Step 3: Risk Evaluation

Step 3.2: Risk Evaluation

Supporting Assets(same as specified in step 2.1)	***Threats (same as specified in step 2.1)***	***Vulnerability (same as specified in step 2.1)***	***Reviewed Impact (from step 2.1)***	***Likelihood (from step 2.2)***	***Risk level (from Table 3.1)***
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authentication	5	4	HIGH
	Ransomware	Poor controls on installed software	4	4	HIGH
	Hypervisor server crash	Faulty load balance on Citrix delivery controllers	4	3	HIGH
	Session Hijacking	CVE-2021-22927	4	3	HIGH
DHV Software	Software crash	Unhadled software exeptions	4	2	MEDIUM
	False Data Input	Faulty access control	4	3	HIGH
Citrix server room(s)	Floods	Lack of flood preventing infrastrucutre	4	3	HIGH
	Fires	Faulty fire coutermeasures	4	2	MEDIUM
	Theft of equipment	Poor physical access control	4	4	HIGH
	Overheating	Faulty cooling system	4	3	HIGH
GSB PCs	Damaged hardware	Poor manifacturing	4	3	HIGH
	Physical key loggers	Poor physical access control	3	4	HIGH
	Reverse Shell Attack	CVE-2022-38652	4	4	HIGH
	Ballot data tampering	CVE-2018-6683	4	3	HIGH
Secure Store for GSB PCs	Flood	Lack of flood preventing infrastrucutre	4	3	HIGH
	Fires	Faulty fire coutermeasures	4	2	MEDIUM
	Theft	Poor physical access control	4	4	HIGH
	Hardware damaging	Poor physical access control	4	4	HIGH
GSB LAN gateway	Network tapping	Broken physical acces control	2	4	MEDIUM
	Configuration tampering	Broken access control	3	4	HIGH
	Route table poisoning	CVE-2016-7406	3	5	HIGH