

Document Name	CSE Critical IT Asset Policy & Register with Cyber Risk Matrix
Document Creation Date	22/06/2022
Document Created By	CISO-CSE
Version Control History	1.4
Document Reviewed Date	05/12/2024
Document Reviewed By	CISO-CSE & CRO-CSE
Document Approved By	Standing Committee on Technology

CSE Critical IT Asset Policy & Register

Overview:

A cyber security risk assessment matrix is a tool that provides a graphical depiction of areas of risk within an organization's digital ecosystem or vendor network.

Objective:

A critical asset risk register is a tool in risk management. It is used to identify potential risks in a particular project or across a company, sometimes to fulfill regulatory compliance but generally to stay on top of potential issues that can derail company objectives relating to critical IT assets.

Scope:

IT risks include hardware and software failure, human error, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods. You can manage IT risks by completing a business risk assessment. Having a business continuity plan can help your business recover from an IT incident separately. Therefore maintaining the critical asset register is the starting point of addressing a disaster if happens in IT and restore it at the earliest possible time by addressing the critical part maintenance. The Scope of this document covers CSE as well as its subsidiary CCMPL.

CSE IT Asset Register and Cyber Risks Matrix

Sl. No.	Asset Category	Asset Name	Nature (Hardware / Software)	Version	Asset Owner	Operation Criticality (High Medium, Low)	Cyber Risk Matrix (High Medium, Low)	Cybersecurity risk	Mitigation measure	Asset Location	Any Remarks
1	<i>Application Server</i>	ODIN Manager	Hardware	HP Proliant DL360G7	ITD	High	High	Low	Firewall	7, LR, Mezz FL	
2	<i>Database Server</i>	ODIN Database	Hardware	HP Proliant DL360G5	ITD	High	High	Low	Firewall	7, LR, Mezz FL	
3	<i>Test Server</i>	ODIN & Class UAT	Hardware	HP Proliant DL120G6	ITD	Low	Low	Low	Firewall	7, LR, Mezz FL	
4	<i>File Server</i>	FTP Server	Hardware	HP Proliant DL120G6	ITD	Medium	Low	High	Firewall	7, LR, Mezz FL	

5	NSE Server	TAP Server	Hardware	HP Proliant DL120G6	ITD	Low	Low	Low	Firewall	7, LR, Mezz FL	
6	Application Server	Class BO Application	Hardware	HP Proliant DL360G5	ITD	High	Low	Low	Firewall	7, LR, Mezz FL	
7	Database Server	Class BO Database	Hardware	HP Proliant DL580G4	ITD	High	Low	Low	Firewall	7, LR, Mezz FL	
8	Application and Database Server	Listing XBRL Server	Hardware	HP Proliant ML30	Listing	High	Low	High	Firewall	7, LR, 4th FL	
9	Application and Database Server	NSDL DP	Hardware	HP Proliant ML360G8	CCMPL	High	Low	Low	Firewall	7, LR, Gr FL	
10	Application and Database Server	DP Back-office	Hardware	HCL Desktop	CCMPL	Low	Low	Low	Firewall	7, LR, Gr FL	
11	Application Server	iBOS Application	Hardware	IBM x3220M4	Accounts	High	Low	Low	Firewall	7, LR, 4th FL	
12	Database Server	iBOS Oracle Database	Hardware	IBM x3400M4	Accounts	High	Low	Low	Firewall	7, LR, 4th FL	
13	Firewall Router	Fortigate 80C	Hardware	Fortigate 80C	ITD	High	Low	Low	Firewall	7, LR, Mezz FL	
14	Router	Core Router	Hardware	HP	ITD	High	Low	Low	Firewall	7, LR, Mezz FL	
15	Firewall Router	Office Internet Firewall	Hardware	SOPHOS SG210	ITD	High	Low	High	Firewall	7, LR, Mezz FL	
16	Desktops	Desktop used by IT Team to connect critical Servers	Hardware	HP/HCL/Lenovo	ITD	Low	Low	Low	Firewall	7, LR, Mezz FL	
17	Desktops of Manager MOP	Hardware	HP/HCL/Lenovo	ITD	Low	Low	Low	Firewall	7, LR, Mezz FL	Hardware	
18	Desktop Used by Manager Surveillance	Hardware	HP/HCL/Lenovo	ITD	Low	Low	Low	Firewall	7, LR, Mezz FL	Hardware	
19	Desktop Used by CISO	Hardware	HP/HCL/Lenovo	ITD	Low	Low	Low	Firewall	7, LR, Mezz FL	Hardware	
20	Desktop used by IT Executive	Hardware	HP/HCL/Lenovo	ITD	Low	Low	Low	Firewall	7, LR, Mezz FL	Hardware	
21	VPN Box	VPN	Hardware	Pulse Secure PS3000	ITD	High	Low	Low	Firewall	7, LR, Mezz FL	
22	Antivirus Server	Kaspersky	Software	Kaspersky	ITD	Low	Low	Low	Firewall	7, LR, Mezz FL	

Note 2- Usage of Firewalls, VPNs, Password Policy, Internet Access Policy, Antivirus, Patch Management, Physical Security, Access Control etc.

Version Control History

Version Change Date: 17/05/2023

Version Number: 1.3

Changes:

- Introduction of Overview, Objective, Process and Scope
- Introduction of Version control History

Version Change Date: 18/09/2023

Version Number: 1.4

Changes:

- Changes in updated list. Exclusion of few servers as they are not being used. Inclusion of CISO & senior officers desktop in the list because they have access and connect to the critical servers as per auditor's advice.