



SOC Annual Report

SOC Monitoring for

XYZ Bank Limited

MSSP Alert
A CyberRisk Alliance Production

TOP
250



STARTUP
CATEGORY



Certificate of Registration

This is to certify that

Cryptogen Nepal Pvt. Ltd.

Manakamana Marg, Naxal Nagpokhari, Kathmandu, 44600, Nepal.

has been assessed by RICL and found to comply with the requirements of

ISO 27001 : 2022
Information Security Management Systems

For the following activities:

Providing Information System and Cyber Security Professional Solution and Services, Sales, Support, Audit, Assessment, Training and Consultancy to its Customers.

(SOA Version: SOA/CNPL/01, Dated 03/07/2024)

This Certificate is Valid from 12/09/2024 Until 11/09/2025

Date of Initial Certification: 12/09/2024

Ist Surveillance on or before: 11/08/2025

IInd Surveillance on or before: 11/08/2026

Certification Valid Until: 11/09/2027



Certificate No.:
24RN09CQ



CB-MS-26213

United Accreditation Foundation INC, 400 North Center Dr Ste 202,
Norfolk, VA 23502, United States of America.

Kuldeep

Director
Royal Impact Certification Ltd.

This certificate can be verified online at www.iafcertsearch.org

This Certificate remains property of RICL, 1207, Delaware Ave # 1634, Welmington, DE 19806 USA.

Must be returned on request or if certificate is withdrawn. Certificate validity is subject

to successful annual surveillance audits. www.riclis.com, info@riclis.com

Table of Contents

Foreword.....	3
Executive Summary.....	4
SOC Key Metrics & Statistics	5
Key Accomplishments	6
Threat Trends Observed	6
Industries Targeted	7
Top Threat Categories	7
Notable Incidents and Activities	8
SOC Maturity Assessment Based on CRG	9
Section E – Detection Domain Assessment	9
Section F – Response and Recovery.....	10
Strategic Improvements & Recommendations for 2082/83	11
Planned Initiatives for 2082/83	12
Conclusion.....	12
Appendix	13
Scoring Scale.....	13

Document Name	Annual Report
Abstract	This report is about the SOC's efforts in 2081/2082 to enhance threat detection, reduce incident response time, and strengthen cybersecurity posture.
Security Classification	Confidential

Authorization			
Document Owner		CryptoGen Nepal	
Prepared By	Simran Karki	Authorized By	Shreenkhala Bhattarai

Amendment Log				
Version	Modification Date	Section	Amendment/ Modification/ Deletion	Brief description of the change
1.1	04:00 PM	Scoring scale	Added	Overall scoring scale

Distribution List	
Role	Name

Foreword

It is with great pride that we, the Security Operations Center (SOC) team at Cryptogen Nepal, present the Annual SOC Report for the year 2081/82, for our esteemed partner, XYZ Bank Limited. This report summarizes a year of focused collaboration, continuous monitoring, and strategic cyber defense operations conducted to safeguard the bank's digital infrastructure and customer data.

The financial sector continues to be a prime target for cyber adversaries, and 2081/82 was no exception. Despite the evolving threat landscape, our SOC team remain focused ensuring detection and response of potential threats targeting the bank's assets and systems. Through 24/7 log monitoring and proactive threat hunting, we significantly enhanced the bank's security visibility and incident readiness.

As we look ahead into 2082/2083, we remain committed to delivering value through cutting-edge security services, continuous improvement, and adaptive defense strategies. We thank XYZ Bank for their trust and partnership in this shared journey toward cyber resilience.

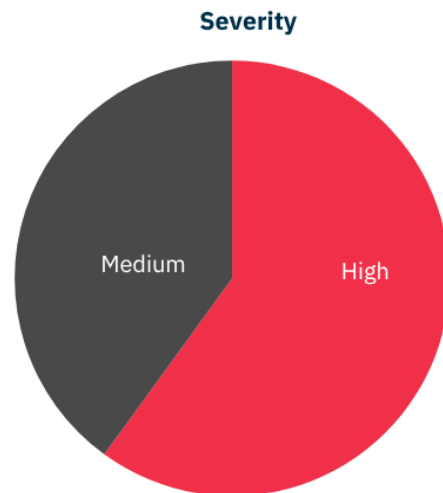
Executive Summary

Over a year our team detected several incidents and notable events. Key highlights include:

2081/82

Top 5 Incidents & Findings

- **Exposure of User Passwords in referrer Header**
User passwords were exposed in plain text within the Referrer Header of an HTTP request, affecting multiple users.
- **Exposure of JBoss Server Over the internet**
A user from India accessed a destination hosting exposed JBOSS and Keycloak services, along with a publicly accessible Temenos login portal.
- **Access to unusual Domain**
An unusual domain connection by user HIRABP was detected, with the firewall flagging a potentially malicious file, RegisterSerialKeys.htm. Further analysis revealed that the domain was hosting an archived site distributing registration keys for End-of-Life (EOL) Microsoft products, which are highly vulnerable due to the lack of security updates.
- **Internal to External Communication with Blacklisted IPs**
Two internal IP (192.168.206.111 and 192.168.6.53) addresses attempted to connect to known malicious external IPs, which were blocked by the firewall. These incidents are marked as high severity due to unknown application details and use of non-standard ports
- **Outbound HTTPS Request to Malicious Destination**
Observed traffic to malicious IP hosted by Hetzner Online GmbH in Germany, is associated with RedLine Stealer malware and flagged as a Command and Control (C2) server by multiple threat intelligence vendors, including Fortinet, BitDefender, and Dr.Web.



Highest Incident Count

The highest number of incident detections occurred in Q1, specifically during the month of Mangsir, with a total of 82805 incidents all of which were maximum false positive.















Targeted Phishing

The email address umesh.sinkwho@XYZbank.com & cardcenter@XYZbank.com received the highest number of phishing emails on Q4.

SOC Key Metrics & Statistics

This section provides a high-level overview of the key performance indicators and statistical insights gathered by the SOC throughout the year 2081/82. It highlights the volume and nature of security events monitored, incidents detected, response times, and resolution rates across each quarter. These metrics reflect the efficiency, scalability, and maturity of the SOC operations delivered by Cryptogen Nepal to XYZ Bank. The data serves as a foundation for evaluating the bank's cybersecurity posture and guiding future improvements in threat detection and response capabilities.

Metric	2081	
Incidents Detected	500K+	
Incidents Resolved	100%	
Average Time to Detect	10 Minutes	
Average Time to Respond	30 Minutes	
Threat Intel Feeds Utilized	MISP, FortiGuard, Virustotal, AbuseIPDB	
Threat Hunts Conducted	5	
New Use Cases Created	80+	
Daily Report	270+	
Weekly Report	35+	
Monthly Report	9	
Quarterly Report	3	
Festive Report	1	

Key Accomplishments



Identified and responded to multiple attempts to exploit vulnerabilities such as Command Injection, SQL Injection, and Directory Traversal, with proactive recommendations to enhance WAF policies accordingly.



Threat hunting were conducted every month to identify gaps in our Security Operations Centre.



Performed threat hunting such as hypothesis based, IOC-based threat hunting exercises targeting emerging threats, including Redcurl, Defend Not AV persistence, ZLoader, and other trending malware campaigns. Reduced threat intelligence false positive threat feeds.



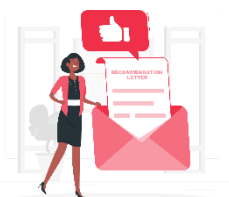
Developed custom alert rules, search templates, and saved searches tailored to the client's specific monitoring and reporting needs.



Continuously optimized alert rules to reduce false positives and enhance the accuracy and effectiveness of threat detection mechanisms.



Delivered daily Analyst Notes summarizing key security events and activities, providing the client with clear visibility into their security posture.



Provided weekly strategic recommendations including in-depth analysis.

Threat Trends Observed

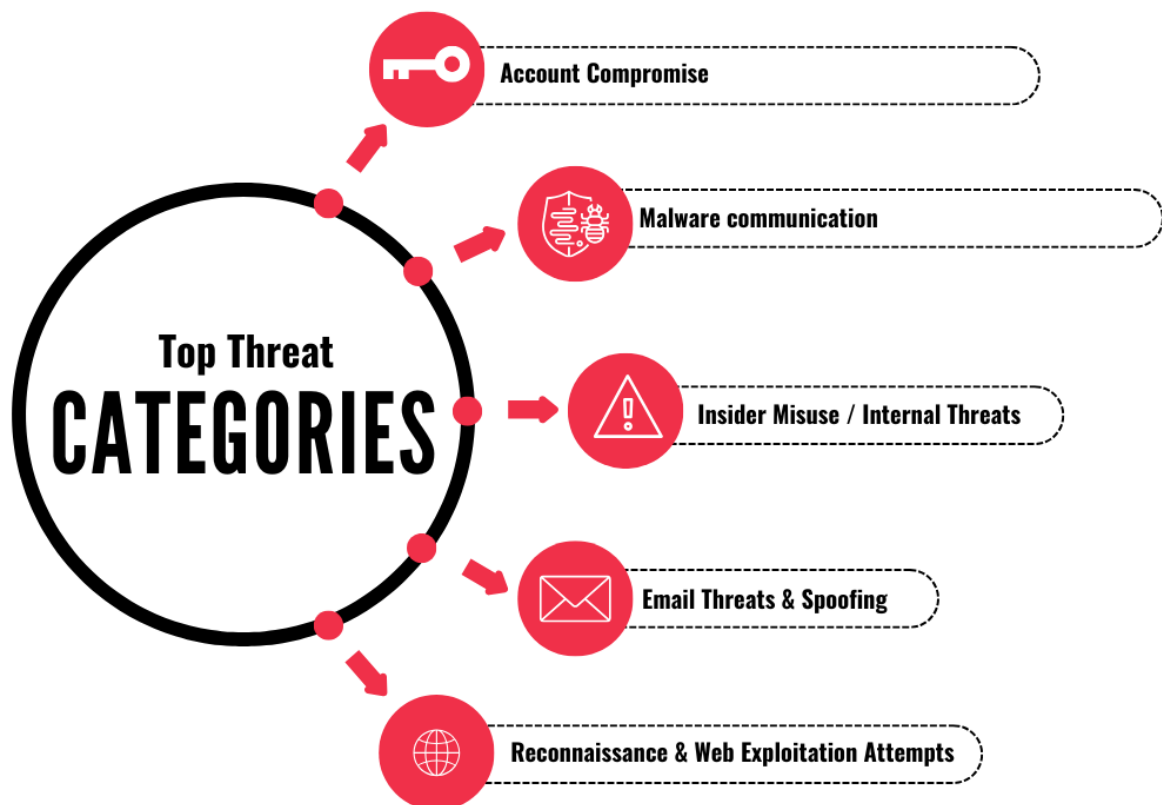
Over the monitoring period of 2081/82, our SOC identified multiple security events that indicate an evolving threat landscape, both in terms of sophistication and

intent. The trends observed demonstrate adversarial interest in exploiting cloud services, abusing trust boundaries, targeting user credentials, and probing for external vulnerabilities.

Industries Targeted

Our Managed Security Services Provider (MSSP) offering is tailored to meet the unique cybersecurity needs of key sectors. We primarily serve Financial Institutions, Educational Institutions, and Government Agencies. These industries are among the most targeted and highly regulated, requiring proactive security measures. Through our MSSP service, we ensure that clients in these sectors receive continuous protection, real-time threat monitoring, and expert incident response to safeguard their critical infrastructure and sensitive data.

Top Threat Categories



Notable Incidents and Activities

- Internal to External Communication with Blacklisted IP
- Outbound Permitted Traffic to FortiGuard Malware IP
- XYZ Virus Detection
- Exposure of User Passwords in referrer Header
- Exposure of JBoss Server Over the internet
- Phishing Mail Detected
- Connection to Domain with Malicious File
- Cisco Firepower Intrusion Detections
- End User DNS Queries to Unauthorized DNS server
- Excessively Denied Connections from an External Country Followed by Success
- Outbound HTTPS Request to Malicious Destination
- Attack Observed from an external IP
- Malicious Attack Type Observed from Single Malicious IP

SOC Maturity Assessment Based on CRG

In 2081, Cryptogen Nepal evaluated its SOC maturity using Nepal Rastra Bank's Cyber Resilience Guidelines (**CRG 2023**) as the core benchmark. The assessment specifically focuses on two critical domains: Detection (**Section E**) and Response & Recovery (**Section F**). Each criterion is mapped to its corresponding CRG reference (e.g., E.II.76, F.II.87), and is evaluated across key parameters such as implementation status, maturity level, and relevance to the bank's operational and strategic goals. The goal of this assessment is not only to meet compliance requirements but to guide the continuous improvement of SOC functions in alignment with industry best practices and NRB's cyber resilience expectations.

Section E – Detection Domain Assessment

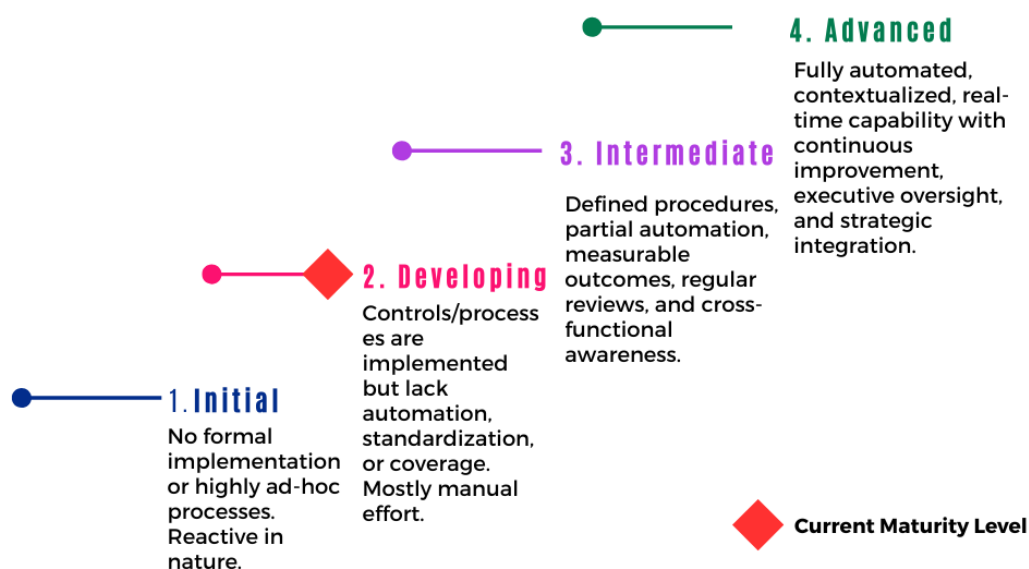
Ref. (CRG)	Guideline Requirement	Current Status	Maturity Level
E.II.76	Continuous monitoring against baseline profiles	FortiSIEM in place lacks UEBA module.	Developing
E.II.77.a	Automated detection systems to correlate network and system alerts	Integrated all endpoints, AD, WAF logs into SIEM, lacks visibility on logs for correlations	Intermediate
E.II.77.b-c	Monitor user activity, remote connections, devices	Partial logging; no endpoint logs	Developing
E.II.77.d-e	Alert thresholds and trigger-based response	Static thresholds defined manually	Initial
E.II.78.a	Analyze behavioral patterns for anomalies	Working on behavior profiling or context-based alerting, need more data.	Initial
E.II.78.b	Use threat intelligence for detection	Tuning required for FortiGuard	Developing
E.II.80	Prevent lateral movement; detect progression	Enabled network visibility for threat propagation	Intermediate
E.II.81	Regular review and testing of detection capabilities	Review and testing done every month by SIEM engineers	Developing
E.II.82-85	Logging, time sync, forensic readiness	Syslog and NTP in place	Intermediate
E.II.86	Centralized event correlation via SOC	SOC in place with dashboards, SLA-based response workflows.	Intermediate

Section F – Response and Recovery

Ref. (CRG)	Guideline Requirement	Current Status	Maturity Level
F.II.87	Cyber incident response capability (detection, containment, recovery)	IR plan exists but is not regularly tested	Developing
F.II.88–89	Root cause analysis and damage assessment	RCA only done for major incidents	Developing
F.II.90	Immediate containment while investigation is ongoing	Ad hoc containment using firewall blocks	Initial
F.II.95–96	Resume operations within 2 hours (RTO)	RTO plan exists but untested	Initial
F.II.97–99	Backup strategy and contingency if RTO fails	Backups taken	Developing
F.II.102–103	Include threat scenarios and consult all business units	Partial involvement of business units	Initial
F.II.104–106	Regular testing and improvement of IR plans	Testing not standardized	Initial

SOC MATURITY MODEL

4 STEPS



Based on the assessment, the organization is currently at the Developing stage of maturity. This conclusion is drawn from the weighted average score of 1.88, calculated using the distribution of ratings across 17 evaluated areas:

- 6 areas are at the Initial level

- 7 areas are at the Developing level
- 4 areas are at the Intermediate level
- 0 areas at Advanced level

This indicates that while some foundational practices are in place, there is still significant room for growth. Continued focus should be placed on standardizing processes, enhancing documentation, and moving more areas from Initial to Intermediate or Advanced maturity levels.

Strategic Improvements & Recommendations for 2082/83

- Tune rules to minimize false positives in incident detection.
- Upgrade the platform to address bugs in older versions and leverage new features.
- Enable endpoint logs for improved visibility and analysis.
- Integrate DNS query logs into SIEM for better detection of DNS-related anomalies.
- Formalize incident response (IR) runbooks and create playbooks for common scenarios (e.g., malware, insider threats, DDoS).
- Run simulation exercises to assess the feasibility of meeting the two-hour recovery time objective (RTO).
- Document and test alternative recovery procedures, including manual fallback, for incident response and recovery.
- Hold tabletop exercises to increase awareness across core banking, finance, and IT teams.
- Regularly test incident response processes to ensure preparedness for future incidents.

Planned Initiatives for 2082/83

- Creating a Playbooks and testing for Incident Response
- Planning for routine based usecases development
- Tune False Positive Incident
- Improvement on deliverables
- Reducing SOC MTTD & MTTR

Conclusion

The year 2081/82 brought a surge in both the sophistication and volume of cyber threats. Despite these challenges, the SOC team has consistently delivered quality in threat detection, response, and prevention. We remain committed to secure XYZ Bank's Digital assets.

Appendix

This appendix outlines the methodology used to evaluate the Security Operations Center (SOC) maturity of XYZ Bank with reference to **NRB's Cyber Resilience Guidelines (CRG) 2023**, specifically **Section E (Detection)** and **Section F (Response & Recovery)**.

Scoring Scale

Each guideline was evaluated using a **4-tier maturity scale**.

Level	Label	Definition
1	Initial	No formal implementation or highly ad-hoc processes. Reactive in nature.
2	Developing	Controls/processes are implemented but lack automation, standardization, or coverage. Mostly manual effort.
3	Intermediate	Defined procedures, partial automation, measurable outcomes, regular reviews, and cross-functional awareness.
4	Advanced	Fully automated, contextualized, real-time capability with continuous improvement, executive oversight, and strategic integration.

OUR SERVICES

Our Services As Information
Security Company Includes:

- SECURITY OPERATIONS CENTER
- INFORMATION SECURITY AUDIT
- SWIFT CSP ASSESSMENT
- DARKWEB MONITORING & BRAND PROTECTION
- VULNERABILITY MANAGEMENT
- PENETRATION TESTING
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER CONFIGURATION ASSESSMENT
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING



CryptoGen Nepal



/cryptogennepal
www.cryptogennepal.com

+977-1-4528928

whois@cryptogennepal.com