A	B	C	D	E	F
What are the hazards?	**Who might be harmed and how?**	**What are you already doing to control the risks?**	**What further action do you need to take to control the risks?**	**Who needs to carry out the action?**	**When is the action needed by?**
Lone Working - Out of hours work installing physical	Slips/trips/falls with heavy equipment whilst alone	No controls in place	Introduction of lone working policy/regular check-ins with line manager to confirm safety. 'Home Safe' call at end of work to confirm all is well.	Policy to be implemented by IT Manager. Compliance should be ongoing by technician.	commencement of project
Lone Working - Working in Server room in isolation	Server room is a locked/temperature controlled environment. Risk of becoming trapped in event of fire/Halon protection being deployed.	No controls in place	All server room working must be notified to manager before start and at end of session. Server room to be left open while staff are working inside. locks should fail open to allow safe escape in event of emergency	Policy to be implemented by IT Manager. Compliance should be ongoing by technician.	commencement of project
Lone working - out of hours	Increased threat of attack from malicious actor resulting in a physical assault	No controls in place	Introduction of lone working policy. Check-in phonecalls to line manager. End of shift safe call to confirm all is well. installation of CCTV to detect intruders and to act as deterrent.	Policy to be implemented by IT Manager. Compliance should be ongoing by technician.	commencement of project
Manual Handling - Moving of heavy PCs, switches and servers as part of installation process	threat of back injury due to lifting heavy items or poor lifting technique	No controls in place	Manual Handling Training Manual Handling Policy introduced Provision of Trolleys or wheels for moving equipment 2 person lift requirement for larger items.	Policy to be implemented by IT Manager. IT manager to organise Manual Handling Training. IT Manager to provide wheels/trolleys. Compliance should be ongoing by technician.	Policy should be prepared prior to project commencement, all manual handling training completed before manual tasks are completed.
Working at Height - installation of network cabling on site	risk of fall from ladder resulting in physical injury	No controls in place	Working at height training (ladders). Introduction of 2 persons working for any height related task. Ladders should be held whilst in use.	Policy to be implemented by IT Manager. Compliance should be ongoing by technician.	commencement of project
Fire Safety - risk of fire from papers being left on top of computers etc	injury or potential death through burns/smoke inhallation	No controls in place	Clear desk policy preventing paperwork from blocking vents etc on computers.	Compliance by all staff	Immediate
Fire safety - risk of fire from faulty electrical equipment	injury or potential death through burns/smoke inhallation	No controls in place	Annual PAT testing of equipment to ensure they are fit for purpose. no personal equipment should be plugged in	PAT Testing schedule managed by IT Manager	within 12 Months of purchase
Electric Shock - risk of shock from faulty equipment	Electric shock resulting in serious injury or death	No controls in place	annual PAT testing of equipment to ensure they are fit for purpose no personal equipment should be plugged in	PAT Testing schedule managed by IT Manager	within 12 Months of purchase
Display screens and workstations	Eye strain from poor lighting on monitor	No controls in place	Annual Display Screen/Workplace assessment by qualified H&S	IT Manager	Every 12 months

... | 1 - H&S Risk Assessment | 2 - Inventory Log | 3 - Security Risk Assessment | 4 - Software Install Log

Wrist pain/rsi from poor keyboard/mouse positioning	No controls in place	Annual Display Screen/Workplace assessment by qualified H&S representative	IT Manager	Every 12 Months
Back Pain from inappropriate chair usage	No controls in place			

Switch	N/A			Manual	192.168.0.220	Server Room	10 Port Switch for Backbone
Switch	N/A			Manual	192.168.0.221	Server Room	40 Port Switch for Client Connectivity
Switch	N/A			Manual	192.168.0.222	Server Room	41 Port Switch for Client Connectivity
Switch	N/A			Manual	192.168.0.223	Server Room	42 Port Switch for Client Connectivity
Printer	PRN01			Manual	192.168.0.10	Workplace	
Printer	PRN02			Manual	192.168.0.11	Workplace	
Printer	PRN03			Manual	192.168.0.12	Workplace	
Printer	PRN04			Manual	192.168.0.13	Workplace	
Printer	PRN05			Manual	192.168.0.14	Workplace	
Gateway Router	N/A			Manual	192.168.0.254	Server Room	Provides internet access to the nextwork

Device Type	Device Name	Serial No.	MAC Address	IP Assignment Method	IP Address	Location	Notes
Server	DC01	123456789	44-BA-E7-97-8A-6B	Manual	192.168.0.1	Server Room	
PC	PC001			DHCP	**Auto Assigned**	Workplace	
PC	PC002			DHCP	**Auto Assigned**	Workplace	
PC	PC003			DHCP	**Auto Assigned**	Workplace	
PC	PC004			DHCP	**Auto Assigned**	Workplace	
PC	PC005			DHCP	**Auto Assigned**	Workplace	
PC	PC006			DHCP	**Auto Assigned**	Workplace	
PC	PC007			DHCP	**Auto Assigned**	Workplace	
PC	PC008			DHCP	**Auto Assigned**	Workplace	
PC	PC009			DHCP	**Auto Assigned**	Workplace	
PC	PC010			DHCP	**Auto Assigned**	Workplace	
PC	PC011			DHCP	**Auto Assigned**	Workplace	
PC	PC012			DHCP	**Auto Assigned**	Workplace	
PC	PC013			DHCP	**Auto Assigned**	Workplace	
PC	PC014			DHCP	**Auto Assigned**	Workplace	
PC	PC015			DHCP	**Auto Assigned**	Workplace	
PC	PC016			DHCP	**Auto Assigned**	Workplace	
PC	PC017			DHCP	**Auto Assigned**	Workplace	
PC	PC018			DHCP	**Auto Assigned**	Workplace	
PC	PC019			DHCP	**Auto Assigned**	Workplace	
PC	PC020			DHCP	**Auto Assigned**	Workplace	
PC	PC021			DHCP	**Auto Assigned**	Workplace	
PC	PC022			DHCP	**Auto Assigned**	Workplace	
PC	PC023			DHCP	**Auto Assigned**	Workplace	
PC	PC024			DHCP	**Auto Assigned**	Workplace	
PC	PC025			DHCP	**Auto Assigned**	Workplace	
PC	PC026			DHCP	**Auto Assigned**	Workplace	
PC	PC027			DHCP	**Auto Assigned**	Workplace	
PC	PC028			DHCP	**Auto Assigned**	Workplace	

RISK REGISTER			Risk Rating				
ID	Status	Description	Probabilit	Impact	Proximity	Rating	Proposed Mitigation Action(s)
R1	Open	Removable Media - potential for data to be lost due to loss of USB drives ETC	Likely	High	<= 3 Mont	20	*Implement Bitlocker to Go on all removable media - enforced by GPO*
R2	Open	Data loss - potential for attacker to intercept confidential emails in transit	Possible	High	>= 6 Mont	13	All confidential documents should be encrypted before sending with passwords provided to recipient separately.
R3	Open	Data Loss - hard copies of data falling into malicious hands via activity such as dumpster diving	Unlikely	High	>= 6 Mont	9	Utilise Data Loss Prevention solution to prevent unauthorised printing of documents. Ensure shredding facilities are easily accessible to all staff. Introduce Data protection policy to enforce shredding of documents.
R4	Open	Data Loss - due to malicious attack on company server	Possible	High	>= 6 Mont	13	Ensure Endpoint software is up to date. Ensure firewall configuration is verified and secure. Server should be hardened to minimise potential attack surface.
R5	Open	Data loss through Data Hijacking - ransomware attack	Likely	High	<= 2 Mont	21	Mandatory training for all staff regarding Phishing Attacks. Implementation of Endpoint Protection software ensure EP software updates are maintained. Introduce malware reporting email
R6	Open	Data loss or malicious attack through compromised passwords being used by malicious actor	Likely	High	<= 2 Mont	21	Mandatory phishing training for all staff. Mandatory password training for all staff. Implementation of complex password policy through Group Policy. Introduction of two factor authentication for logging into systems
R7	Open	Data loss through data being copied to personal phones	Likely	Medium	< 2 weeks	19	Implement ban on use of personal devices for company data.
R8	Open	Data loss through loss of company phc	Likely	High	<= 3 Mont	20	Mobile device management software introduced. Remote lock and remote wipe set up in case of lost devices. Requirement for pin number or biometrics for access to company mobile devices
R9	Open	DDOS attack on company server preventing access to resources	Unlikely	Medium	>= 6 Mont	7	Ensure firewall is configured to prevent access for ICMP traffic.

Device ID:	DC01	Location:	Server Room		
Installed Date:	14th Oct 2020	Installed By	Dan Troke	Install Type	Full Installation
Software / Drivers Installed	Notes: Windows Server 2016 Datacenter (Desktop Experience) Eset Antivirus software				
Installation Notes	Notes: All Drivers were automatically installed as part of the Windows Installation Server Roles - ADDS / DNS / DHCP added to server Local Admin Details: Administrator/ionsiTypl4				
Vulnerabilities Notes	Notes: All software is up to date including AV and Operating System USB ports are live allowing USB drives etc to be plugged in that could allow viruses to be maliciously added or potential for an attacker to compromise the system One server is installed for all roles with no duplicate				
Recommended Actions	Notes: Disable Server USB ports to prevent unauthorised access Install a second server and configure as a cluster to remove single point of failure.				

Device ID:	PC001	Location:	Workplace		
Installed Date:	14th Oct 2020	Installed By	Dan Troke	Install Type	Full installation
Software / Drivers Installed	Notes: Windows 10 Professional <Product Key: VTVTN-HYT4R-DVFGR-MYUIT-FVERR> Eset Antivirus Software Office 2019 Software <Product Key: SDFV4-WEFEW-SDVS3-FVF45-DCSD8> Microsoft Teams Microsoft Project 2019 <Product Key: SDFWE-ERGBF-RGBNG-FDVFR-HGNGH>				
Installation Notes	Notes: All drivers were installed automatically as part of the Windows 10 installation. Local Admin details: Admin/ionsiTypl2				
Vulnerabilities Notes	Notes: All Software is up to date including AV and operating system, the Antivirus is set to automatically update the virus definition files on a daily basis.				
Recommended Actions	Notes: It is recomended that the updates are set to automatic and that this is done via a group policy to stop the users turning this feature off again.				

Device ID:	Mobile Device	Location:	Office		
Installed Date:	5th Oct 2020	Installed By	Dan Troke	Install Type	Updates
Software / Drivers Installed	Notes: All OS updates are completed AVG Antivirus (Mobile) Find My Phone				
Installation Notes	Notes: Screen lock implemented Joined to OfficeWifi network				
Vulnerabilities Notes	Notes: All software is up to date including Antivirus software. because of the mobile OS the in built "Store" will flag to the user when the user needs to update the installed software (Apps)				
Recommended Actions	Notes: An "end point" should installed such as Microsoft intune to ensure that mobile devices are better secured. This is an additional element to the Office 365 subscription.				