM) It is recommended to follow automated approach for greater accuracy and efficiency.	**Not Complied**	**Not Done**
14	It is recommended to create a central repository of all Operations related Policy/Procedure documents, Standard Operating Procedures, working documents like trackers, templates etc.. This would enable the PPMO team when onboarding new employees, contractors, and for knowledge transfer in cases on transition of work to new partners/outsourced partner.	**Not Complied**	**Not Done**
15	It is recommended to perform the following: □ Update the Network Diagram, as and when required and get it approved from the PPMO management □ Diagrams should consist of the following information clearly: o Subnets (VLAN IDs, Names, Network address and subnet mask) o Services o Logical interfaces o Routing protocol information	**Not Complied**	**Not Done**
16	Ensure up-to-date firewall policy, effective anti-virus and anti-malware programs, and intrusion detection systems to alert IT of attempted unauthorized access	**Not Complied**	**Not Done**
17	It is recommended to define, document and implement a process to regularly analyze and review the available logs for any anomalies. Also, deployment of the syslog server can aid in managing the various logs being generated in the e-GP system.	**Not Complied**	**Not Done**
18	It is recommended that the IT team should ensure the following:	**Not Complied**	**Not Done**

S.no	Recommendations Made	Status of Compliance	Remarks
	Define and implement a 'Vulnerability Management' process Take proactive steps to identify and minimize the vulnerabilities in their environment before they got exploited by any malicious attacker Testing and implementation of Security Patches and Updates Further, PPMO should monitor and track the vulnerabilities identified and discuss the solutions and budget at the IT Steering Committee meeting for fixing the gaps in a timely manner.		
19	It is recommended to Define and Implement a Security Incident Event monitoring process Implement a Security incident response mechanism, to primarily develop a well understood and predictable response against destructive events and intrusions. Perform Security Incident Monitoring and define the escalation matrix Analyse security logs real-time and reports should be shared with PPMO A real time log monitoring system (e.g. SIEM tool) should be implemented for the real time security incident monitoring and escalation. As discussed with PPMO, there is a plan to implement SIEM tool in 2018.	**Not Complied**	**Not Done**
20	It is recommended to: Install the antivirus solution over the RHEL servers. e.g. Clam AV Track for the latest signature updates and implement them Files uploaded by the e-GP users should be scanned for virus threats Utilize the gateway antivirus modules available over the Firewall, which is currently available but not being used	**Not Complied**	**Not Done**
21	It is recommended to identify and classify the data assets based on nominal values according to its sensitivity (e.g., impact of applicable laws and regulations). By classifying data, PPMO can identify the risk and impact of an incident based upon what type of data is involved. For example, data might be classified as: public, internal, confidential (or highly confidential), restricted, regulatory,	**Not Complied**	**Not Done**

S.no	Recommendations Made	Status of Compliance	Remarks
	or top secret, as per the best industry practices.		
22	It is recommended to define a risk assessment methodology and perform a risk assessment at least annually, or in case of any major change. Assess information and infrastructure scope Understand Threats and Vulnerabilities in your environment Estimate the impact w.r.t. Integrity, Availability and Confidentiality Determine the Risk for a particular threat/vulnerability in terms of likelihood, magnitude of impact and adequacy of existing security controls to eliminate the risk Prepare a risk register and prioritize the critical risks Outline the possible controls that could mitigate or eliminate the identified risks Present it to the Steering committee for mitigation and risk acceptance approval	**Not Complied**	**Not Done**
23	It is recommended to define and implement an Incident Management Policy, with the roles and responsibilities and response time defined for resolution of customer/user issues. The incident management process should cover the following: Classification of Service Requests and Incidents and their priorities Logging of tickets either manually or using some automated ticketing tool (e.g. CA Service Desk). Tracking the tickets to closure Root cause analysis to be performed for incidents raised It is recommended that PPMO should set up a technical IT Helpdesk for registering customer complaints, and providing resolution to the user issues.	**Partially Complied** **Not Complied** **Partially complied** **Not Complied**	**Policy is not defined but done on need basis** **Not Done** **Not done properly but development and IT Team are doing this** **Not Done**
24	It is recommended to define and implement a formal physical security plan effectively to mitigate security risks in the secure areas. Visitors should not be allowed to carry laptops/pen drives	**Not Complied**	**Not Done**

S.no	Recommendations Made	Status of Compliance	Remarks
	and other inside the data centre. Further, restricted items should be listed and displayed at the entrance of the data centre.		
25	It is recommended to: ⁃ Deploy a CAPTCHA mechanism in the login form ⁃ Deploy OTP based authentication at the login page for two factor authentication	**Not Complied**	**Not Done**
26	It is recommended to mandate the use of digital signatures while uploading documents in the e-GP portal. Digital signatures increase efficiency and accountability for every stakeholder.	**Not Complied**	**Not Done**
27	It is recommended to enforce the following password parameters: ⁃ Maximum Password Age – 45 Days ⁃ Enforce Password History – 3 times ⁃ Account Lockout – 5 attempts	**Not Complied**	**Not Done**
28	It is recommended that the following password settings must be enabled/defined for the Red Hat Linux server : ⁃ Minimum Password Strength : 15 ⁃ Password Complexity: Combination of alpha-numeric, special characters ⁃ Password Minimum age : 1 Day ⁃ Password Maximum age defined : 45 Days ⁃ Account lockout : 3	**Not Complied**	**Not Done**
29	It is recommended that PPMO must implement the usage of an RADIUS/AAA device to define and implement password parameters for the network devices.	**Not Complied**	**Not Done**
30	It is recommended that: ⁃ Unique user IDs and user names should be assigned to all individuals using the e-GP system ⁃ Review the duplicate instances existing in the system and take appropriate action	**Not Complied**	**Not Done**
31	It is recommended to create a new 'eproc' database user having limited privileges, to authenticate all the e-GP user defined actions, as defined to perform the specific actions. E.g. - Select, Insert, Update, View, Show, Edit Further, the user access should be restricted to required tables only.	**Not Complied**	**Not Done**
32	It is recommended to: ⁃ Define the performance targets so as to ensure that the end user requirements are being met	**Not Complied**	**Not Done**

S.no	Recommendations Made	Status of Compliance	Remarks
	□ Continuous Monitoring to be performed to compare the response time numbers and performance of system with its earlier releases or competitor's comparable products or applications □ Define a threshold for the peak load and observe/evaluate the behavior of the system for a particular time		
33	It is recommended that e-GP coding standards should be drafted, finalized, approved and implemented .The document should be regularly updated and maintained as per the technological changes.	**Partially Complied**	**Not done completely but standard JAVA coding standard is followed.**
34	□ It is recommended to perform the following activities: □ Perform threat modeling from a potential attacker's perspective, as opposed to a defender's viewpoint □ Go with a structured approach that enables you to identify, quantify, and address the security risks associated with an application □ Documentation produced as part of the threat modeling process, at the beginning of the development phase should be maintained and retained □ The threat modeling process can be decomposed into 3 high level steps o Decompose the application o Determine and rank threats o Determine Counter measures and mitigation	**Not Complied**	**Not Done**
35	It is recommended to include the Fail secure and Open design concepts, and design the security mechanism so that a failure will follow the same execution path as disallowing the operation. For example, security methods like is Authorized(), is Authenticated(), and validate() should all return false if there is an exception during processing. If security controls can throw exceptions, they must be very clear about exactly what that condition means.	**Not Complied**	**Not Done**
36	It is recommended that the URL should be masked to download any such sensitive document to avoid any possibility of SQL Injection.	**Not Complied**	**Not Done**

S.no	Recommendations Made	Status of Compliance	Remarks
37	A systematic java upgrade should be planned, tested and implemented by the PPMO IT team • Plan an upgrade of Java and related components • Dependencies like Application server upgrade to be done one at a time	**Not Complied**	**Not Done**
38	It is recommended that PPMO IT Team ensures that the developers for the e-GP system (in-house or outsourced) have relevant experience and are trained, to a minimum, in the identified secured coding standards covering the following: □ Software development checklist for secured coding □ Avoiding Buffer Overflows and Underflows describes the various types of buffer overflows and explains how to avoid them. □ Validating Input and Interprocess Communication discusses why and how you must validate every type of input your program receives from untrusted sources □ Race Conditions and Secure File Operations explains how race conditions occur, discusses ways to avoid them, and describes insecure and secure file operations □ How to avoid running code with elevated privileges and what to do if you can't avoid it entirely □ Designing Secure User Interfaces □ Designing Secure Helpers and Daemons describe how to design helper applications in ways that are conducive to privilege separation.	**Not Complied**	**Not Done**
39	It is recommended to document the approvals, test cases and closure process and reporting to all relevant stakeholders. A documented process to be defined and implemented for regular fixing of all the open test results, that includes □ Documentation of the details of the fixes made □ Test Cases and Test results □ Timely closure of the same in the test report	**Not Complied**	**Not Done**
40	It is recommended that: □ For the InnoDB table issue, enable the InnoDB Monitors to obtain information about a problem and apply the requisite solution □ For the Alfresco related issues, use logstash, a tool for managing events and logs	**Not Complied**	**Not Done**

S.no	Recommendations Made	Status of Compliance	Remarks
	(https://www.elastic.co/products/logstash)		
41	It is recommended to identify and document a process for proactive performance monitoring and tuning. Monitoring performance at various levels should be undertaken as per a documented procedure which should cover: □ Operating System □ Database level □ DMS level □ Application level □ Database lock contentions □ Application memory leaks □ Swap and buffer configurations Use performance test results to help stakeholders make informed architecture and business decisions	**Not Complied**	**Not Done**
42	It is recommended to : □ Design load tests that replicate actual workload at both normal and anticipated peak times □ Conduct stress testing with the key performance indicators (network, disk, processor, memory) and business indicators such as number of bid submissions lost, user login failures, and so on. □ Deploy performance specialist and try to fine tune the-GP system performance, as and when required. □ Design benchmarks to rate the performance □ Use profiling tools/instrument the application to identify issues □ Use tools to identify memory issues, database issues Use of source Code analysis tools – e.g. Vera code or Fortify to identify any code related vulnerabilities	**Not Complied**	**Not Done**
43	It is recommended to prepare an annual audit calendar and audit plan specifying the IT areas to be audited, along with the timelines. Internal audits should be conducted as per the IA plan defined at the beginning of the year.	**Not Complied**	**Not Done**

Also, ESC Private Limited had carried out the review of existing hardware deployment architecture dated 15th September, 2017 wherein gap analysis was done in relation global trend and PPMO scenario. They had made some suggestions to make e-GP Phase II more successful. The following recommendations had been made whose status is as follows:

Table 2: Third Party Assurance Report by ESC Private Limited (September 2017)

S. No	Gap Analysis by ESC Pvt Ltd	Action taken by PPMO
1	Absolute High Availability has not been possible due to licensing issue with Alfresco and other clustering needs. It is the very reason, the current set up is in Active-Passive mode with minimal manual intervention in cases of hardware failures despite being a worst case scenario.	PPMO has already instructed existing O and M consultant regarding this so that absolute high availability can be implemented.
2	SMTP server dependency during ISP switchover has been witnessed due to cross connection issue between ISP's individual SMTP gateways (Subisu and NTC).	PPMO has already discussed with concerned ISP and Genese (Amazon Web Service Partner) for mass mailing solution. Also, PPMO has reduced the number of emails to be sent to the users. Similarly, PPMO implemented SMS Service for OTP forwarding to the bidders.
3	Network monitoring tools is working but as per time features need to be upgraded to use it in par with other commercial monitoring tools.	Currently, PPMO is using NagiOS as networking monitoring tool and this year going to implement hardware based security information and event management tool (SIEM).
4	Disk utilization by jboss and latency during file handling by Alfresco need further assessment and alternative solutions.	This issue has already been reduced but not up to the level we expected. PPMO is researching and experimenting (in co ordination with O and M consultant) for different options for this issue.
5	Database backups need to be automated and streamlined with best practice scheduler policies.	Currently database backup is done with the help of cron job in linux.
6	Threat Management System to cope with evolving threats and attacks are inevitable. The current sonicwall device is most suited for small and medium level applications rather than enterprise level applications like bolpatra.	This year, PPMO is going to procure latest web application firewall (WAF) with DDOS feature to resolve this issue.

Also, during our visit to Department of Roads (DOR), Babarmahal, Kathmandu we came across an issue where the bid of DOR was forwarded to Department of Urban Development and Building Construction (DUDBC) for approval. We were told that the function of delegation of authority assigned in the system is not working properly.

iii. Risk: PPMO does not have a in house internal IT audit department. Also, DOIT conducts the IT audit for government organization on request basis. Over dependency upon the third party to conduct IT audit may lead to: Non identification of system related issues

at the time they are generated as there is a huge gap of occurrence of the issues and the time they are reported

iv. Impact: Lack of resources within the organization may lead to over dependency upon the outsourced third parties. Also, as status of recommendations made by DOIT and DTTILLP has not been provided to us due to which we cannot assure that those recommendations have been acted upon or not.

v. Recommendations: It recommended to build the capacity and a in house team to conduct IT audit of E-GP on regular basis as E-GP is used by the end users or say public at large. Also, it is recommended to enact upon the recommendations provided by DOIT and DTTILLP within a specified time frame.

vi. Management Response:

2.1.5 Human Resources

i. Criteria: Management should have adequate personnel procedures to ensure that only suitable staffs are employed, with the requisite IT experience and knowledge, and an assessment of staff suitability in respect of security integrity has been performed. Terms of employment should cover security and the breaches thereof.

ii. Audit Observation: It has been observed that the IT team of PPMO consists of 1 IT director and 4 Officers. Out of 4 officers, 3 are computer engineer (1 position vacant) and one is Computer Officer. Presently, all the staffs in IT department are from IT background. The IT Section is responsible to create a hassle free e-procurement platform for E-GP users. The available human resource is not sufficient to cater the needs to end users. Also, there is over dependency upon the outsourced staffs for System Administrator, Network Administrator and database administrator as the core employees are not available. The dependency upon the outsourced staffs should be minimized as the system is always at risk when in the hands of core outsourced staffs. Support, maintenance, development, feature enhancement, etc works can be outsourced. But the core tasks should be handled by the in house team of PPMO. Outsource staffs i.e. are from DG Market Private Limited whose responsibility is to function as System Administrator, Network Administrator and Database Administrator. So, the core functions of IT department are carried out by the Outsourced Company. (For reference we have obtained the staff structure of IT department).

iii. Risk: Inadequate manpower leads to exposure of following risks: a. Risk of over dependency upon outsourced staffs which may lead to lack of internal skills and expertise b. Outsourced staff will be over powered and in house staffs will not be capable to develop their capabilities. C. Manpower shortage at a certain juncture.

iv. Impact: Lack of human resource may impact upon the productivity of the organization. Lack of adequate core human resource will result in over dependency upon the outsourced staffs.

v. Recommendation: It is recommended that PPMO should hire the required number of capable staffs and parallely carry out the core activities of E-GP such as Network

Administrator, System Administrator and Database Administrator. All the changes/ updates etc to be done in software should be done by in house staff of PPMO and this can only be possible if PPMO hires qualified and capable staffs.

vi. Management response:

2.1.6 Training

i. Criteria: Training and support should be provided to all users to address their IT needs to ensure proper use of IT resources for business need. This should include emphasis on security awareness training. Staff induction should also cover these areas.

ii. Audit Observation: It has been observed that there is no separate training plan. Staffs are sent for training on need basis. None of the staffs of IT department went for training in last Fiscal year 2074-75 and till date. As per conversation with IT director, no IT budget was available as well as they were not in need of training due to which the staffs did not go for training. However, E-GP was pilot launched on 2nd Baisakh 2073 and fully launched on 1st shrawan 2074. Till date around 6000 end users, stakeholders, have been trained for E-GP software. In the FY 2074-75 training to 1550 users have been provided on E-GP.

iii. Risk: Lack of training to the Core staff members of IT department may result in lack of awareness of the staffs about the enhanced features of E-GP; integrity of documents; etc.

iv. Impact: End Users do not get training on need basis, no time plan for regular training due to which the users of E-GP are not aware of its enhanced features as well as its ease of use.

v. Recommendation: It is recommended to provide training to the IT team of PPMO on regular basis who can in turn train the end users of EGP; fix the bugs in the system; maintain the integrity of data in the system; cope up with the system updates and minimize the dependency upon the outsource staffs.

vi. Management Response:

2.1.7 Compliance

i. Criteria: IT systems should be regularly checked for compliance with security standards, and operational systems examined to ensure hardware and software controls have been properly implemented. Such testing should be performed by experienced systems engineers, supported by appropriate software packages, and should encompass penetration testing. The results of testing should be reported and any discrepancies followed up and resolved

ii. Audit Observation: It has been observed that no documented security standards and operational system compliance are available. DOIT did VAPT test in 2071/72 and thereafter once in 2074-75 in by Deloitte. No guided policy document which specifies it needs to be done twice in a year. The recommendation done by Deloitte has been forwarded to consultants for implementation. Security standard and operation system

compliance is in draft phase and not approved. Outside networks are blocked by firewall. Unwanted ports are disabled. Unwanted and suspicious activities are blocked through their IP address. Direct route access is not allowed in the host server. Other servers are in private network and can be accessed through VPN only. Two operating tools PENDORA and ZENOSS (Open source) are being tested for monitoring network, application and system.

iii. Risk: There are no policy documents which specifies the activities to be done mandatorily, security standards to be followed; etc which may lead to absence of responsibility of the IT team of PPMO in case of any mishappenings.

iv. Impact: Follow up activity is done on need basis. No time frame has been cited to conduct VAPT.

v. Recommendation: It is recommended to formulate the policy and compliance documents and get it approved by the management.

vi. Management Response:

2.1.8 Helpdesk

i. Criteria: Procedures should be in place to provide adequate and timely IT assistance and support to end users. This should include establishing and operating a help desk and monitoring end user satisfaction with the IT environment. IT problems should be analyzed for the existence of trends and the incidence of reoccurrence, and the necessary actions put in place. Performance Indicators should be set for Helpdesk response times.

ii. Audit Observation: It has been observed that PPMO has a outsourced helpdesk system from IT Defense , Sifal, kathmandu. The supply of services has been agreed @ (redacted). Section 3 of TOR with IT defense describes the "Scope of Services". Considering the report available, it has been observed that Scope of services have not been met. Enquires from the end users are lodged through telephone. Also, the company provides training to E-GP users on request basis. No access to database given to helpdesk people. If internal issue is raised helpdesk people contacts database administrator and system administrator to facilitate the end users. Parallelly if the end user goes to helpdesk people, end users are trained, educated to overcome the issues. No automated software is available to create the tickets of issue lodged and solved. Hence, no exact response time can be depicted. Also, helpdesk support is provided only during office hours. There is no system of providing help 24*7. During the FY 2074-75 helpdesk service to 1325 users have been provided. The record of helpdesk is raw and is not dependable. For instance, the following report has been submitted by IT defense:

Table 3: Helpdesk Sample Report

Request From (redacted)	Name of Office	Phone Number
	Rashmi and Pandey Construction	98511932XX
	DDC Solu	98424111XX

Table 4: Helpdesk Training Sample List

Training date	Request By	Name of PE	Address of PE	Participant (redacted)	Designation	Training Module
01/02/2075	PPMO	Devmai Municipality	Ilam		Engineer	Pubic Entity
01/11/2075	PPMO	Khotang Halri	Khotang		MD	Bidder

iii. Risk: Absence of a defined helpdesk management plan elevates the risk of any such users request remain unattended which elevates the risk of unresolved requests within an agreed timeframe. A service request or incident could remain unattended for a significant period of time without formal logging and tracking.

iv. Impact: Real time monitoring system is not available due to which the issues faced by stake holders and end users may remain un-noticed.

v. Recommendation: It is recommended to enact a 24*7 monitoring system. A real time incident monitoring tool SIEM can be implemented to provide real time security incident monitoring and escalation. It is recommended to define and implement an incident Management Policy. The policy should define the roles and responsibilities as well as the response time for resolution of the issue of the users.

vi. Management Response:

2.2 Logical Access Security

2.2.1 Procedures

i. Criteria: The client should have formally documented procedures in place that define its approach to system logical access security, particularly as it relates to the confidentiality and integrity of data and information.

ii. Audit Observation: It has been observed that PPMO has defined E-GP directives and user log manuals for user's , bidder's and banker's wherein responsibilities and duties has been set out. Each user has his/her own username and password for security aspect. When users are transferred their User ID and passwords are blocked. User

Access manual is available in draft version yet to be approved and implemented by the management.

iii. Risk: Non availability of the manuals may lead to unauthorized access/ disclosure of sensitive data; modification of sensitive data.

iv. Impact: may lead to disclosure of sensitive data and information, confusion in rights and responsibilities of the users.

v. Recommendation: It is recommended to authenticate the user access manual and clearly define their duties; responsibilities; rights; breach of information, etc

vi. Management Response:

2.2.2 Passwords

i. Criteria: There should be a defined password policy for system administrators and general users. This should be communicated to all staff dictating best password practice for users; historically alpha-numeric with a symbol was considered strong but due to complexity it is considered that memorable passwords that are not obvious are the strongest. Each system user should have a unique identifying user name or user ID. There should be a policy enforcing that passwords are strong and retained unless there is evidence the password has been compromised. Passwords should be strongly protected, for verification purposes this should be by hashing and salting (encryption is used for different purposes from verification) . All default passwords on system hardware and software should be changed; particularly key points in the infrastructure such as routers, firewalls and wireless access points. Section 16 Directive requires that tenders are prescribed for using One Time Password sent by the system. (The UK National Cyber Security Centre website contains the latest thinking on password policy)

ii. Audit Observation: It has been observed that Passwords are alphanumeric and symbolic in nature minimum of 8 characters. No regulation for timeframe of change of passwords. System has firewall, Encryption, Key Logger, default passwords, OTP. There is no specific password policy to govern the password issuance; change; updation; deletion; security management. OTP is issued by the system to the bidders through emails and SMS before the submission of bid document. There is no compulsory password changing system and no automatic password expiry period.

iii. Risk: Lack of password security features; malicious attackers may forcefully attack the system and bring the whole system down.

iv. Impact: Passwords may be hacked; data and information confidential to the organization may be leaked and forged.

v. Recommendation: It is recommended to enable the following password settings: Minimum Password strength-15; Minimum age of Password- 1 day; Maximum age of Password- 45 days; implement a specific software for defining and implementing password parameters of network devices.

vi. Management Response:

2.2.3 Log In/Log Out

i. Criteria: There should be log out/ log in procedures to protect the system integrity and the responsibilities should be communicated to users. User accounts should be disabled after a limited number of unsuccessful log on/ Log In attempts. The number of unsuccessful log-on/ Log-In attempts should be limited and recorded.

ii. Audit Observation: It has been observed that PPMO has a system of automatic log out from E-GP if the page remains unused for an hour. Log Out Policy is not available. Audit Log is available. Login is allowed for 5 attempts. In case login is failed in all 5 attempts then the system gets locked for 15 minutes. Log In Policy is not available but audit logs are maintained.

For instance the audit logs available are as follows:

Table 5:Log In/ Log Out Sample Report

User ID	User Activities	User Time Stamp	IP Address	Created On	Created By
503X	Logging for: fetch Branch List	2018-08-24; 10:58:45	202.50.52.X	2018-08-24; 10:58:45	503X
466X	Opened Tender Information to show summary	2018-08-24; 10:58:47	202.50.52.X	2018-08-24; 10:58:47	466X

iii. Risk: E-GP system may be vulnerable to Brute Force Attack.

iv. Impact: System may be prune to attacks.

v. Recommendation: There should be a clear policy in place specifying the log in attempts/ log out timing; screensaver to appear after it gets automatically log out; an automated email to the user about the system being logged in after certain number of attempts or logged out after a certain time frame.

vi. Management Response :

2.2.4 Segregation of Users

i. Criteria: Shared areas should be restricted through password controls, and selected facilities should be restricted to specific categories of user. Standard user access profiles for common categories of applications should be used sparingly. The information systems should make use of menu options, security gateways and logical user domains; this will ensure appropriate segregation of users and duties on the IT system

ii. Audit Observation: We have observed that there are two types of Users. i. System User ii. Application User. In case of Application users there are 4 category of users: Super User (PPMO); Public Entity (Admin, Creator, User, Approver and Accountant); Bank

(Maker, Checker and Central); Bidder (User). There is a directive for Application User. The directive is being followed too. Only one category is system administrator is in place. The system administrator is a consultant outsourced by PPMO. The right of the consultant is used by an IT Engineer from PPMO in understanding basis between the two. But there is no specific directive for system users.

For Instance, we have taken a TOR of PPMO with Nabil Bank wherein responsibility of Bank clause 6 (b) states that Bank shall verify the bid document fee, bid security etc within 2 working days from receipt in the Bank's dashboard after the bidder uploads the electronic files. It has been observed that out of 38,094 bank instruments, 21,895 (56%) instruments were verified after 2 working days and 17,009 (44%) instruments were verified within 2 working days. Hence, there needs to be a system to control such environment.

iii. Risk: There is a risk of overlaps and gaps in segregation of duties which may lead to fraud

iv. Impact: This raises the chance of fraud and may also over or underload staff leading to a reduction in quality and efficiency.

v. Recommendation: It is recommended that PPMO should be outsourcing their IT Operations to a third party, with the onsite model with clear assignment of authority and responsibility over e-GP operations and ensuring segregation of duties.

vi. Management Response:

2.2.5 Audit Logs and Monitoring

i. Criteria: Audit Logs should be switched on and set to monitor all users; including system administration. The IT department management should periodically review each significant system and application to identify any instances of unauthorized user access. Processing errors and access violations should be logged and the logs routinely reviewed. Any unusual or unexpected items should be followed up.

ii. Observation: It has been observed that audit logs are available only for the issues lodged by PPMO IT team to their consultant through a software called GITLAB. These audit logs are only internal in nature and record the timings, status of issue, etc. However, for the issues lodged by the users of E-GP no audit log is available. Issues are lodged through telephone and the outsource helpdesk company prepares and submits a report of the issues sorted out by them. They basically train the users about the issue. But the report is not a audit log.

iii. Risk: Audit logs are only accessed when users faces any problems. Audit logs are not pre-active but pro active in nature. No separate policy for audit logs is available.

iv. Impact: Audit logs or the report is not reviewed on a regular basis. Major issues may be repetitive in nature and remain unidentified.

v. Recommendation: It is recommended to maintain audit logs and confirm that they are switched on. There should be a monitoring system in place to actively monitor these logs and take actions on the issues before they arise in the system.

2.2.6 Starters and Leavers

i. Criteria: The client should establish formal policies and procedures ensuring control of new employee's access to the system and the update and/or removal of systems access rights to employees who change job duties or leave the organization.

ii. Observation: It has been observed that Starters are assigned user name and passwords and even given orientation about the system. In case of leavers user id and passwords are blocked. Incase leaver is a system user then whole set of user name and password is changed. No recording for the same is done. Username and passwords of leavers are removed and handed over one day prior to the day they are leaving office. The same is confirmed through emails. No separate documentation is available.

iii. Risk: The main risk with non-removal of access for leavers is that their account could be taken over by someone else in Department of Customs and used to cover up fraudulent activities.

iv. Impact: This can lead to a potential bypassing of segregation of duties.

v. Recommendation: It is recommended to prepare a policy document specifying the procedures for assigning the rights starters and leavers.

vi. Management Response:

2.2.7 Administrators

i. Criteria: Administrator rights should only be assigned to a limited number of individuals who require those rights to perform their job duties. The activities of systems administrators and other privileged users should also be logged and subject to periodic review.

ii. Audit Observation: It has been observed that two personnel have been assigned administrator rights. Both are from outsourcing company. Logs of System administrator are maintained. Administrators are provided with Super user rights. No review is done for the activities performed by system administrators. System administrators carry out the activities in the servers only after approval from the IT director. Presently there are two administrators:

Anup Gyawali- Representative from DG Market Pvt Ltd and Amod Ulak- Representative from PPMO.

iii. Risk: The risk is that system administrators have access to most/all of the functionality of the system and their work needs to be carefully controlled and subject to review.

iv. Impact: May lead to fraud, stealing of sensitive data and information of users.

v. Recommendation: It is recommended to review the access privilege provided to system administrators, super users and approved by the IT head in a frequent interval of time.

vi. Management Response:

2.2.8 Application Controls

i. Criteria: The client should ensure a control environment exists over the integrity of general input controls and data capture to ensure data is complete, authorized and accurate. These procedures should be documented, and such controls should typically include the use of authorized user lists, standard input forms, format checks, range checks, reasonableness checks, dependency checks, the use of check digits, and general management review procedures. This will be particularly important where systems interface manually or automatically with each other.

ii. Audit Observation: It has been observed that PPMO doesn't have a specific system map available defining the control over data. Data is transferred automatically. Activity diagram is not available. UAT Conducted in TEST server before implementing it in LIVE server.

iii. Risk: Integrity of data cannot be assured.

iv. Impact:

v. Recommendation: It is recommended to prepare a system map of E-GP clearly defining the controls established over the data, application controls as system map provides visibility to an end-to end process. A system map provides overall snapshot of the business identifying the areas of risk, challenges, short comings and directing the ways for improvement.

vi. Management Response:

2.2.9 Anti-Virus

i. Criteria: The client should establish procedures against malicious programs through the use of anti-virus detection and repair software and policies limiting the installation of unapproved programmes and procedures for reporting suspected occurrences of viruses.

ii. Audit Observation: It has been observed that no antivirus is used for application control i.e. E-GP software. In case of developer device, antivirus is used the one available in market. As antivirus is not used for E-GP so files uploaded in the system is not scanned for virus.

iii. Risk: A virus may attack the system leading to data corruption and infecting other systems in the network.

iv. Impact: May lead to reputation loss of PPMO and failure in the contracting process.

v. Recommendation: It is recommended to install antivirus in the E-GP system. Documents uploaded in the system should be compulsorily scanned before being uploaded.

vi. Management Response:

2.2.10 Firewall

i. Criteria: Connections with business partners and public networks should be adequately managed and controlled by a firewall. The firewall should hide the structure of the client's network, provide an audit trail of communications with public parties, generate alarms when suspicious activity is suspected, and defend the client's network from viruses

ii. Audit Observation: It has been observed that there is no approved firewall policy. Presently, Sonicwall is being used. Presently, PPMO is using a firewall draft policy which is in practice

For instance, such report is generated:

Table 6: Firewall Sample Report

From	To	Source	Destination	Service	Action	Users Incl	Users Excl	
DMZ	LAN	Any	Any	Any	Deny	All	None	
DMZ	DMZ	Any	All X2 Management IP	HTTPS Mgmt	Allow	All	None	
VPN	LAN	Any	All Interface IP	HTTP Mgmt	Allow	All	None	

iii. Risk: Non availability of policy may create security loopholes that might allow malicious traffic to sneak into a private network or block the legitimate traffic and disrupt the normal business process.

iv. Impact: Quality of protection provided by the firewall depends upon the quality of its policy. Lack of policy may hamper normal business procedures.

v. Recommendation: It is recommended to formulate a firewall policy. Firewalls are always prone to new threats over the network. Hence, firewall policy should be flexible enough to modify rules to allow or protect the operation of some services.

vi. Management Response:

2.2.11 Database Security

i. Criteria: The data on the EGP database is of value and its security is a specific risk area. It would be expected that the database is secured and a strong method of disguising data is implemented. It would also be expected that the controls noted in the rest of the audit test steps apply to the Database.

ii. Audit Observation: It has been observed that activity log of the database administrator is maintained. Database activity monitoring tools is not available. All the documents are preserved in encrypted form. We have obtained the database log as well as data being

saved in encrypted form. Review of activities carried out by database administrator is not done.

iii. Risk: Confidentiality of data cannot be assured as database administrator is an outsourced person.

iv. Impact: Unusual activity may not be picked up properly by current procedures and control activity.

v. Recommendation: It is recommended to review the activities of database administrator on a regular basis and appoint in house database administrator, if possible.

2.3 Physical Access Security

2.3.1 Procedures

i. Criteria: The client should have formal procedures in place that define its approach to physical security. These policies and procedures should apply equally to hardware and software, and should also apply to equipment and data used off-site or managed by an external supplier. Procedures should be in place for communicating this policy to employees and requiring them to acknowledge that they have read, understood, and agreed to these policies.

ii. Audit Observation: It has been observed that there are no written policy and procedures available for physical access security. For backup data security, PPMO is adhering to the requirements of GIDC. System runs from GIDC and a backup is kept in central office of PPMO and GIDC also. In case of central office, keys for physical security of backup data is kept with IT director. Physical security in GIDC is assured by GIDC. Monthly visit from central office is done to GIDC.

iii. Risk: Lack of procedures for physical access security over the assets may lead to unauthorized access of assets.

iv. Impact: There could be a loss of data and/or revenue; this would lead to reputation loss of the organization.

v. Recommendation: It is recommended to formulate a policy for physical security of the assets of the organization.

vi. Management Response:

2.3.2 Physical Security

i. Criteria: Physical security should be achieved through the use of physical barriers to entry (e.g. access restricted to key or keypad holders) where specific IT hardware and software is held. The client should operate general security procedures such a security passes and visitor logs.

ii. Audit Observation: It has been observed that manual Log is maintained for entry and exit to server rooms, network switches, etc. System and Network Architecture is

assigned with the responsibility to access server rooms, network switches. Rooms where local servers are kept are not locked.

iii. Risk: Manual logs are not dependable. It may lead to unauthorized access to sensitive premises, theft of hardware, etc.

iv. Impact: Loss of reputation of the organization.

v. Recommendation: It is recommended to secure the access to server rooms. Items restricted in such rooms or sensitive areas should be listed out and displayed at the entrance area.

vi. Management Response:

2.3.3 Monitoring

i. Criteria: Management should initiate regular reviews of the software and data content of critical system to identify the potential presence of unauthorized files and data or errors in automated business process flows. All exceptions should be logged and followed up. There is a specific risk that the evaluations steps in EGP are not being used. Assess what management have done to analyze the reasons for this and correct the issue.

ii. Audit Observation: It has been observed that Critical issues lodged by users are cleared by internal staffs of PPMO primarily and in case they cannot resolve it, the same is transferred to outsource agency. If there is bug in the system it is fixed, or if the issue lodged by user is critical it is tested and resolved. Evaluation is EGP is not used completely. As directive specifies a compulsory use of technical bid evaluation, feature beyond that is not compulsorily used. Based upon the issues lodged, in case of change in PPA and PPR/ standard bidding document, change/ update is done in system. No regular review of software is done.

iii. Risk: There is a risk that a major issue/ incident may not be recognized timely which may hamper the performance of the system.

iv. Impact: Normal business activities may slow down, system may not be updated timely.

v. Recommendation: It is recommended to do regular review of the system.

vi. Management response:

2.3.4 Back-Up

i. Criteria: Management should ensure that all data is backed-up on a regular basis (at least daily) and that such back-up is maintained in a secure location off-site. Full documentation of all back-up should be maintained, together with documented restoration procedures. At least three generations, or cycles, of backed-up information should be maintained. All back-up data should be tested on a regular basis.

ii. Audit Observation: It has been observed that Back Up of data is being done daily twice a day. Back up takes around 20 mins time and regular activity is not halted during the

backup. Backup server has not been tested. Backup of data can only be done by system administrator. Backup is maintained at GIDC as well as central office of PPMO.

iii. Risk: Without the proper restoration testing, it cannot be assures that backed up data can be successfully restored and used.

iv. Impact: Backup data may not be restored for use without proper and timely testing.

v. Recommendation: It is recommended to define a separate Back Up Policy. There should be a plan/ schedule for restoration of backed up data. Restoring should be done on regular basis.

vi. Management Response:

2.3.5 Third Parties

i. Criteria: Access to internal networks and/or applications by suppliers, customers, and/or other business partners (i.e third parties) should be approved by appropriate management and limited to those networks and/or applications required for the conduct of the business. Representatives of suppliers, customers and other business partners should be required to adhere to the client's own policies, procedures and security standards when accessing the client's systems. The client should also have a contractual right to audit third parties.

ii. Audit Observation: It has been observed that PPMO has appointed various third parties such as Helpdesk Manager, System Administrators, Network Administrators, Database Administrators, SMS service provider, etc. PPMO has entered into contract with all the parties clearing specifying their responsibilities, deliverables, value of contract, time period, etc. Administrators are provided with the right to access the system, network and database and are controlled through their individual passwords and user rights.

iii. Risk: Over dependency on Outsource company may lead to loss of control. There is a risk that the contract with the third parties may not get renewed timely which may hamper the regular activities.

iv. Impact: Trust of the end users of E-GP upon the in house staffs will diminish as they will be depending upon the third parties for the service.

v. Recommendation: It is recommended to ensure that contract with the third parties assure value for money, are renewed timely and evaluation of their performance is done in a regular time frame. Also, emphasis needs to be given to empower the in house staffs rather than being dependent upon the third parties.

vi. Management Response:

2.3.6 Interfaces

i. Criteria: Where networks, disks, or tapes are used to transfer data, management should ensure that the transfer is both complete and accurate. Where data is transmitted across networks, there should be a communication protocol that determines the format of transmitted data and incorporates automatic error detection and correction facilities

ii. Audit Observation: It has been observed that Entry done by user goes directly to database. Back up is done regularly. Data cannot be accessed through tapes. But hard disk is allowed to transfer the data and get it uploaded. No virus scanning of the external device is done before uploading the data in the system. External hard disk is rarely used. Time and again the data is checked for completeness and accuracy but there is no guideline available for it. HTTPS (hypertext transfer protocol secure) protocol is used for transmission of data across the network.

iii. Risk: There is a risk that data may not have been transferred accurately and completely over the network as there is no review mechanism for it.

iv. Impact: As hard disk is allowed to transfer the data and manual intervention is needed it cannot be assured that data has been transferred completely and accurately.

v. Recommendation: It is recommended to transfer the data completely and accurately through a secure network and also a guideline for the same shall be available.

vi. Management Response:

2.3.7 Environmental Defences

i. Criteria: All hardware and software should be located in environmental locations and be secure from the risk of fire and flood. All power supplies should be protected, and there should be access to alternative power supplies.

ii. Audit Observation: It has been observed that all the hardware and software belongs to PPMO but risk of fire, flood, earthquake, uninterrupted power supply is assured by GIDC.

iii. Risk: There is a risk that the infrastructure provided by GIDC to secure the data from flood, fire, earthquake, uninterrupted power supply may not be sufficient as no document about the infrastructure details is available.

iv. Impact: May lead to loss of data and failure in the contracting process.

v. Recommendation: It is recommended to get an assurance about the sufficiency of infrastructure of GIDC.

vi. Management Response:

2.3.8 Security Logs

i. Criteria: There should be a mechanism in place for recording all security threats, whether actual or averted. This should be required by the security policy, and may utilize a security log. This should be reviewed by senior management, and all security incidents, whatever their nature, acted upon and resolved through the introduction of security enhancements. The use of formal disciplinary procedures should also be considered.

ii. Audit Observation: It has been observed that Network Monitoring tool is installed. No dedicated device for monitoring security issues i.e. SIEM is not available. The tool reviews the behavior of transactions. In case the behavior is different from regular one,

alert message is given to the system thereafter further steps are taken to secure the system from the mis happenings.

iii. Risk: As the logs are not monitored pro-actively, it may lead to failure to detect the unauthorized activities on the network. There is a risk of unauthorized modification or deletion of logs.

iv. Impact: Evidence may not be available on case to case basis in case further investigation needs to be done.

v. Recommendation: It is recommended to implement a SYSLOG server; analyze the security logs on a regular basis and review the reports; implement a real time monitoring tool.

vi. Management Response:

2.3.9 Assets Register

i. Criteria: All system hardware and software should be adequately documented through the use of a hardware and software inventory. The inventory should include databases, data files, systems documentation, manuals, and archived information. Policies should exist that ensure that such inventories are updated on a regular basis, and that periodic physical reconciliations are performed. These checks should also record any developments required to the physical infrastructure and repairs and maintenance to allow the most effective use of ICT and allow the updating of the plan for asset purchase cycles. Such control should also ensure that the client is not in breach of any software licenses.

ii. Audit Observation: It has been observed that no Separate hardware and software register is available. No separate physical security available for hardware and software. Individual system have antivirus. AMC are available for hardware and software. Internal health check of system is done every week. And visit to GIDC is done every month to check physical alarms. Information about the internal health check is reported through email and is done by the ONM. However separate plan for up gradation of hardware and software is not available. License version of Operating system i.e Linux and Red Hat (Enterprise Version is presently used) is available but has not been used and implemented. All the application of database is in Java which is open source. For database MYSQL is used which is enterprise version. For Content Management, ALFRESCO is being used which is community version (free version).

iii. Risk: lack of assets tracker could lead to ineffective management of assets.

iv. Impact: Status of assets cannot be assured.

v. Recommendation: It is recommended to install a asset tracker which captures the details of assets, date of use, due date of AMC, life of asset, ownership of asset, etc.

vi. Management Response:

2.3.10 Data Disposal

i. Criteria: The client should have procedures for the confidential disposal of sensitive data including on paper, magnetic and optical media, USB storage, disposal of old PC's etc.

ii. Audit Observation: It has been observed that no data has been disposed till data as well as no disposal policy available.

iii. Risk: Data storage space may be insufficient if unwanted and repetitive nature of data are not disposed off.

iv. Impact: Confidential data and information may enter the Public domain.

v. Recommendation: It is recommended to identify the unwanted data and information in the database, zip them, and dispose them after the approval from authorized personnel. Also, data storage space can be increased. Presently 78% of the disk space has already been occupied. Various methods such as Purging, Clearing, etc can be used. However, verification of data disposed off should be done.

vi. Management Response:

2.3.11 Business Continuity Plan and Disaster Recovery Plans (and Drills)

i. Criteria: Management should have conducted an impact analysis and developed a business continuity plan and disaster recovery plan. This should incorporate an analysis of risk and potential impact (including damage scale and recovery period), and assign responsibilities and actions to take in the event of a disaster. Contingencies should include manual and automated solutions, and consider alternative locations and externally provided services. The plan should be subject to periodic testing, be subject to regular review and be updated when necessary.

ii. Audit Observation: It has been observed that Business Continuity Plan and Disaster Recovery Plan is not available. BCP shall include emergency response system, incident response plan, point of recovery, recovery time objective for E-GP. Disaster recovery site is not available.

iii. Risk: Absence of BCP may bring whole system to halt in the long run. No testing/ drills can be performed. In the situation of cyber-attacks, natural calamities, lack of DRP may lead to discontinuity of E-GP operations.

iv. Impact: Confidentiality and integrity of information and data may be hampered. May result in monetary loss and reputation loss of the organization.

v. Recommendation: It is recommended that PPMO should have a formal documented BCP plan approved and implemented. Plan for contingency for natural calamities, external threats, etc should also be incorporated. Such plans should be updated on a regular basis. PPMO has identifies Hetauda as DR site. DR Plan should be in place approved and implemented. Potential threats to the E-GP environment should be identified and accordingly DR plan should be prepared.

vi. Management response:

2.4 System Implementation and Operations (Development and Maintenance)

2.4.1 Central Records

i. Criteria: It is expected that the records of used software are maintained in Department of Information and Technology (DOIT).

ii. Audit Observation: It has been observed that the E-GP software is registered with DOIT. We have taken a snapshot for assuring whether E-GP has been listed in DOIT or not. The details are as follows:

Table 7: Central Record Listing details

S.No	Officer's Name (redacted)	Name of Organisation	Name of Software	Software Type	Nature of Job	Status	Created On
1		Public Procurement Monitoring Office	Electronic Government Procurement System (e-GP)	Good governance and administration	New Development	Running	2017-08-24

iii. Impact: Listing of software with DOIT ensures that the organization has complied with the government rules and regulation.

2.4.2 Customized/ Bespoke IT System

i. Criteria: The definition and prioritization of system developments and maintenance should be consistent with business strategy and defined requirements and standards. Project documentation should be maintained and should include system requirement definitions, risk analysis, cost-benefit analysis, and security risk assessments. Wherever possible, the client should make use of reputable commercial software, and should minimize the amount of bespoke software introduced to the operational environment.

ii. Audit Observation: It has been observed that the system has been customized by PWC to fulfill the needs of Public Procurement Act of Nepal. The issues lodged by users, Public entities, banks, or changes made by government are reviewed by the IT team and after final discussion and approval from responsible personnel updates/ changes/ review is made in the system. No fixed timeframe is available for review of the system. Such issues are not cited out in strategic plan of PPMO as there is no separate IT plan and IT strategic Plan. They do not have a separate policy for ensuring value for money, risk minimization and appropriate system has been ensured. Worldwide methodology for data security, network security, access to data, etc is being followed. Review of the implemented system has been done by a outsourced company ESC Private Limited in 2017 and made some recommendations along with gap analysis some of which are yet to be implemented.

iii. Risk: System is at risk whether the features of customized version are used properly or not.

iv. Impact: Value for money, data integrity cannot be assured.

v. Recommendation: It is recommended to review the system on a regular basis. Also, the review report should ensure that the customized features in the software are fulfilling the requirements of Public Procurement Act of Nepal. The system review should report on the reasons for failure of users to make the full use of E-GP software for e-procurement process.

vi. Management Response:

2.4.3 Senior Management Approval

i. Criteria: High level management approval should be obtained and evidenced for new systems development and changes to existing systems. User department and IT department approval should also be obtained

ii. Audit Observation: It has been observed that documentation for change request as well as system development is available along with the process to be followed to making such changes/ up gradation in the system. The changes to be made are first tested in the test server and the results are recorded. After that, change request is made by the administrator to the IT department's Computer Engineer for recommendation which is finally approved by IT Director. For Instance :

CMNo: S02-01 Date: 7th June, 2018

Table 8: Senior Management Approval Sample list

Change Request Type	Test Result	Remarks	Deployment date	Deployment assigned to (redacted)
Re-enable SLAVE replication	Replication from 10 to 60 started (One Time Replication)	Check Command below to restart; to enable auto replication, job will be set up	7th June, 2018	

The request is initiated by (redacted). Test is also performed by them and sent for recommendation to (redacted) (Computer Engineer) and approved by Manish B. (IT Director). There is no process of periodic review of changes made in the system.

iii. Risk : There is no automatic change tracker available so changes made in the application/ software cannot be tracked automatically.

iv. Impact: In case any changes made are outdated or not required then due to lack of periodic review mechanism they cannot be identified.

v. Recommendation: It is recommended to install a automatic tracker and arrange a system of periodic review of such changes made.

vi. Management response:

2.4.4 Segregation of Environments

i. Criteria: The client should maintain separate environments (preferably both logical and physical) for the development, modification, testing and migration of data for IT solutions that are separate from the live operating environment. Access to the test environment should be strictly regulated through the use of passwords. Staff responsible for developments should be separate from those responsible for testing.

ii. Audit Observation: It has been observed that the outsourced consultants make the testing of all the changes/ enhancement/ modification as well development in the server (SIT server-test server). One who does the testing in the server makes the development in the system. Till date no migration has been done. Different username and passwords are available for test server as well as live server. However, there is no system that the one who does testing in test server is not allowed to apply the change in the LIVE server.

For instance, in the above change request form, changes in the test server have been tested by (redacted) and (redacted) and also implemented in LIVE Server by them.

iii. Risk: There is a risk of fraud, unauthorized changes can be made in the system as segregation of duties is not done.

iv. Impact: System may be prone to attacks, confidential data may be leaked.

v. Recommendation: It is recommended to make a clear segregation of duties among the outsourced staffs to ensure the system, network and database is completely secured.

vi. Management Response:

2.4.5 User Acceptance Tests

i. Criteria: The client should establish procedures incorporating user acceptance of new developments that ensure that end users are active involved in the test process and formally sign off their acceptance.

ii. Audit Observation: It has been observed that for implementation of Phase I and Phase II no UAT are available. Presently, the request for change/ software development made by PPMO to outsourced third party (DG Market PVT ltd) is maintained through UAT. This is presently in testing phase and yet to be implemented so no chances of follow ups on results of UAT.

iii. Risk: Due to lack of UAT document, we cannot ensure that the objectives for implementation of Phase I and II of E-GP system has been achieved or not.

iv. Impact: Confirmation whether all the tests required for implementation of software were conducted or not cannot be obtained.

v. Recommendation: It is recommended to approve the format of UAT now onwards from the management and record all the changes to be made in the system.
vi. Management Response:

2.4.6 Change Management

i. Criteria: The client should have formal procedures that detail its policy towards both systems acquisition and change management. These should include established procedures for emergency system modifications.
ii. Audit Observation: It has been observed that In case of any kind of changes are to be made in the system, those are done though approval from IT director. For acquisition, need analysis is done then budget is available or not is assessed. The PPMO secretary discusses the same with the IT team and then gives the green signal to acquire the system if he finds it feasible. Procedures have not been defined for change management, system acquisition as well as for emergency system modification.
iii. Risk: There is a risk of fraud, unauthorized changes can be made in the system as segregation of duties is not done.
iv. Impact: System may be prone to attacks, confidential data may be leaked.
v. Recommendation: It is recommended to define a procedure for change management, system acquisition and response to emergency modifications.
vi. Management Response:

2.4.7 Warranties

i. Criteria: Management should ensure that appropriate warranty agreements are in place for hardware and software purchase.
ii. Audit Observation: It has been observed that at the time of procurement of hardware and software, existence of warranty is assured. The goods procured should meet the specification criteria cited by PPMO.
iii. Risk: There is a risk that after certain period of time hardware/ software runs out of warranty after which its operating cost will be increased. Also, Cost-Benefit Analysis of such assets is not done during their operation.
iv. Impact: Cost to the organization may increase.
v. Recommendation: It is recommended to assure that all the assets procured have a certain specified warranty period. After the expiry of the warranty period, cost benefit analysis of such assets needs to be done and informed to the management.
vi. Management Response:

2.4.8 Post Implementation Review

i. Criteria: Post implementation reviews and follow up should be performed for all developments and changes. The extent of analysis and testing should be increased where system modifications are made in an emergency.

ii. Audit Observation: It has been observed that there is no schedule for post implementation review and follow up. The reviews are done after the issues are lodged.
iii. Risk: There is a risk that due to non-availability of periodic review system post implementation, the incidents, bugs, problems faced by the may remain unknown. Impact: Smooth operation of the System may be hampered, whether the implementation made in the system was correct or not cannot be ensured.
iv. Recommendation: It is recommended to enact a Pre-active assessment methodology to identify the issues prior to their generation/ involvement in the system.
v. Management response:

2.5 System Performance

2.5.1 Directives- Registration

i. Criteria: Whether ministries/departments/central level offices are registered with system administrator (PPMO) for the purpose of system operations? (Section 6 of Directives)
ii. Audit Observation: It has been observed that all the ministries/ department/ central level offices are registered with PPMO. They sent a application to PPMO in the format prescribed by PPMO for registration. They are provided with admin user id and password through email after which they can create three types of users: creator; approver and reviewer. Till date 1634 Public entities have been registered with PPMO. Sec 7 (4) of the directives states that states, district and local level government offices should contact their related central level offices/department/ ministries to get registered with PPMO for getting registered. However, it has been observed that such organizations directly contact PPMO without getting confirmation from their central offices for registration. For instance, Nepal Rastra Bank Dhangadhi, Armed Police Force, Morang no.3, etc.
iii. Risk: There is a risk that the local level/ district level offices are bypassing their related department/ ministries/ central level offices to get registered with PPMO.
iv. Impact: Control over the local level, district level organization is at risk.
v. Recommendation: It is recommended that PPMO registers the local level/state level offices only after they get confirmation from their related ministries/ departments/ central level offices.
vi. Management Response:

2.5.2 Directives- User Registration

i. Criteria: Whether the system operator ministries, departments, central level offices and head office of banks have provided users' registration for running system to state, district or local level entities that are interested to operate online public procurement

transactions? (Directive no 7/8). Whether tender notice and documents are published online? (Directive no 13).

ii. Audit Observation: It has been observed that PPMO gives access to central level offices/ provinces who then in turn provides access to the local level offices falling under their regime. Directive no.7(4) states that provinces, districts and local level offices should get registered from their central offices. But the practice is not being followed. Such entities are directly being registered with PPMO. All the tender notices and documents are published online in EGP and also in national daily.

iii. Risk: There is a risk that the local level/ district level offices are bypassing their related department/ ministries/ central level offices to get registered with PPMO.

iv. Impact: Control over the local level, district level organization is at risk.

v. Recommendation: It is recommended that PPMO registers the local level/state level offices only after they get confirmation from their related ministries/ departments/ central level offices.

vi. Management Response:

2.5.3 Directives- Tender Registration

i. Criteria: Whether the bidders have registered tenders through online? (Directive no 15)

ii. Audit Observation: It has been observed that all the eligible bidders have registered tenders through online as well as uploadable format. Both online mode and uploadable mode are used. Most of the bidders fill their tenders in a excel format and upload them online.

iii. Risk: There is a risk that the inbuilt features of E-GP is not used such as filling up the BOQ, tender details, etc. Users upload the excel sheet in their own format which is accepted by the system.

iv. Impact: The customized features are not used completely. No uniformity in the format.

v. Recommendation: It is recommended that the excel format should be specified by the system itself and shall be uniform for bidder.

vi. Management Response:

2.5.4 Directives- Tender Evaluation

i. Criteria: Whether the evaluations of tenders are done through online system? (Directive no 8). Whether the letter of intent of tenders, review of decisions and approvals are done through the system? (Directive no 23). Whether the approvals of advance payments, advances, running bills, final bill payments and liquidated damage payments are granted through online? (Section 28 of Directive no 28).

ii. Audit Observation: It has been observed that it is optional to carry out evaluation of tenders through online. There is an in-built feature in the system to issue LOI, LOA through EGP. But it is not used completely. There is a system to update approval of

advance payment, advances, running bills, final bill payment and liquidated damage payment in the system. But only few PEs have used the feature.
For Instance,

Table 9: Sample List of Bids

Category of tenders	Number of Tenders	Tenders Cancelled	Tenders Uploaded in excel format	Two Envelope Procedure	Single Envelope Procedure
Consultancy	152	0	0	0	152
Goods Procurement	1985	34	1287	0	664
Works	5159	27	1231	1818	2083
Total	7296	61	2518	1818	2899

From the above chart we can see that total 7296 tenders were applied out of which 61 were cancelled. 2518 valid tenders were submitted by uploading in excel format. Technical evaluation was only done for 2899 tenders after which manual process was followed to complete the process and for 1818 tenders both technical as well as financial evaluation was done.

iii. Risk: Complete features of E-GP post evaluation such as awarding of tender, letter of interest, advance payment, running bill payment, etc has not been used.

iv. Impact: Feasibility of E-GP cannot be assured.

v. Recommendation: It is recommended to make compulsory to use all the features of E-GP for its effectiveness.

vi. Management Response:

2.5.5 Directives- Section 35 (5)

i. Criteria: Section 35(5) of e-GP directives requires that all the purchase/procurement procedures should be done in accordance with e-GP directives. Such disclosure shall be compulsorily be made in the procurement notice document available in online portal as well as data sheet related to bolpatra. Also, Section 35 states that government offices shall compulsorily use e-GP in case the procurement exceeds the following threshold:

- In case of Consultancy: Rs. 2 million
- In case of Procurement of Goods : Rs. 6 million
- In case of Construction works: Rs. 20 million

ii. Audit Observation: It has been observed that "It's compulsory to use e-GP for procurement exceeding the above cited threshold has not been cited in online procurement notice as well as data sheet related to Bolpatra. The following instances has been observed:

Table 10: Sample of Bids Published Online

Name of Organization	First date of Publication of Notice	Job Description	Bid Security Amount	Estimated Amount	Contract No
Department of Local Infrastructure (DoLI)	2nd October, 2018	Supply and delivery of 13,26,32, 36 and 40mm dia Wires Ropes	55,000 (USD)(around 2.5%)	22,000,000.00(USD)	ICB/TB/WR/01-2018/19
Kankai Municipality, Jhapa	2075-05-14	Hydraulic Excavator (Not less than 165 HP)	275,000.00(NRs.) (around 2.5%)	Nrs. 11,000,000.00	Kankai/01/075-76

As both the above cited bids exceeds the threshold limit, bids should be opened electronically as per section 35(3) of e-GP directives which has been cited in point no. 6 of bid document of DoLI. However, the same has not been specified in bid document of Kankai Municipality. Point 7 of bid document of Kankai Municipality states that "bids shall be opened in presence of bidders representative". Hence, the e-GP directive has not been complied.

iii. Risk: Assessment of all the bid documents of government offices to whom section 35 is applicable cannot be done. Hence, it cannot be assured that e-GP directive has been complied or not.

iv. Impact: e-GP directive non compliance, lack of knowledge and training among the users of e-GP about the compulsory clauses of directives to be followed.

v. Recommendation: It is recommended to train the public entities about the importance of directives and actions that can be taken by the regulatory body in case of non-compliance. Also, there should be a auto check mechanism in built in e-GP to assure that the directives have been complied with.

vi. Management Response:

Appendix 1 : List of Acronyms

- AMC-Annual Maintenance Cost
- ASOSAI- Asian Organization of Supreme Audit Institutions
- BCP- Business Continuity Plan
- DOIT- Department of Information Technology
- DoLI- Department of Local Infrastructure
- DRP- Disaster Recovery Plan
- DTTILLP- Deloitte Touche Tohmatsu India LLP
- E-GP- Electronic Government procurement
- GEA- Government Enterprise Architecture
- GIDC- Government Integrated Data Centre
- HTTPs- Hypertext Transfer Protocol secure
- ICT- Information and Communication Technology
- INTOSAI- International Organization of Supreme Audit Institutions
- IT- Information Technology
- LOA- Letter of Authorization
- LOI- Letter of Intent
- OandM- Operation and Maintenance
- OTP- One Time Password
- PE- Public Entity
- PPA- Public Procurement Act
- PPMIS- Public Procurement Management Information System
- PPMO-Public Procurement Monitoring office
- PPR- Public Procurement Rules
- PWC- Price Waterhouse Coopers
- SIEM-Security Information and event Management
- TOR- Terms of Reference
- UAT-User Acceptance Test
- USB- Universal Serial Bus
- VAPT-Vulnerability Assessment and Penetration testing

Appendix-2: Glossary

- **AMC-Annual Maintenance Cost** - these are the costs associated with ensuring that IT assets will be maintained.
- **ASOSAI- Asian Organization of Supreme Audit Institutions -** forum and workshop for Asian Supreme Audit Institutions.
- **BCP- Business Continuity Plan–** this is the record of the creation of systems of prevention and recovery to mitigate against risks to an organization.
- **DOIT- Department of Information Technology**
- **DoLI- Department of Local Infrastructure**
- **DTTILLP- Deloitte Touche Tohmatsu India LLP**– a consulting firm
- **DRP- Disaster Recovery Plan–** this is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster
- **E-GP- Electronic Government procurement** – software for public sector procurement intended to increase transparency and objectivity in the procurement process.
- **GEA- Government Enterprise Architecture–** this is the design of the optimal placement of resources in the IT environment for the support of the business function
- **GIDC- Government Integrated Data Centre–** a data centre is a facility used to house computer systems; this provides back-up and safeguarding of data for the public sector.
- **HTTPs- Hypertext Transfer Protocol secure**Protocols are the language that computers use to communicate to each other; this protocol allows computers connected to each other to communicate by use of hypertext links embedded in documents or web pages.
- **ICT- Information and Communication Technology –** relates to computer and telephony technology.
- **INTOSAI- International Organization of Supreme Audit Institutions-** forum and workshop for International Supreme Audit Institutions.
- **IT- Information Technology –** relates to computer data processing and management.
- **LOA- Letter of Authorization**
- **LOI- Letter of Intent**
- **OandM- Operation and Maintenance**
- **OTP- One Time Password**– a password issued for one time use.
- **PE- Public Entity**
- **PPA- Public Procurement Act**
- **PPR- Public Procurement Rules**
- **PPMIS- Public Procurement Management Information System**
- **PPMO-Public Procurement Monitoring office**
- **PWC- Price Waterhouse Coopers**– a consulting firm
- **SIEM-Security Information and Event Management**– in the field of computer security SIEM are software products and services which combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.
- **TOR- Terms of Reference**

- **UAT-User Acceptance Test–** before a change, usually a major change, is made to an IT system it will be tested on users first to ensure that it is appropriate; results will be recorded, retained and communicated to management before they approve changes.
- **USB- Universal Serial Bus -** is an industry standard that establishes specifications for cables, connectors and protocols for connection, communication and power supply between personal computers and their peripheral devices.
- **VAPT-Vulnerability Assessment and Penetration testing -** this is a hacking attack by an ethical hacker designed to inform management of vulnerabilities and security weaknesses in the network or applications.

Appendix 3- Action Plan Timetable –e-GP

Key

- Red denotes High Risk, prompt action should be taken.
- Yellow denotes Medium Risk. Action should be taken but it is not so urgent as to be required immediately.
- Green denotes Low Risk. Action should be taken but this will be on a cost / benefit basis and when capacity allows.

*ASAP = As soon as possible

E-GP

Reference	Action Point	Who to be done by	When it needs to be done by *	Completed by who and date completed
	GOVERNANCE			
2.1.2 - Policy	**It is recommended to draft, finalize and approve the following policy documents so that a clear picture can be formed to assign responsibilities to relevant personnel.** **a. Information Technology Policy** **b. Security Policy** **c. Business Continuity Plan** **d. Disaster Recovery Plan** **e. Hardware Policy** **f. Software Policy** **g. Policy for confidentiality of Data** **h. Backup Policy** **i. Remote Access Policy** **j. Change Management Policy** **k. ICT Training Policy** **l. Third Party Usage Policy**	**IT Director**	**ASAP**	
2.1.3 - Strategy	**PPMO should have a strategic plan for IT and in particular E-GP; this should be supported, to ensure delivery by an operational annual IT plan.**	**IT Director**	**ASAP**	
2.1.4 Third	**It is of great concern that the World**	**IT**	**ASAP**	

Party Assurance	**Bank / Deloitte report on e-GP has had so little action taken on its recommendations, over 6 months after it was issued. Immediate action must be taken to deal with its recommendations; particularly those of a more serious nature. Further to thisPPMO should build their in-house capacity to ensure control risks are minimised and reduce their dependence on third parties.**	**Director**		
2.1.5 -Human Resources	**PPMO should hire the required number of IT staff; particularly for the areas where control risks are the greatest; particularly the posts of Network Administrator, System Administrator and Database Administrator.**	**HR and IT Directors**	**ASAP**	
2.1.6 - Training	**There is currently no training plan, nor is staff training taking place. A training plan should be developed by IT management and supported by the Board in the annual budget.This should cover both internal and external training. Ensuring delivery of IT training should be built into the annual IT plan and strategy and be one of the objectives of the IT Director forming part of the annual appraisal of that post.**	**Senior Management / IT Director**	**For Jan 2019**	
2.1.8 - Helpdesk	**It is recommended to enact a 24*7 helpdesk and monitoring system. A role of Helpdesk Manager should be given to a current staff member. All reports to the helpdesk should be recorded and escalated to management as appropriate. Monthly a report should go to management highlighting issues raised for governance.**	**Senior Management / IT Director**	**ASAP**	
2.1.1 – Governance	**Form a separate ICT steering committee to address eGP issues. This should meet on a regular basis, probably monthly. This role could also be added to the scope of work of the existing Technical Committee.**	**Senior Mgt / IT Director**	**ASAP**	
2.1.7 - Compliance	**Security policy should include a minimum number of penetration tests to be conducted annually; the minimum should be 2 annually but for a significant**	**IT Director /Helpdesk**	**ASAP**	

	system possibly more depending on managements perception of risk. A system should be put in place to ensure the penetration tests take place and that any actions arising from it are monitored to ensure prompt performance. the minimum should be 2 penetration tests. Senior Management must implement a review to assess what further compliance work should be undertaken by e-GP specialists; this should include consideration of the appropriate and prompt upgrades and patching of e-GP.	Manager		
LOGICAL ACCESS SECURITY				
2.2.2 - Passwords	It is an urgent action to ensure that there is a password policy and that key activities are implemented; it is recommended that this follows the guidance provided by the National Cyber Security Centre (UK).(https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach)	IT Director / System Administrator	ASAP	
2.2.3 – Log in / Log Out	A log in/out policy should be included in the security policy. Immediate action is required to specify log in attempts/ log out timing and an automated email to the user about the system being logged out after a certain number of failed attempts or logged out after a certain time frame etc.	IT Director / System Administrator	ASAP	
2.2.9 – Anti-virus	During the audit we were unable to obtain a clear explanation why e-GP does not have anti-virus installed. We consider that the use of the Oracle security feature without anti-virus on the servers is unlikely to give an acceptable level of protection. It is recommended to install antivirus in the e-GP system.	IT Director	ASAP	
2.2.10 - Firewall	It is recommended that the IT Department formulate a firewall policy and that this is approved by senior management; this must include allocation of responsibility and maintenance of the firewall. Review of	IT Director / Senior Management	ASAP	

	the current firewall settings should form a part of an Internal Audit / DOIT review.			
2.2.1 – Logical Access Security Procedures	Assign responsibility for ensuring that security procedures in the User Manual are being followed. Active use of security procedures should be monitored and reported on regularly to the IT Director. A first security procedure review should be performed by internal audit / DOIT to establish a baseline.	IT Director / Systems Administrator	For Jan 2019	
2.2.4 – Segregation of Users	To ensure security PPMO must review their IT Operations on a regular, ongoing basis. Clear assignment of authority and responsibility over e-GP operations must be set and ensure segregation of duties.	IT Director / Systems Administrator	By Jan 2019	
2.2.5 – Audit Logs and Monitoring	Audit Log policy should be included in the PPMO IT security policy. Audit logs should be actively monitored on a regular basis to strengthen system security. This action should form a group of regular checks that are reported to the IT Director. Any issues identified and actions taken should be recorded and reported as appropriate.	System Administrator	ASAP	
2.2.7 - Administrators	It is recommended to review the access logs and access rights provided to system administrators and super users on a regular basis. This should be reported to the IT Director for appropriate action.	IT Director.	Monthly	
2.2.8 – Application Controls	PPMO should have a system map of e-GP clearly defining the controls established over the data and application controls to assist with setting strategic and operational planning. This will help to identify areas of risk and opportunity. This should be updated on at least an annual basis or after any major system changes.	IT Director	In time to feed into the annual and strategic planning process.	
2.2.11 – Database Security	Ideally the post of database administrator should not be out-sourced, an in-house database administrator would reduce control risks. The activities of the Database	IT Director / Database Administ	ASAP	

	Administrator should be reviewed on a regular basis by the IT Director reviewing the relevant audit logs.	rator		
2.2.6 –Starters and Leavers	Starters and Leaversadministration methodology for promptly dealing with IT user access rights should be documented in the starters / leavers policy held by HR and managed and monitored by the Network administrator.	IT and HR Director. Network Administrator	By the end of the first quarter of 2019	
PHYSICAL ACCESS SECURITY				
2.3.2 – Physical Security	The IT Department must take immediate action to secure access to server rooms by ensuring they are locked. Visitor logs to the data centre must be maintained and reviewed for unusual access.	IT Director / Network Administrator	ASAP	
2.3.5 – Third Parties	The IT Department should maintain a record of all third parties involved with the eGPsystem. It should be ensured that service level agreements are in place with all appropriate third parties. There should also be a review of third party contracts, process and procedures to ensure that contracts ensure that third parties have to adhere to PPMO's standards and also that PPMO has rights of audit. Further PPMO must seek to ensure that key administrator roles in the e-GP system are filled by internal staff.	IT Director / Network Administrator	ASAP	
2.3.8 – Security Logs	Implement a system to ensure security logs are reviewed on a regular basis and unusual incidents acted upon immediately and reported to management needs to be designed and implemented. Responsibility for this should be clearly assigned by the IT Director. Management; there should also be a review to assess whether they need a SYSLOG server.	IT Director / Systems Administrator	ASAP	
2.3.9 – Assets Register	The asset register information needs to include full information about the life cycle of assets including warranty cost and expiry information; management should consider using an asset tracker.	IT Director / Network Administ	In time for the next asset purchase budgeting	

	Once this exercise has been completed a review reporting to the IT Director should be conducting to assess aging of warranties and assets.	rator	cycle.	
2.3.11 – BCP and DRP	PPMO must put in place business and disaster recovery plans. These should be tested annually.	IT Director / Senior Management	ASAP	
2.3.1 Physical Access Security - Procedures	It is recommended that the IT Director should formulate a policy for physical security of the assets and this should be approved by senior management. Physical Security arrangements should be reviewed by Internal Audit / DOIT and an action plan with timetable for strengthening physical security prepared, actioned and monitored by the IT Department.	IT Director / Senior Management	In time to feed into policy development and approval.	
2.3.3 - Monitoring	Regular review of the system and of the data content must be undertaken to identify any unauthorised files and data. This monitoring check should be reported to the IT Director. This should be included insecurity policy. An initial review may be undertaken as part of an internal audit / DOIT review	IT Director / Network Administrator	Within the first quarter of 2019	
2.3.6 - Interfaces	The IT Department must put into place a review mechanism to ensure that data has transferred correctly between interfaces.	IT Director / System Administrator	ASAP	
2.3.10 – Data Disposal	Management should implement a process to identify unwanted data and information in the database and ensure disposal against best practice methodology. Management should also review to assess whether data storage space can be increased.	IT Director / System Administrator	By the end of the first quarter of 2019	
2.3.4 – Back Up	The IT Director should formulate a separate Back Up Policy to be approved by senior management; this will form part of the policy work.	IT Director	In time to feed into policy development and approval as at 2.1.2	
2.3.7 –	Management should write to GIDC to	IT	First quarter	

Environmental Defences	**obtain assurance about the environmental sufficiency of the infrastructure of GIDC**	**Director**	**2019**	
CHANGE AND SYSTEM MANAGEMENT				
2.4.2 – Customised Bespoke / IT System	**It is recommended to review the system on a regular basis. Also, the review report should ensure that the customized features in the software are fulfilling the requirements of Public Procurement Act of Nepal. The system review should report on the reasons for failure of users to make the full use of E-GP software for e-procurement process. Additionally it is not clear that patching and upgrades to e-GP are happening on a timely basis. Management should review and implement a system to ensure the timely installation of patches and upgrades required for e-GP.**	**IT Director / Systems Administrator**	**ASAP**	
2.4.7 Warranties	**Ensure that all key assets procured for the e-GP network have a remaining warranty period. After the expiry of the warranty period, cost benefit analysis of renewing the warranties against renewing the assets needs to be done and reported to management for approval and action.**	**IT Director / Network Administrator**	**In time for the next asset purchase budgeting cycle.**	
2.4.3– Senior Management Approval of IT Changes	**It is recommended to install an automatic change management tracker and arrange a system of periodic review by the IT Director to ensure changes are made and approved at a sufficiently senior level.**	**IT Director**	**By the end of the first quarter of 2019**	
2.4.5 – User Acceptance Tests	**UAT formats and results of UAT testing must be approved by senior management. These approvals should be retained with records of the UAT for all significant system developments.**	**IT Director**	**By the end of the first quarter of 2019**	
2.4.6 – Change Management	**Management should put in place a formal policy and procedure for change management, system acquisition and response to emergency modifications**	**IT Director**	**In time to feed into policy development and approval as at 2.1.2**	
2.4.1 – Central Records	**It is recommended to implement a system to ensure that DOIT is informed**	**IT Director**	**By the end of the first**	

	of new software being used by PPMO.		quarter 2019	
2.4.4 – Segregation of Environment	Segregation of duties among the staff working on testing and development of e-GP should be formally documented in the e-GP user manual	IT Director	By the end of the first quarter of 2019	
2.4.8 –Post Implementation Review	Formal procedures for post implementation reviews should be built into IT change management policy.	IT Director	In time to feed into policy development and approval as at 2.1.2	
COMPLIANCE WITH DIRECTIVES				
2.5.4 – Directive 8,23, 28 – Use of the EgP for various stages of the bidding process	It is recommended to make it compulsory to use all the features of E-GP, at the moment only compulsory features of the system are used.	IT Director / System Administrator	ASAP	
2.5.1 – Directive 6 – Registration with System Administrator (PPMO)	It is recommended that PPMO registers the local level/state level offices only after they get confirmation from their related ministries/ departments/ central level offices.	IT Director / System Administrator	By the end of the first quarter of 2019	
2.5.2 –Directive 13 - Registration with state, district or local level entities	It is recommended that PPMO registers the local level/state level offices only after they get confirmation from their related ministries/ departments/ central level offices.	IT Director / System Administrator	By the end of the first quarter of 2019	
2.5.3 – Directive 15 - Bidders registration of tenders online	An update should be done by the IT unit to ensure that only a standardised excel format built into e-GP should be specified by the system itself to ensure uniformity of tenders.	IT Director / System Administrator	By the end of the first quarter of 2019	
2.5.5 – Directive 35 – Compliance with e-GP Directives	It is recommended to train the public entities about the importance of directives and actions that can be taken by the regulatory body in case of non-compliance. Also, there should be an auto check mechanism in built in e-GP to assure that the directives have been complied with.	IT Director / System Administrator	By the end of the first quarter of 2019	