Step 4: Risk Treatment

Step 4.1: Risk Treatment and Calculation of Residual Risk for Supporting Assets

Supporting Assets (same as specified in step 2.1)	*Threats (same as specified in step 3.1)*	*Vulnerability (same as specified in step 3.1)*	*Pre-Controls*	*Post-Controls*	*Reviewed Impact (from step 3.1)*	*Likelihood (from step 3.2)*	*Residual Impact*	*Residual Likelihood*	*Residual Risk level (from Table 3.1)*
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authenticati on	Deploy latest version of the hypervisor software	Reset admin credentials	5	4	4	2	MEDIUM
			Configure hard logical separation between hypervisor and guest OSs	Backup hijacked hypervisor image for forensics					
			Backup the hypervisor configuration	Restore configuration					
			Keep hypervisor management traffic separated from users traffic	Disaster recovery					
	Ransomware	Poor controls on installed software	Use approved removable drives only	Backup hypervisor image for forensics	4	4	2	3	LOW
			Backup the hypervisor configuration	Restore hypervisor configuration					
			Keep logs of installation requests	Re-distribute software					
			Deploy latest version of the hypervisor software and latest version of the guest OSs	Re-deploy guest machines					
	Hypervisor server crash	Faulty load balance on Citrix delivery controllers	Test the virtualization server configuration	Restore hypervisor configuration	4	3	3	2	LOW
			Backup the hypervisor configuration	Re-deploy guest machines					
	Session Hijacking	CVE-2021-22927	Upgrade to Citrix ADC and Citrix Gateway 13.0-82.41 or later releases	MAV:N/MAC:L/MPR:N/MUI:R/MS:U/MC:N/MI:N/MA:N	4	3	1	3	LOW
			Modify the device's SAML action&profile configurations accordingly to what stated in the						
GSB PCs	Damaged hardware	Poor manifacturing	Test systems before deploying	If the equipment has a backup appliance, use backup	4	3	3	1	LOW
			Buy some backup PCs	Disaster recovery					
	Physical key loggers	Poor physical access control	Check I/O hardware before deploying	Check for misconduct tied to user credentials	3	4	3	2	LOW
				Reset users credential					
	Reverse Shell Attack	CVE-2022-38652	Run the software on a Linux based OS	MAV:N/MAC:L/MPR:L/MUI:N/MS:C/MC:N/MI:N/MA:N	4	4	1	4	MEDIUM
	Ballots data tampering	CVE-2018-6683	Update McAfee DLP to build 10.0.505 / 11.0.405 or later	MAV:P/MAC:L/MPR:L/MUI:N/MS:C/MC:N/MI:N/MA:N	4	3	1	3	MEDIUM
GSB LAN gateway	Network tapping	Broken physical access control	Audit personeel access to secure room	Reset passwords for interested GSB	2	4	1	1	LOW
			Put security officer at entry point	Remove network tap					
			Adopt CCTV cameras						
	Configuration tampering	Broken access control	Backup gateway configuration	Disaster recovery	3	4	3	2	LOW
			Deploy with latest firmware						
			Check for vulnerabilities and official fixes / workarounds						
	Route table poisoning	CVE-2016-7406	Update Dropbear suite to version >= 2016.74	MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:N	4	5	1	5	MEDIUM