				Check audit for misconduct					
Diginetwerk	*Coremelt*	*Communication links have limited bit-rate*	Implement stronger link redundancy	Enforce a probabilistic packages drop in order to punish aggressive flows	4	2	3	1	LOW
			Monitor traffic to detect anomalies						
	Unauthorized wired connection	*Broken physical access control to routers*	Install intrusion prevention system	Check logs of databases and authentication services for malicious	5	3	4	2	MEDIUM
				Disaster recovery					
				Blacklist IP					
	Router crash	*Poor load balancing*	Implement VRRP or proprietary alternative	Automated switch to backup router through VRRP	4	3	1	3	LOW
			Configuration backup	Restore router with backed up configuration					
	Broken link	*Poor network redundancy*	Implement stronger link redundancy	If the link is broken and there is no redundancy, recovery plan is needed	4	3	4	2	MEDIUM
	Downtimes	*Hardware needs power*		Disaster recovery	4	2	4	2	MEDIUM
	Routing loop	*Poor router and L3 switch configuration testing*	Backup configuration	Reset and restore configuration	4	3	3	2	LOW
			Test routers and L3 switch configurations						
VPN	Unauthorized access to virtual network	Poor third party policies	Adopt zero trust model on the perimeter of the VPN tunneling Check incident history of third party provider to select	Disaster recovery	3	4	3	3	MEDIUM
Firewall appliance	System crash	*Poor load balancing*	Install firewall with that supports the required bitrate	Reset firewall with backed up configuration	4	3	2	2	LOW
			Backup firewall configuration						
	Configuration file tampering	*Broken authentication*	Backup firewall configuration	Reset firewall with backed up configuration	4	4	4	2	MEDIUM
			Deploy with latest firmware	Disaster recovery					
			Check for vulnerabilities and official fixes / workarounds						
Virtual Desktop Infrastructure (Citrix)	Hyperjacking	Broken authorization&authenticatio n	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					
DHV Software	Sotware crash	Unhadled software exeptions	Perform unit testing	Disaster recovery	4	2	4	1	MEDIUM
	False Data Input	Faulty access control	Adopt least priviledge access control	Disaster recovery	4	3	4	2	MEDIUM
			System logs and audit						
Citrix server room(s)	Floods	Lack of flood preventing infrastrucutre	Avoid using rooms with water pipes behind walls	Disaster recovery	4	3	4	2	MEDIUM
			Define flood response roles and train personeel						
			Put server room on second floor or above						
	Fires	Faulty fire countermeasures	Define fire response roles and train personeel	Disaster recovery	4	2	4	1	MEDIUM
			Install fire suppression system with inert gas						
	Theft of equipment	Poor physical access control	Adopt CCTV cameras	If the equipment has a backup appliance, use backup	4	4	4	1	MEDIUM
			Use biometrical access control	Disaster recovery					
			Audit personeel access to server room						
	Overheating	Faulty cooling system	Install temperature sensors	If the equipment has a backup appliance, use backup	4	3	4	1	MEDIUM
			Adopt enclosed hot aisles	Disaster recovery					
			Switch off unnecessary and reduntant hardware when the temperature raises up						
			Perform due maintenance on the AC						
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					
Secure Store for GSB PCs	Flood	Lack of flood preventing infrastrucutre	Define flood response roles and train personeel	Disaster recovery	4	3	4	2	MEDIUM
			Avoid using rooms with water pipes behind walls						
			Put store room on second floor or above						
	Fires	Faulty fire countermeasures	Install fire alarms	Disaster recovery	4	2	4	1	MEDIUM
			Define fire response roles and train personeel						
			Buy inert fire estinguishers						
	Theft	Poor physical access control	Audit personeel access to secure room	If the equipment has a backup appliance, use backup	4	4	4	1	MEDIUM
			Put security officer at entry point	Disaster recovery					
			Adopt CCTV cameras						
	Hardware damaging	Poor physical access control	Audit personeel access to secure room	If the equipment has a backup appliance, use backup	4	4	4	1	MEDIUM
			Put security officer at entry point	Disaster recovery					
			Adopt CCTV cameras						
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						