Cyber Security Management Internal Risk Assessment Report

VERSION 1.0 **DATE: 11/09/2024**

Auditee Details

Name: xyzanushika

Designation: xyz

Office Name: xyz

Department: Others

Centre for Entrepreneurship Development Madhya Pradesh (CEDMAP)
Under Department of MSME, Govt of Madhya Pradesh

IMPLEMENTING AGENCY

Cyber Law Pioneers

CONTENTS

1. Preface

This 'Cyber Security Internal Risk Assessment' is a part of our training program. Trainee will participate and submit this assessment report for understanding, study and establish cyber security measures and controls within government organization. This report may contains organization/department confidential information and is prepared in confidence to the officers/employee for their internal use and research. While the report serves as a useful reference and may be used by officer/employee with the approval of consent authority.

While the information provided is based on current best practices, policy and standards prescribed and recommended by Central and State Government for cyber security given below: While the information provided is based on current best practices, policy and standards prescribed and recommended by Central and State Government for cyber security given below:

- Guidelines on Information Security Practices for Government Entities Issued by Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics and Information Technology Government of India
- Guidelines on Information Security for Protection of Critical Information Infrastructure issued by Cert-In (Cert-in/NISAP/01, 01 May 2006)
- CYBER SECURITY AUDIT BASELINE REQUIREMENTS (NSCS-46-16 October 2020) Issued by NATIONAL SECURITYCOUNCILSECRETARIAT of Government of India
- MANUAL ON SAFETY AND SECURITY OF CHILDREN IN SCHOOLS Developed by NATIONAL COMMISSION FOR PROTECTION OF CHILD RIGHTS

2. Executive Summary

The main objective is to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising infommtion security awareness among all stakeholders with a vision to facilitate safe, secure and resilient Information Infrastructure.

To protect against cyber threats, it is important for government entities to implement strong cybersecurity measures and follow best practices. As ICT infrastructure of the Government entities is one of the preferred targets of the malicious actors, responsibility of implementing good cyber security practices for protecting computers, servers, applications, electronic systems, networks, and data from digital attacks, also remain with the ICT assets' owner i.e. Government entity.

The purpose of this Cyber Security Management Internal Risk Assessment is to establish a prioritized baseline for cyber security measures and controls within government organizations and their associated organizations. The Internal Risk Assessment shall assist security teams to implement baseline and essential controls and procedures to protect their Cyber infrastructure from prominent threats.

This internal risk assessment cover best practices segregated in different security domains such as Network Security, Application Security, Data Security, Auditing, Third Party Outsourcing. Due to the ever-evolving threat landscape, this document is envisaged to be an organic document and would be updated as per changing threat landscape. Also provides department/office with insight into the resilience of its systems to withstand attacks from unauthorized users and the potential for valid users to abuse their privileges and access.

3. Controls

Cybersecurity audit controls recommended by Cert-In and NCIIPC are systematic measures and procedures used to evaluate the effectiveness of an organization's cybersecurity practices. These controls ensure that security policies and procedures are not only designed correctly but also implemented and functioning as intended. The main objectives of these cyber security assessment are to identify vulnerabilities, ensure compliance with regulations, and enhance overall security posture.

The families of controls into which the Cyber Security Management Internal Risk Assessment for the protection of organization have been divided are:

- General Security
- Desktop/Laptop/Printer Security
- Network & Infrastructure Security
- Email Security
- Social Media Security
- Internet Browsing Security
- Removable Media Security
- Mobile Phone Security

These controls are taken from the guidelines and instructions issued by Cert-In & NCIIPC.

4. Methodology

a. An account will be created on the web portal for training registration and other tasks, in which a special process will be created for CSM INTERNAL RISK ASSESSMENT.

b. Options will be given in the online sheet on different topics for internal risk assessment, in which the trainee will answer according to the condition and knowledge of the office.

c. During training, every trainee can ask controls related questions through questionnaire options given in the online account.

d. All trainees can take internal risk assessment twice.

f. Once trainee will submit the assessment, the expert will review the report and if there will be any deficiency or non compliance found then reject the report with suggestions. Trainee will get one more chance to submit the assessment again with appropriate correction. After second submission, tramee will get final report.

5. Risk Rating

The risk rating for each finding in this report is based on CYBER SECURITY AUDIT BASELINE REQUIREMENTS issued by NATIONALSECURITY COUNCIL SECRETARIAT of Government of India. Here's a guide to interpreting the risk rating:

As per Clause 06 of CYBER SECURITYAUDIT BASELINE REOUIREMENTS Organisation's Cyber Infrastructure is classified into three risk profiles. These risk profile classifications need to be done by the organisation themselves and as an outcome of risk assessment: -

(a) High Risk Information Infrastructure: Cyber-attack or disruption to cyber infrastructure will have impact on national security, public health & safety, economy, critical government operations or critical operations of the organisation.

(b) Medium Risk Information Infrastructure: Cyber-attack or disruption to cyber infrastructure will have impact limited within organisation and its dependencies but essential services of organisation will get affected.

(c) Low Risk Information Infrastructure: Cyber-attack or disruption to cyber infrastructure will have minimal impact on functions of the organizations.

6. Goals and Objectives

As part of our cyber security training program our team evaluated the protection of its people, process, data, systems and networks to ensure that controls are in place. The objectives of this assessment are highlighted below:

- To identify technical as well as logical vulnerabilities/weaknesses in the application and provide recommendations for risk mitigation.
- To implement cyber security management system in the office.
- To trained the officers and other stakeholders to identify the risk and related cyber security measures.

7. Scope

The internal self-risk assessment will include the physical and logical security of computer resources, data and other technical equipment installed and used in the office/school premises and compliance with applicable law.

The internal audit will cover important topics like desktop security, internet security, safe use of social media, mobile phone security, digital signature, electronic payment system, etc.

8. Findings

Assessment	**Answer**	**Risk**	**Admin Status**	**Suggestion**
Only use authorized and approved removable media devices provided by the organization.	Yes	Low	Compliance	
Bring Your Own Device (BYOD) should be restricted and no unknown devices should be allowed in the network without authorization by the Network Administrator.	No	Low	Non-Compliance	na
Whether official email ID registered with Bank Account used by other employee other than appropriate authority?	NA	Low	Compliance	no

Whether Standard User (non-administrator) account is set for the user for accessing the computer/laptops for regular work?	Yes	Medium	Non-Compliance	na
Data must not be shared with outsiders without explicit & case specific approval of authority	No	High	Non-Compliance	Not suppoted
general control	Yes	Low	Compliance	

9. Disclaimer

The findings and recommendations contained in this report are based on the data and circumstances available at the time of the assessment and may not cover all potential vulnerabilities or threats. The detailed information given in this report is provided by participant on the basis of his/her practice and knowledge and the same is assessed by the expert team of CEDMAP for the purpose of training.

10. Conclusion

The Cybersecurity Internal Self-Risk Assessment Report provides a valuable overview of the current cybersecurity posture within the department/office. This assessment highlights key areas of strength and identifies potential vulnerabilities, offering a foundational understanding of the department's risk landscape. While the report serves as a useful reference, it is crucial to recognize that cybersecurity is an ongoing process that evolves with emerging threats and technological advancements. The recommendations provided should be considered as starting points for enhancing security measures rather than comprehensive solutions.

Implementing the recommended actions and continually reviewing and updating security practices will help mitigate risks and strengthen overall cybersecurity resilience.