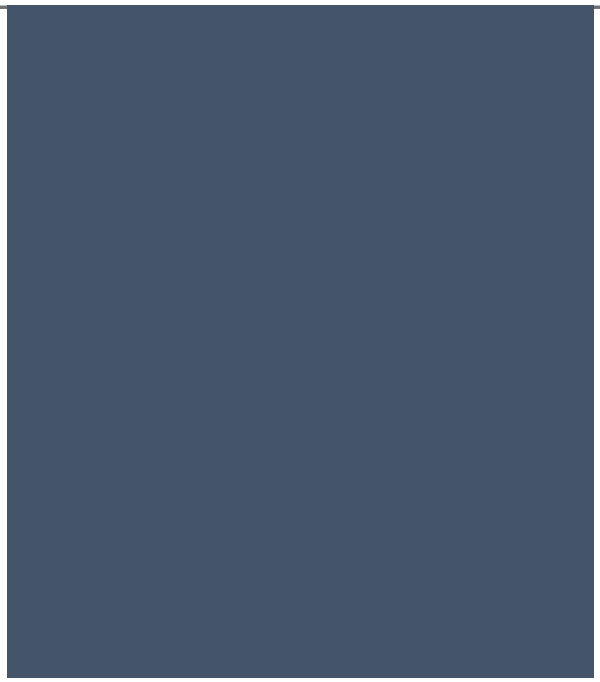


PKI RCA Audit & Vulnerability Assessment / Penetration Testing (VAPT) Proposal

For:

Office of Controller of Certification (OCC)

By:

KB Chitracar & Co.

KB
Chitracar & Co
Chartered Accountants

ALLIOTT GROUP
A Worldwide Allince of Independent Account, Law and Consulting Firms

Date: 12th March 2020

To
Office of Controller of Certification (OCC)
Anamnagar, Kathmandu
Nepal

Subject: PKI RCA Audit and Vulnerability Assessment/Penetration Testing (VAPT) of PKI Root CA

Respected Sir/ Madam,

We are pleased to present our proposal for your review. We have a better understanding of the Information System Audit requirements.

As one of the leading Chartered Accountancy firms in Nepal, KB Chitracar & Co. has been at the forefront in execution of a wide array of financial projects for individuals, government, and large corporations.

Thank you for the opportunity to participate in this bid.

Sincerely,

_____ _____

CA. Manish Raj Uprety
KB Chitracar & Co.
manish@kbc-ca.com.np
+977 9851026986
+977 01 5261011

Table of Contents

KB Chitracar & Co. Company Profile

KB Chitracar & Co (KBC) is a firm of long standing in accounting practice in Nepal. Since its establishment in 1970 it has been providing quality professional services to the public and private sector for the last four and half decades. The firm was founded by Komal Chitracar who is the senior and managing partner of the firm.

KBC is a full member of Alliott Group which is a worldwide alliance of independent accounting, law and consulting firms. With more than 200 member firms in some 68 countries, the group meets the local and cross-border needs of its members and their clients.

KBC has a very scrupulous policy in accepting engagements and has a strong risk control system to ensure independence of audit. Truth and professional integrity associated with due care and diligence are its cardinal principles of service delivery. KBC takes professional ethics very seriously in practice. KBC also provides bookkeeping services as well as various advisory and other professional services as per clients' requirements.

KBC has long and wide experience of providing professional services including accounting, audit & assurance, taxation as well as advisory services to a large number of clients engaged in the various economic activities in public, private as well as in social sectors. KBC's client profile includes financial and commercial institutions and the various types of for profit and not - for profit organizations.

KBC has been providing services to several international donors, international lending agencies and international NGOs to audit or to carry out agreed- upon procedures of fund transfers to local agencies or organizations for the various programs and projects being implemented in Nepal.

KBC is enlisted in the panel of auditors qualified to conduct audit for USAID and has been providing such service continually since 1990 to audit utilization of US grants to the government and local NGOs for the various types of project activities in Nepal.

Affiliations

KB Chitracar & Co (KBC) is the full member of Alliott Group, an international group of accounting, legal and consultancy firms. Extending throughout Europe, Africa, the Middle East, North America, Latin America and Asia Pacific, Alliott Group has merged the reality of global ambition with the need for truly local coverage. KBC was the associated firm of Coopers & Lybrand since 1990 till its international merger. KBC has been working since 2002 with the membership of Institute of Chartered Accountants of Nepal. The institute is an autonomous body authorized to undertake accounting profession in Nepal.

Human Resources

We believe in a team work and work with coordination and transparency. Our team comprises of the likeminded professionals with the varied experience and skills and is committed to providing a high standard of service. We have a proven track record of delivering quality services in due time with meeting our client's empathy. Our staffs are well versed in managing complex and high value assignments. Personal development is important to us and the future success of the firm. We encourage everyone to develop themselves and offer ongoing training to both professional and non-professional staff.

Our human resource strengths comprise of well trained professional staff who have versatile exposure with large number of enterprises in the various types of business and industry as well as social, development and charitable activities. We have networking arrangement with other chartered accountants, management experts, IT specialists, engineers, marketing experts, economists, statisticians, legal advisors and operation research analysts as resource persons who are readily available on a call basis. The arrangement enables the firm to handle assignments of varied size and nature as well as to deliver the services in due time at a short call.

Our Services

1. Audit and Assurance Services

We maintain the highest level of professionalism and quality control in the delivery of our audit and assurance services. We adhere to the principles of independence, integrity and due professional care in every stages of our assignment. Our audit and assurance services include:

- Statutory Audits
- Audits and Review Engagements
- Compliance and Special Purpose Audits (Audit or Agreed- upon procedures on behalf of donors of projects with international funding, Performance audit of projects)
- Internal Control System Study and Evaluation
- Information System Audit

2. Accounting Solutions

We provide accounting solutions to our clients and help manage the complexity of their business. We provide our expertise to solve the financial and business concerns of our clients.

- Reviewing, Designing and Implementation of Accounting Systems
- Book Keeping Services
- Payroll Accounting

3. Business Advisory and Consulting Services

We help business achieve its growth potential. We offer business advisory and other consulting services to our clients to help them do the better business. Our expertise is in the following areas:

- Financial Analysis, Business Diagnosis and Due Diligence
- HR Development (Training, Developing personnel policy and job description, Compensation Survey, Recruitment, Outsourcing), workshops, seminars and counseling
- Project appraisals
- Feasibility Study of the Projects and Ventures
- Investment Analyses and Project Reports
- Setting up new business
- FDI consulting
- IFRS implementation and transitioning
- Financial review and monitoring
- System Development

4. Tax and Legal

Our expert team consisting of the chartered accountants and lawyers provide tax and legal services to national as well as international clients. Our experts will help you take the legitimate tax advantages through proper tax planning.

- Tax advice and services to local and foreign clients
- Formation of companies
- Company secretarial services

Project Details

Information Systems AuditMethodology and Work Process

Audit methodology

There are various methodologies (approaches) for conducting IS Audit which are listed below for reference. Among these below listed methodologies auditor is required to select one method and agree with Auditee so that best audit is conducted for benefit of organization. This selected method helps to obtain sufficient appropriate audit evidence to form reasonable conclusions and on the same conclusions auditor base his opinion. Different approaches to conduct the audit are as follows:

- Systems-based Auditing Method
- Directional Auditing Method
- Risk-based Auditing Method

Risk – Based Auditing Method

Risk is the combination of the probability of an event and its consequences which may negatively impact the assets, processes or objectives of a specific business or organization. Risk analysis helps to identify risks and vulnerabilities so the IS auditor can determine the controls needed to mitigate those risk. The risk analysis is based upon reviewing:

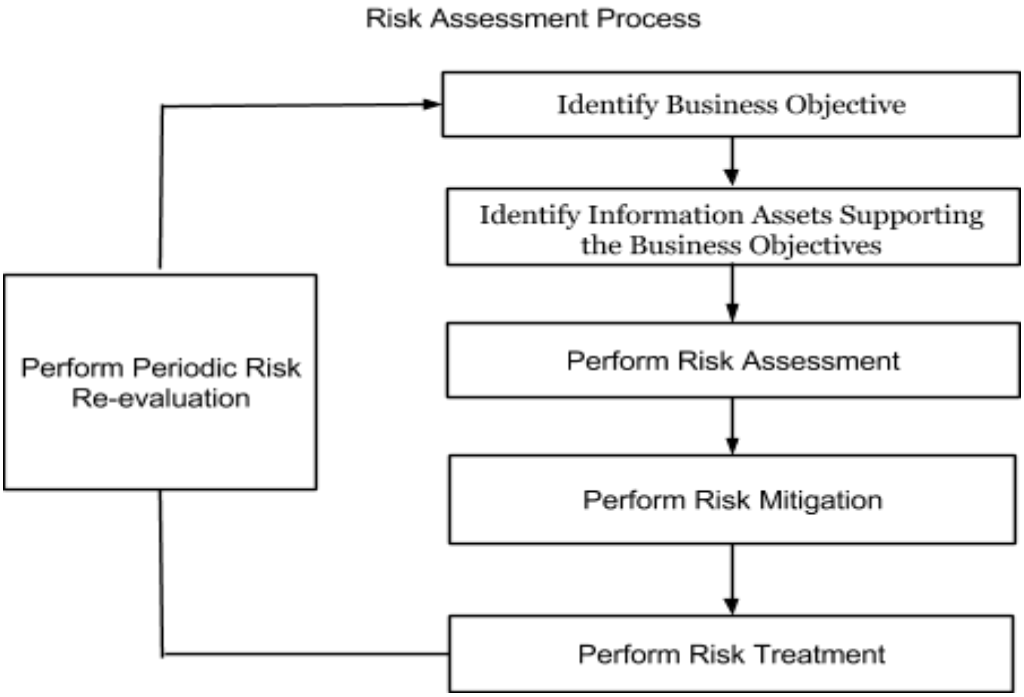
1. The purpose and nature of business, environment in which the business operates.
2. The dependency on the technology to process and deliver business information
3. The business risk of using IT and how it impacts the achievement of the business goals and objectives

The process of risk analysis will help our clients to

1. Integrate the management of IT risks into the overall enterprise risk management of the organization
2. Make well-informed decision about the extent of the risk, the risk appetite and the risk tolerance of the enterprise
3. Understand how to respond to the risk

The assessment of countermeasure will be performed through a cost-benefit as well as high criticality based analysis where controls to mitigate risks are selected to reduce risks to a level acceptable to management, this analysis process may be based on any of the following:

1. The cost of the control compared to the benefit of minimizing the risk
2. Management's appetite for risk (the level of residual risk that management is prepared to accept)
3. Preferred risk-reduction methods (terminate the risk, minimize probability of occurrence, minimize impact, transfer the risk via insurance)



A single Risk Assessment process consists of identifying threats, vulnerability, its exploitation probability and calculation of its impact. A single Risk Mitigation process consists of mapping risks with control in place. A single Risk Treatment process consists of treating significant risks which are not mitigated by existing controls. Each of the risks identified in the risk assessment needs to be treated. Possible risk response options include:

1. **Risk mitigation**: applying appropriate controls to reduce the risks
2. **Risk acceptance**: Knowingly and objectively not taking action, providing the risk clearly satisfies the organizations policy and criteria for risk acceptance
3. **Risk avoidance:** Avoiding risks by not allowing actions that would case the risks to occur
4. **Risk transfer:** Transferring the associated risks to other parties, e.g. insurers or suppliers

Audit Phases

Audit phase	Sub-phase
PHASE I: Planning the audit Engagement	Audit subject
	Audit objective
	Audit scope
PHASE II: Audit planning	Pre-audit planning
PHASE III: Executing the audit plan	Audit procedures and steps for data gathering
PHASE IV: Monitor project activity	Procedures for evaluating the test or review results.
	Procedures for communication with management
	Audit report preparation

This process collects and evaluate evidence to determine whether the information systems and related resources adequately safeguard assets, maintain data and system integrity and availability, provide relevant and reliable information, achieve organizational goals effectively, consume resources efficiently, and have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented, or detected and corrected, in a timely manner. Compliance with NRB and progress of prior audit controls are main issue of this audit. Financial audits, operational audits, can come in-between while conducting IS audit.

Gap Analysis

A gap analysis can be defined as the determination of the difference between current knowledge/practices (what we are doing) and current Evidence Based Practices (what we should be doing). Gaps can occur in knowledge, skills or practice, infrastructure used, policies implemented, process work flow, communication mechanism etc. The GAP Assessment also serves to establish baseline measures from which to measure progress toward future IT goals and plans. This self-study is not intended to replace development of a comprehensive strategic plan for IT, but is rather meant as a prerequisite to ensure that the required resources and conditions are in place for implementation of a strategic plan for IT by the time. The purpose of this gap analysis is to quickly identify the most obvious gaps in Auditee organization and then to begin to fill those gaps with the use of existing resources or new.

Steps to Performing a Gap Analysis:

- Planning
- Execution
- Determining the best practice
- Report

Outcomes of GAP Analysis

- Pre Assessment Survey Report
- GAP Analysis report
- Suggestions and Recommendations

IT Policy Review

Policy Review is the process of checking all the necessary documents for Information Security. Policy review is the most important phase of Audit as it drives organizations process and structure of work. These policies help organizations to minimize repetitive decision making from top management for each small works of Information Security and assigning it to IT head or CISO as per defined. Policy is set of documents containing process and procedures and is segregated in 4 major categories with 47 subcategories.

Documents are segregated into 4 types:

1. Documents Related to Management System
2. Documents Related to Risk Management
3. Documents Related to Information Security Controls
4. Documents Related to Internal Audit

Quality Assurance

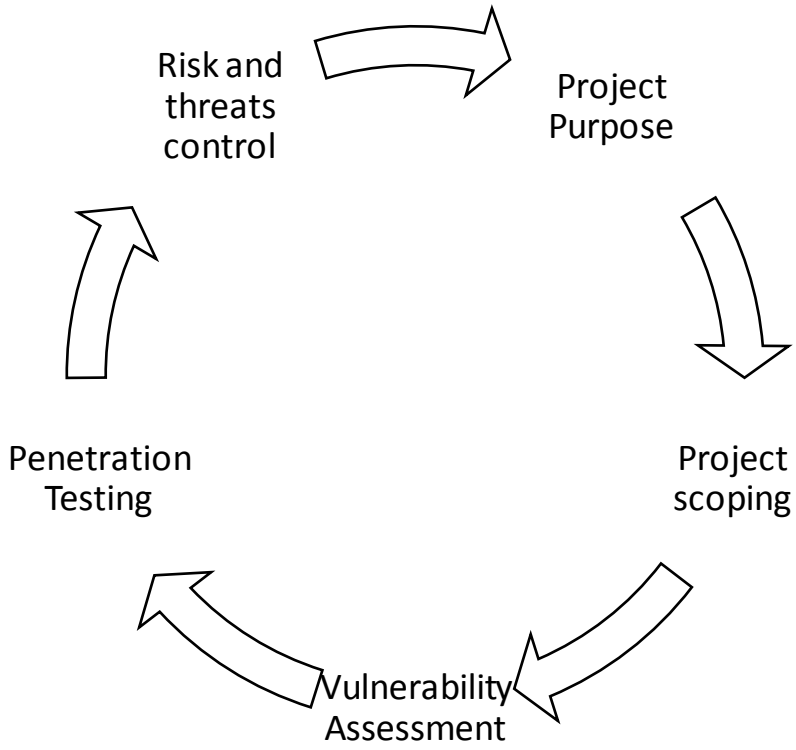
In this process Technological systems are tested against vulnerabilities.
Under this Phase we deal with the testing of

- Hardware Systems
  Hardware Level Test is trending these days, all the resources that we use in our organization may not be branded and proprietary which means there is a huge potential in these hardware for malware. So these hardware systems are assessed, inspected for malware. This hardware may be computers, routers, switches, AP, USB devices etc.
  Also in this part of testing Network and System are also tested for vulnerabilities.
- Software Systems
  Organizations are supported by software at highest level; each system we see is being computerized. From HR management to Operation Management, from attendance management to payroll, ERP, CBS each system has to be secure and well performing. So for ensuring quality systems will be tested against functional, security, performance and compatibility errors if mentioned in scope else we will directly conduct VAPT for security.

VAPT (Vulnerability Assessment and Penetration Testing)

Vulnerability Assessment and Penetration Testing are one of the effective procedures to measure, assess as well as weigh the security architecture considered or implemented in any software/network architecture. VAPT is one of the most important phases of risk assessment.

A successful penetration test also depends upon the successful project management. The scope of testing, rules of engagement, and highly specified procedures are key to successful test. Due to the sensitive nature of the project, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results.



Application Security Checklist

We follow the Open Web Application Security Project (OWASP) 2017 to test for the following security issues:

A1:2017-Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

A6:2017-Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and

verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

A7:2017-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

A9:2017-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defences and enable various attacks and impacts.

A10:2017-Insufficient Logging&Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Network Security Checklist

1. Outdated/ Missing security patches
2. Weak or default passwords
3. Misconfigured firewall rule bases
4. Computer and server vulnerabilities
5. Firewall vulnerabilities
6. Router Vulnerabilities
7. Switch Vulnerabilities
8. Newly installed system components
9. Misconfigured devices
10. Threats from email, malware, and VPN connections
11. Website flaws
12. Exposure of confidential and sensitive content
13. Unsupported version of OS
14. Insecure Certificate Usage

Confidentiality

We require strict adherence by our partners and staff to ethical rules of our profession and firm. In all aspects of our practice our partners and staff maintain a strict standard of confidentiality towards information which is obtained during the course of carrying out our professional duties. Furthermore, the organization and its people maintain complete independence of interest in relationships with clients.

Limitations and Professional Liability

Our review procedures will not constitute financial assignment, the objective of which is the expression of an opinion on the financial statements or specified elements, accounts or items thereof. Accordingly, we will be unable to express such an opinion at the conclusion of our work. Our deliverables are intended solely for the use of the Organization and will be restricted to use within the Organization.

It is important to recognize that there are inherent limitations in our process. For example, our procedures are generally based on the concept of selective testing of the data being examined and are; therefore, subject to the limitations that material error, fraud, and other illegal acts having a direct and material financial impact, if they exist, may not be detected. Also, because of the characteristics of fraud, particularly those involving concealment through collusion and falsified documentation (including forgery), the audit may not detect a material fraud.

In no event shall Eminence Ways, its partners, or employees be liable for any loss, damage, cost or expense arising in any way from fraudulent acts, or omissions, mis-representations, or willful default on the part of the Organization.

In no circumstances shall any liability of Eminence Ways, its partners or employees relating to services provided in connection with the engagement set out in this letter (or addition or variation thereto) exceed the amount paid to us in respect of the professional charges for those services as mentioned in our financial proposal.

Responsibilities of the Organization

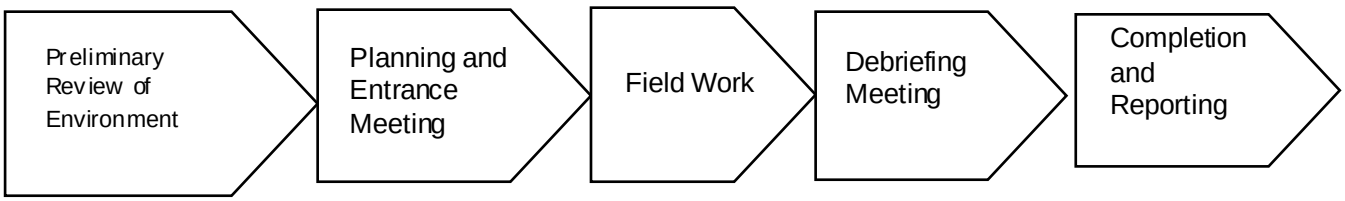
The Organization shall fully cooperate to us for providing documents information. It shall be responsible for making available to us, upon request, all of the necessary information and personnel to whom we can direct inquiries and request information to perform our engagement.

We will make specific inquiries of management when performing the audit. In addition, we may require a representation letter from members of management who are responsible for or are knowledgeable, directly or through others in the Organization about specified financial statement elements, accounts or items, management assertions, etc. The results of our review tests, the responses to our inquiries and the written representations, if any, comprise the evidential matter we intend to rely upon in forming our findings.

Team Composition and Task Assignments

In recognition of the fact that the engagement is quite challenging and needs to be completed in a very strict time schedule, we to mobilize a full-fledged experienced and dedicated team to this engagement. *Besides the key professional staff, we strongly feel that other support Staff with relevant experience would need to be fielded to successfully execute this engagement.*

Time Schedule



5 Days **4 Days** **24 Days** **4 Days** **7 Days**

Service Cost and Pricing

DESCRIPTION	AMOUNT
PKI RCA Audit & Vulnerability Assessment / Penetration Testing (VAPT) Fee	NRs 8,82,000
VAT 13%	NRs 1,14,660/-
TOTAL	**9,96,660/-**

Annexure

- Company Registration
- PAN/ VAT Certificate
- Latest VAT Clearance

नेपाल चार्टर्ड एकाउन्टेन्ट्स संस्था
The Institute of Chartered Accountants of Nepal
(Established under Nepal Chartered Accountants Act, 1997)

संस्था दर्ता नं. 0003

मिति: २०५९/०५/२८

लेखा व्यवसायी संस्था
दर्ता प्रमाणपत्र

नेपाल चार्टर्ड एकाउन्टेन्ट्स ऐन, २०५३ को दफा २८ (क) र नेपाल चार्टर्ड एकाउन्टेन्ट्स नियम, २०५६ को नियम ५८ बमोजिम के. बि. चित्रकार एण्ड कम्पनी, चार्टर्ड एकाउन्टेन्टस् (एकलौटी फर्म) लाई दर्ता गरिएको छ । यो प्रमाणपत्र २०५९ साल भाद्र २८ गते देखि २०६० साल आषाढ मसान्त सम्म र नवीकरण गराएमा नवीकरण अवधिसम्म बहाल रहने छ ।

Firm Reg. No. 0003

Date : September 13, 2002

FIRM REGISTRATION CERTIFICATE

In pursuant to Section 28 (1) of Nepal Chartered Accountants Act, 1997 and Regulation 58 of Nepal Chartered Accountants Regulation, 1999, **K. B. Chitracar & Company**, Chartered Accountants (Proprietorship Firm) has been registered. This Certificate shall be valid from September 13, 2002 to July 16, 2003 and upto the renewed date in case of renewal.

पुरुषोत्तम लाल श्रेष्ठ
कार्यकारी निर्देशक
Purusottam Lal Shrestha
Executive Director

विजय कुमार अग्रवाल
अध्यक्ष
Bijay Kumar Agrawal
President

K.B CHITRACAR & CO Chartered Accountants

नेपाल सरकार

अर्थ मन्त्रालय

आन्तरिक राजस्व विभाग

स्थायी लेखा नम्बर (PAN) दर्ता प्रमाण पत्र

स्थायी लेखा नम्बर	:	६ ० ६ २ ६ ९ ७ ६ ६
आन्तरिक राजस्व कार्यालय	:	आन्तरिक राजस्व कार्यालय ललितपुर

दर्ता मिति

	दिन	महिना	साल
आयकर:	०६	०४	२०७४
मु. अ. कर:	१८	०४	२०७४

कारोबारको नाम	:	के. वि. चित्रकार एण्ड कंपनी
करदाताको प्रकार	:	साझेदारी फर्म
ठेगाना	:	वार्ड नं. १०, ज्वागल महानगरपालिका: ललितपुर, ललितपुर
व्यवसायका कारोबारहरु	:	दर्तावाल लेखाबर्ता तथा परीक्षक,

करदाताको दस्तखत

कर अधिकृतको दस्तखत

करदाताले पालना गर्नुपर्ने कार्यव्यहरु:

- कारोबार गर्ने अनिवार्य रुपमा बिल बिलक जारी गर्नुपर्ने ।
- मु.अ.करमा दर्ता हुने पश्चात कर अवधि (मासिक वा त्रैमासिक वा चौमासिक) समाप्त भएको २५ दिनभित्र मु.अ.कर विवरण तथा मु.अ.कर रकम बुझाउनु पर्ने ।
- अन्तःशुल्क लाग्ने कारोबार गर्नेले अन्तःशुल्क व्यवस्था गरेकोमा चाहेक प्रत्येक महिना समाप्त भएको २५ दिनभित्र मासिकोवारी र अन्तःशुल्क रकम बुझाउनु पर्ने ।
- प्रत्येक आर्थिक वर्षको आय विवरण तोकिए बमोजिम बुझाउनु पर्ने ।
- समयमा विवरण र कर रकम नबुझाएमा ब्याज, शुल्क र जरिवाना लाग्नेछ ।
- यो प्रमाणपत्र देखिने गरी कारोबार स्थल/मुख्य कार्यालयमा राख्नु पर्नेछ ।
- यसै हिसिवा भएमा आन्तरिकमा सम्पर्क राख्नुहोला ।

नेपाल सरकार

अर्थ मन्त्रालय

आन्तरिक राजस्व विभाग

आन्तरिक राजस्व कार्यालय ललितपुर-1

(आयकर नियमावली, २०५८ को नियम २६ संग सम्बन्धित)

यो विवरण मिति २०७६.१०.२६ मा रुजु भएको छ।

प.सं: २०७६.०७७

च.नं. ५१८६

मिति: २०७६.१०.२६

बिषय : कर चुक्ता प्रमाण पत्र ।

श्री के. वि. चित्रकार एण्ड कंपनी

१०-ललितपुर,

स्थायी लेखा नं : ६ ०६ २६ ९७६ ६

यस कार्यालय अन्तर्गत दर्ता रहेका तपाईं ले आ.व २०७५.०७६ मा देहाय बमोजिमको आय रकमको आय विवरण मिति २०७६.०९.२९ मा यस कार्यालयमा पेश गरी सो अनुसार देहाय बमोजिमको आयकर दखिला गरेकोले यो कर चुक्ताको प्रमाण पत्र प्रदान गरिएको छ।

आय विवरण पेश गरेको मिति	जम्मा आय (कारोबार) रकम रू	कर योग्य आय रु.	दाखिला गरको कर रकम रु
२०७६.०९.२९	३५,६ ३९,१८१.००	५,६ ७८,२२६.००	१,४१९,५५६.००

१९०१२६

.....

लिलकबहादुर थापा

(कर अधिकृत)

कर अधिकृत

पुनश्च: यो प्रमाणपत्र त्यस फर्म/ उद्योग कम्पनी / संस्थाले पेश गरेको विवरणको आधारमा जारी गरिएको छ। पेश भएको आय विवरण ज्ञानबिनमा परेमा आयकर ऐन, २०५८ को दफा १०१बमोजिम संशोधित कर निर्धारण हुन सक्ने जानकारी गराईन्छ।

-

CONTACT INFORMATION

KB Chitracar & Co.
Chartered Accountants
Jwagal, Lalitpur
Contact No: +977-1-5261011; 5261013
Fax: 5260985
PO Box: 2043
Email: info@kbc-ca.com.np