CryptoGen Nepal

Sample Report

Information System Audit

For

XYZ Bank Limited (XYZBL)

EST. 2019

Document Control

Document Name	Draft report of Information Systems Audit
Abstract	This document details the Audit approaches and detailed Audit findings of the existing assets of "XYZ Bank Limited".
Security Classification	Restricted
Location	XYZ Bank Limited, Nepal Country Office, Kathmandu

Authorization		
Document Owner	**Prepared by**	**Authorized by**
CryptoGen Nepal	Full Name	Full Name

Amendment Log				
Version	**Modification Date**	**Section**	**Amendment/ Modification/ Deletion**	**Brief description of the change**
1.0		NIL	NIL	Draft Report

Distribution list	
Name	**Role**
Full Name	Project Manager

Disclaimer

CryptoGen Nepal has designed, performed the Information System Audit with reference to the in-house developed and international Information System Audit/Assurance Program. The Audit has been followed with the Risk based approach and includes the audit and assessment on sampling basis wherever feasible to conclude our opinion. Hence, the work should not be considered inclusive of all proper information, procedures, and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. The audit conducted is of sample components of the ISMS. It may very well be possible that all the sampled components result in non-conformity or vice versa. CryptoGen Nepal disclaims any claim made against the audit and assessment as if ALL procedures/tests have been performed.

Reservation of Rights

This Report is solely used for the purpose for Reporting to XYZ Bank Limited stakeholders for the findings derived from our assessment during the performance of the mutual agreed scope. Hence, the information hereafter stated are highly confidential and should not be disclosed to any other party without obtaining consent of either party. No other right or permission is obtained/granted with respect to this scope of work completed.

Table of contents

Abbreviations

Index	Definition
PRTG	Paessler Router Traffic Grapher
MTTR	Mean Time to Respond
NAS	Network-Attached Storage
BCP	Business continuity Plan
COO	Chief Operating Officer
CCTV	Closed Circuit Television
POC	Point of Contact
CBS	Core Banking Software
IT	Information Technology
CIAA	Confidentiality, Integrity, and Availability and Authenticity
POC	Point of Contact
IS	Information Systems
DC	Data Center
DR	Disaster Recovery
DRP	Disaster Recovery Plan
ISMS	Information Security Management System
HRMS	Human Resource Management System
ICT	Information & Communication Technology
ISACA	Information Systems Audit and Control Association
SOP	Standard Operating Procedure
ITAF	Information Technology Audit Framework
NRB	Nepal Rastra Bank
OS	Operating system
UPS	Uninterrupted Power Supply
SL/SLAs	Service Level/Service Level Agreement/s
VAPT	Vulnerability Assessment and Penetration Testing

Executive Summary

XYZ Bank Limited (XYZBL), classified as an “A” Class financial institution by Nepal Rastra Bank is one of the most prominent banks in the country which was founded on December 24, 2002. XYZBL has extended its services nationwide through 183 branches and 3 extension counters. It has consistently earned recognition for its reliability, credibility, and technological advancement within the Nepali banking sector. The bank aims to contribute to Nepal's financial markets with a commitment to high integrity, transparency, and consistency.

IT Audit is critical for the Company to manage cyber risk, improve data security, and uncover the vulnerabilities and risks inherent in the existing IT infrastructure and software for further improvement. To analyze and assure the system's integrity, IT audits examine important systems, technology, architecture, and processes to ensure that information assets are secure, dependable, and available, as well as in compliance with the NRB IT Guidelines. XYZ Bank Limited (XYZBL), aims to conduct an Information System Audit (IS audit) of its ICT and MIS Systems and sought a consultant to assess the existing system, identify possible security gaps and areas which needs to be enhanced to make the system more secure and efficient. We, CryptoGen Nepal (CGN) as a certified professional, agreed to conduct the assessment as per the scope of work under industry best practices.

For the audit, we, CryptoGen Nepal have followed the ISO/IEC 27001 and NRB IT guidelines. We have considered 3 major elements (People, Process, and Technology) for successful business growth. The preliminary assessment period lasted from start date to end date. After a series of inspections, interviews, and reviews conducted by the auditee in an organized manner with qualified team members of CryptoGen Nepal, we have shared our findings with the management.

Conclusion

The detailed Audit findings are provided in the following section, we would like to draw the attention of XYZBL's higher management team, IT team members and other staffs to thoroughly review the recommendations provided. We are confident that these recommendations will be duly taken into consideration and be addressed by the team concerned to take XYZBL to the next level with improvements in all three sectors, i.e., people, process, and technology.

Even though most of the controls were found to be in place to protect the systems, our audit revealed that additional system access security controls need to be implemented to strengthen protection over company records and customer information.

Finally, we would like to thank each and everyone involved for their support, and co-operation from the inception to the closure of this Audit Project and expect the fixation or compliance during our verification and follow-up phase.

Objective and Scope

Objective

The objective was to analyze and evaluate the organization's present IT environment, as well as its controls, policies, procedures, and practices. The methods in place determine whether the organization conforms to the requirements established in the NRB IT Guidelines and the organization's internal Information & Communication Technology (ICT) Policy which are the primary components examined during the audit.

The Audit Project started along with the VAPT Project. The VAPT project's goal was to find flaws, issues, and vulnerabilities in the targeted systems, networks, and mobile applications, as well as to review the current security status and network position to analyze and exploit the discovered vulnerabilities and potential issues that could be used to break into networks and escalate the vulnerabilities to have the greatest impact.

The objectives of the Audit were to.

- Identify the security status of Information Systems associated with the organization.
- Provide suggestions/feedback for mitigating risks associated with potential weaknesses identified.

- Provide reasonable assurance on maintenance of Confidentiality, Integrity, and Availability and Authenticity (CIAA) of the Company's information systems.
- Verify the adequacy and effectiveness of the infrastructure and application's security controls against prevailing and potential security threats and vulnerabilities to the Company's environment.
- Identifying areas with deficiencies in internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions.

Scope of Work

- Policy, Standard Operating Procedure, Guidelines, Standard Practices & Regulatory Requirements.
- Physical and Environmental Security
- DC/DR Hardware
- Operating System Audit of Servers, Systems, and Networking Equipment
- Support
- Application System Security Audit (Third Party, In-house Developed, etc.)
- Audit of DBMS and Data Security
- Network Security Audit
- Email System
- IS Audit of ATM and Card Operational Processes
- Payment Systems (SWIFT, Remittance, NCHL IPS, RTGS, etc.)
- Call center system and service agreement
- Cloud Security Audit
- Others

Scope of the Services

Conduction of a detailed security audit of IT Systems owned and managed by XYZBL in line with proven international practices security standards/ methodologies to conduct the security assessments.

Areas of Focus

Governance, Risk and Compliance Of IT

IT governance is a formal framework that provides a structure for organizations to ensure that IT investments support business objectives and stakeholders need. They require periodic reviews to avoid any outdated information leaving the organization vulnerable to unsolicited risks or incompliance. These reviews include various approaches and strategies to manage the organizations' risks and compliances.

Corporate governance practices, regulations, and compliances and assess the gap covering the following areas:

- IT Standards and related frameworks, policies, and procedures review and implementation gap assessment
- Risk assessment procedures
- IT organization structure review
- References from other related systems and policies in place as per industry practices and legal requirements
    - NRB IT Guidelines 2012
    - ISO 27001 Standard

IT Assets Acquisition, Development, and Implementation

The section covers how we as IT auditors provide assurance that the practices for the acquisition, development, testing, implementation, maintenance, replacement, and disposal of IT Assets are adequate and effective to meet the organization's strategies and objectives. The audit will examine the Business Case and Feasibility Analysis and test the System Development Methodologies and ensure the post-implementation reviews are also made as they ought to be.

It is expected the auditee has proper controls in place for planning the procurement and acquisition, replacement, maintenance, and disposal of IT assets and practices change management procedures as any changes to the assets should be transparent and within a controlled environment.

The following areas are covered

- Outsourcing policies, AMCs
- Asset inventory and documentation
- SLA management
- Security Assurance Requirement Analysis
- Implementation and change management

Protection of Information Assets (IT System architecture and infrastructure Security)

Understanding of the value of information assets is a key consideration for information systems management. It includes the comprehensive list of Mobile, Wireless, and Internet-of-Things (IoT) Devices - computer equipment, phones, network, email, data, and any access-related items such as cards, tokens, and passwords, etc. We examine Information Asset Security Frameworks, Standards, and Guidelines. All assets should be identified, evaluated, classified, and protected based on their value, their location, risk, and sensitivity. As some assets are more sensitive than others. We perform risk-based audits by assigning levels to the information resources.

This area of focus aims to provide assurance that the information assets' confidentiality, integrity, and availability are ensured by the enterprises' security policies, standards, procedures, and controls.

- Physical Security control and Segregation of duties
- Fire / flooding / water leakage / gas leakage etcetera.
- Assets safeguarding, Handling of movement of Man/Material/ Media/ Backup / Software/ Hardware / Information
- Electrical supply, redundancy of power level, Generator, UPS
- Surveillance systems
- Pest prevention (rodent prevention) systems
- NDC reviews
- Access rights, Administration Control, and privileges

Information Systems Operations, Service Management & Business Resilience

Operations should ensure that the systems, infrastructure, and the applications in the organization operate as intended when needed.

Business resilience planning is a governance and risk management responsibility that an organization must address to enable them to survive and thrive in an increasingly hostile environment. It encompasses crisis management and business continuity and responds to all types of risks that an organization may face, from cyber threats to natural disasters, and much else besides. Along with addressing the consequences of a major incident, business resilience relates to the ability of an organization to adapt to the new environment and circumstances following that incident.

The following areas are covered to see if the IS operations meet the requirement of their use cases if a proper service management structure is deployed to ensure that people, technology, and processes are deployed to achieve the business requirements, and if proper safeguards are in place to minimize the cost, risk and the time period of the disruption to processes critical for business.

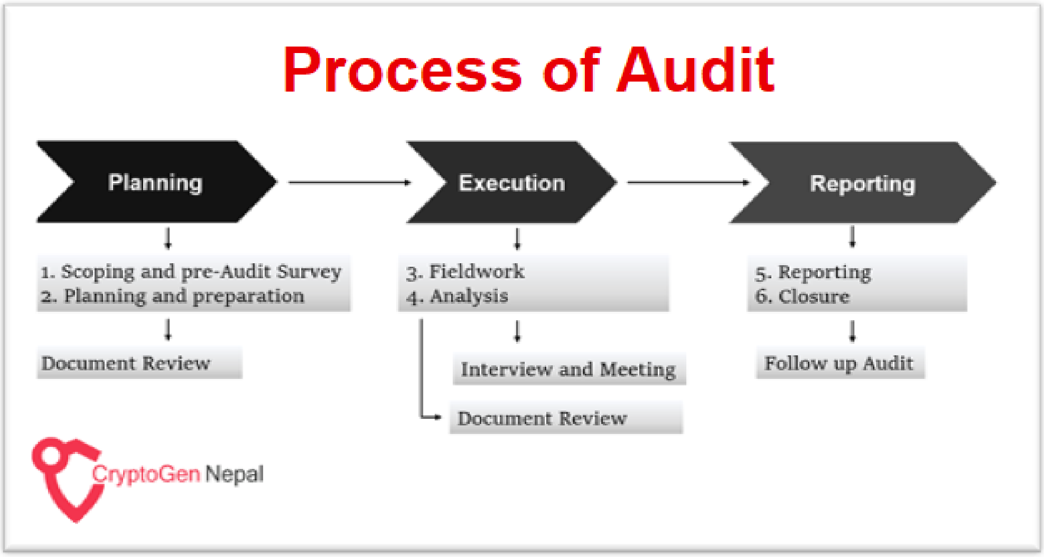
- Hardware, OS setup, maintenance, Patches, & Software management
- Services and Ports accessibility
- Segregation of Duties in all IT operations
- Asset management, maintenance, and optimization
- Change Management Procedures
- Password policy and strategies
- Information assets configurations and policies
- Risk assessment & Disaster Recovery Plans and strategies
- Data Backup, Retention, Restoration, Synchronization, Change Management and System Resiliency and their monitoring
- Data leakage controls, media handling, disposal
- Incidence response review, Disaster recovery teams
- Redundancy and replication of network and sites
- Staff Training and test drills
- Log monitoring mechanism, its sufficiency, security, maintenance, and backup
- Vulnerability Assessment & Penetration Testing

Network Security

- Network Architecture Review
- Devices and Links Redundancies
- Implemented Network Security controls
- Outsourced services management
- Network Level Accesses, controls, logs
- Offsite working procedures
- Firewall Configuration reviews
- Centralized logs management procedures
- Privileges reviews

Approach and Methodology

The Information System Audit includes various procedures guided under ISACA ITAF.



The approach followed during the planning, execution and reporting phases are outlined below.

- ***Scoping and pre-audit survey***

During this phase, we determined the main areas of focus for the Audit and the areas explicitly out-of-scope based on the scope discussed with XYZBL. Here, we paid particular attention to information security risks and controls associated with the auditee. During the pre-audit survey we asked for pertinent documentation for review. XYZBL nominated a "Point of Contact", responsible for ensuring that the auditors have access and can safely visit different areas of the company and find relevant personnel and information necessary to conduct the work.

- ***Planning and preparation - Document Review***

The overall scope of work was further broken down by generating an audit work plan taking into account, the security requirements and any information that was already evident at this stage (such as information-security relevant laws, regulations, and standards that were known to apply to similar organizations in the industry). The overall timing and resourcing of the audit were negotiated and agreed by the management of the organizations.

- ***Fieldwork - Interview & Meeting***

During the fieldwork phase, audit evidence was gathered by working methodically through the work plan. The first part of the fieldwork typically involved a documentation review where we read and noted documentation relating to and arising from the ISMS (Scope Agreement, IT Directive, Supplier Relationship Documentation, Log records, policies, and procedures, etc.)

During the second part of the work, necessary technical compliance tests were conducted to verify that the IT systems were configured in accordance with the organization's information security policies, standards, and guidelines.

The following tasks were conducted during this phase.

- Interviewing staff, managers, and other stakeholders associated with the Audit.
- Review of ISMS documents, printouts, and data
- Observation of IT and IS processes
- Review of system/ network Architecture
- Review of Security of applications
- Checking system security configurations
- Review Datacenter and physical security

Classification of Findings

the classification scheme for evaluating findings is designed to prioritize and address issues based on their criticality to the organization's operations and security. This scheme categorizes findings into four levels: **Critical**, **High**, **Medium**, and **Low**. Critical findings are those that pose immediate and severe risks requiring urgent attention. High findings, while not immediately threatening, still present significant risks that could escalate. Medium findings represent moderate risks, whereas, Low findings involve minimal risks with long-term action plans to be addressed. The classification scheme helps the organization allocate resources efficiently, and responses are timely and effective, enhancing the organization's ability to manage and mitigate risks systematically. Each finding is documented with a detailed rationale for its classification and accompanied by specific recommendations for remedial actions, ensuring clear communication and accountability.

Audit Findings Classification Scheme

- **Critical**: Issues that pose an immediate and severe risk to the organization's operations, security, or compliance requirements. These findings typically involve a direct threat to the infrastructure's integrity, confidentiality, or availability and require immediate attention.

- **High**: Findings that present a significant risk which could potentially lead to critical impact if not addressed promptly. These are less immediate than critical issues but still require swift action to prevent escalation.
- **Medium:** Issues that present a moderate risk and could negatively affect the organization but do not have an immediate or severe impact. These findings concern areas where controls are in place but need improvement.
- **Low:** Findings that represent a low risk and have minimal impact on the organization. These issues are more about optimization rather than direct threats.

We also introduce a Performance-Based Classification system designed to highlight and categorize the operational and security practices observed within the organization. This classification not only identifies areas requiring improvement but also recognizes and celebrates exemplary performance where standards are not only met but exceeded. The categories within this system—**Exemplary**, **Satisfactory**, and **Needs Improvement**—serve to provide a clear and structured understanding of how well current practices align with industry benchmarks and organizational goals.

- **Exemplary:** Findings that demonstrate best practices, exceptional compliance, or innovative solutions that significantly enhance the organization's processes or security posture.
- **Satisfactory:** Findings where the practices meet industry standards and organizational policies effectively but don't necessarily exceed expectations.
- **Needs Improvement:** Areas that meet the minimum requirements but could benefit from further refinement to achieve better efficiency or effectiveness
- **Deficient:** Areas where the minimum requirement is not met while significantly lacking necessary controls, or do not meet the minimum standards required by organizational policies, legal regulations, or industry guidelines.

Audit Details and Findings

This section covers the control mappings considering the NRB IT Guidelines 2012 and ISO 27001.

1. Context of the Organization

Control Title – Understanding the needs and expectations of interested parties				
Classification:				
Risk-Based:	**Low**		Performance-Based:	**Satisfactory**
Reference: ISO/IEC 27001 4.2 Understanding the needs and expectations of interested parties				
Description: To meet the standard, the organization must assess its ISMS stakeholders, understand their needs and expectations, and consider legal, regulatory, contractual, and other relevant internal and external factors that impact the ISMS's intended outcomes. This ensures alignment with stakeholders' requirements.				
Observation: • Most of the compliance requirements set by the NRB IT guidelines were found to be fulfilled by the XYZBL. The following sections give information on XYZBL's ISMS operating processes, findings, and compliance status.				
Recommendation: • It is suggested that any partial and non-compliances found in the IS and VAPT reports be addressed before the next audit session.				
Management Response:				

APPENDIX A: List of Key Information

List of documentation reviewed

1. **IT Policy and Procedures**

- Information Security Policy
- Information Technology Policy
- Work From Home Policy
- SOP User Access Control
- SOP Business Continuity Plan and Disaster Recovery
- SOP Software Development, Interface and Support
- SOP Maintenance, Procurement and Disposal of Hardware
- SOP Work from Home
- SOP Information Technology (IT) & Digital Banking (DB) Department Profile
- Etc.

2. **Service Level Agreement between ABC Company and XYZ Bank Limited**
3. **Service Level Agreement between DEF Company and XYZ Bank Limited**

List of People Interviewed

Point of Contacts	Department
Full Name1	**IT Officer**
Full Name2	**HR Manager**
Full Name3	**Assistant Administration Manager**
Full Name4	**Senior IT Officer**
Etc.	**Etc.**