Numbers Sheet Name	Numbers Table Name	Excel Worksheet Name
RA - Front Cover		
	Table 1	RA - Front Cover
Risk Assessment		
	Table 1	Risk Assessment
Likelyhood Scale		
	"All Drawings from the Sheet"	Likelyhood Scale
Consequence Scale		
	Table 1	Consequence Scale
Risk Acceptance scale		
	"All Drawings from the Sheet"	Risk Acceptance scale
Control Domains and Attributes		
	"All Drawings from the Sheet"	Control Domains and Attributes
Threats		
	"All Drawings from the Sheet"	Threats
Vulnerabilities		
	"All Drawings from the Sheet"	Vulnerabilities
NOTES		
	Table 1	NOTES

Hospital of No-Security

Document information				
Document name	Risk Assessment	**Last updated date**		21.11.2024
Risk assessor name:	Andrei Cirlig (20049583)	**Document Classification:**		
Date created:	18.10.2024			

Asset (describe with authentic citations where possible)	Vulnerability	Vulnerability Code	Threat to IS properties CIA	Threat Code	Consequence (C) Rating	Likelihood (L) Rating	Risk Rating (R = C x L)	Risk Treatment category (Accept/Reduce/ Trasfer/Avoid)	Itemised Mitigations (describe with authentic citations), split into more rows if needed	Control domain from ISO 27002 and its type (https://herts.instructure.com/courses/108403/pages/2-dot-4-1-dot-2-iso-27002-2022-reference-slash-advisory-document?module_item_id=3118336)	Revised likelyhood rating (anwer should be a number from the likelihood table)	Residual Risk Rating	Risk Acceptance Status	Your relavent Policy statement Number addressing the control	
	How could it happen (describe with authentic citations where possible)	Vulnerability code from ISO/IEC 2005:2022(E)	What could happen (describe with authentic citations where possible)	Threat code from ISO/IEC 2005:2022(E)	What is the worse thing can happen? (anwer should be a number from the consequence table)	What are the chances of the event occuring? (anwer should be a number from the likelihood table)									
Electronic Health Record (EHR) System	File read/inclusion vulnerability in the AJP connector in Apache Tomcat(CVE-2020-1938)	VS01, VS02	If the web application allowed file upload and stored those files within the web application then this, along with the ability to process a file as a JSP, made remote code execution possible.	TH05 , TH07, TH10, TO04	4	3	12	Avoid	Patch and Update software(Github 2021) , Input validation and authentication	Management of technical vulnerabilities (Technical/Preventive)	1	3	Low	3.3.5 , 3.4.8 , 3.4.10.7 , 3.4.10.4	
Medical Imaging Workstations (PACS)	DICOM files can contain the header for an executable file(CVE-2019-11687)	VN01 , VS07	The preamble of a DICOM file that complies with this specification can contain the header for an executable file, such as Portable Executable (PE) malware.	TH08, TH23, TH25, TO04	3	3	9	Reduce	Implement an AV (Antivirus) solution on all medical imaging systems.In the situation where an AV solution cannot be installed, processes and procedures have to be in place to scan portable/removable media for suspicious files before introducing the media into the medical network.(CISA 2019)	Protection against malware (Technical/Preventive)	1	3	Low	3.4.9 , 3.3.5 , 3.3.3	
Laboratory Information Management System (LIMS) running on Windows server 2019	Remote code execution vulnerability targeting MS exchange servers(CVE-2021-31206)	VS02, VS13	There is flaw in the parsing of archive-file format for Microsoft Windows or CAB(Cabinet) files. The process does not properly validate a user-supplied path prior to using it in file operations and an attacker can leverage this to execute arbitrary code.	TH13, TH23, TC04, TO04	4	4	16	Avoid	Apply Windows Updates and Patches(CloudSEK2021)	Management of technical vulnerabilities (Technical/Preventive)	1	4	Low	3.3.3 , 3.4.7 , 3.4.10.4	
Diagnostic Equipment (e.g., Ultrasound Machines, MRI Scanners)	Desktop environment escape vulnerability(CVE-2020-6977)	VS02, VS16	Specially crafted inputs can allow the user to escape the restricted environment, resulting in access to the underlying operating system.	TH15, TH23, TI01	3	3	9	Reduce	Ensure there is physical protections in place to prevent the devices from any unauthorized access and encourage security awareness throughout the hospital staff to ensure clinical staff will report any unauthorized person trying to login or otherwise tamper with a medical device.(CISA 2024)	Physical access control (Physical/Preventive)	2	6	Low	3.4.10.10 , 3.3 , 3.4.7	
Hospital Management System (HMS)	privilege escalation issue via the session token parameter(CVE-2023-31498)	VS13, VS01	The system does not have proper session management in place, making it vulnerable to session hijacking.An attacker can register as a patient and obtain a valid session token. With this token, the attacker can then access the Doctor and Admin panels without any authentication credentials.	TH08, TH10, TC02, TO04	4	4	16	Avoid	The system should assign a specific role to each user upon registration and verify the role before allowing access to sensitive areas of the system. Additionally, the system should implement a mechanism to invalidate sessions upon logout or after a period of inactivity.(Github 2023)	Identity & Access Management (People/Preventive)	1	4	Low	3.3.3 , 3.3.5 , 3.4.10.6	
Firewall	Denial of service (DoS) vulnerability (CVE-2024-20353)	VN05, VN08	A vulnerability in the management and VPN web servers.could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition.	TH25, TC01, TI03	3	3	9	Reduce	Cisco has released updates that address the vulnerability.(CISCO 2024)	Management of technical vulnerabilities (Technical/Preventive)	1	3	Low	3.4.10.6 , 3.4.10.9 , 3.4.7	
Cloud Storage Solutions	Server-side request forgery (CVE-2024-31897)	VS02 , VS14	An authenticated attacker can send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	TH10 , TH15, TH25	3	4	12	Avoid	Update the software (IBM 2024) , Implementing strong MFA	Management of technical vulnerabilities (Technical/Preventive)	1	4	Low	3.4.7 , 3.4.10.7	
Data Backup System	Missing encryption of sensitive data vulnerability in login component(CVE-2023-52950)	VS14, VS06	Missing encryption of sensitive data vulnerability in login component allows adjacent man-in-the-middle attackers to obtain user credential via unspecified vectors.	TH08, TH10, TH15, TO04, TO02	3	3	9	Reduce	Use updates and patches provided by the manufacturer (Synology 2024)	Management of technical vulnerabilities (Technical/Preventive)	2	6	Low	3.4.7 , 3.4.8 , 3.4.7	
Access Control Systems (e.g., Biometric Scanners)	Lack of Physical Security for Biometric Scanners	VH08 - Unprotected storage	Biometric scanners that are not physically secured may be susceptible to tampering, theft, or physical attacks.	TH17, TH12, TH10, TO02 , TO01	2	3	6	Reduce	Place biometric scanners in secure, monitored locations to prevent tampering	Physical security (Physical/Preventive)	2	6	Low	3.4.10.10 , 3.3.6 , 3.3.3	
Confidential Information (Physical Copy)	Theft of media or documents due to lack of established monitoring mechanisms for security breaches.	VS04 , VH09, VP06	Sensitive information, such as personal identifiers, financial records, patient data, or proprietary business information, can be stolen or copied by unauthorized individuals.	TH06, TH10, TH20, TO04 , TO01	3	3	9	Reduce	Lock document storage areas and install surveillance to prevent unauthorized access.	Physical security (Physical/Preventive)	2	6	Low	3.4.3 , 3.4.5 , 3.4.3	
IoT-enabled water filtration system	Equipment damage or compromised water quality by a changing filtration settings	VS16 - Unnecessary services enabled	IoT-enabled water filtration systems may have unnecessary open ports or services which attackers could exploit.	TH20, TH15, TI01	3	4	12	Avoid	Monitor for unusual activity and set up alerts for anomalies	Monitoring and alerting (Technological/Detective)	1	4	Low	3.4.10.10 , 3.4.10.8 , 3.4.7	
Human Resource	Intentional/deliberate information leakage attempt	VP06,V018	Organizations CIA will be compromised	TC02,TO04,TH24	4	2	8	Avoid	Information security awareness, education, and training, Disciplinary process	People/Preventive	1	2	Low	3.4.10.5 3.3.3 3.3.2 3.4.10.7	
Laptops/Desktops	Unauthorized access due to lack of access control policy	VO26,VS13,VP06	Potential to data leakage	TH04,TH06,TH08,TH10	3	2	6	Reduce	Using a solid authentication system	Technological/Preventive	1	2	Low	3.4.3 3.4.10.2 3.4.10.5	
Enterprise Software	Misuse of privileges due to lack of audit	VS05,VS06,VS07	Disruptions in the supply chain	TH10,TH13,TH18,TH19	3	2	6	Reduce	Employee training , applying strict security practices	People/Preventive	1	2	Low	3.4.3 3.4.10.2 3.4.10.5 , 3.3.3	

CISA (2024). GE Healthcare Ultrasound Products, Available at: https://www.cisa.gov/news-events/ics-medical-advisories/icsma-20-049-02, Accessed 19/11/2024

CloudSEK(2021).Advisory: 0-day RCE Vulnerability in Microsoft Exchange , Available at: https://www.cloudsek.com/threatintelligence/advisory-0-day-rce-vulnerability-in-microsoft-exchange-actively-exploited-by-threat-actors

CISA (2019). DICOM Standard in Medical Devices, Available at: https://www.cisa.gov/news-events/ics-alerts/ics-alert-19-162-01, Accessed 19/11/2024

Github (2021). Hacking-Vulnerability-CVE-2020-1938-Ghostcat, Available at: https://github.com/Hancheng-Lei/Hacking-Vulnerability-CVE-2020-1938-Ghostcat/blob/main/CVE-2020-1938.md, Accessed 19/11/2024

Github (2023).CVE-2023-31498 - Session hijacking leading to privilege escalation, Available at: https://gist.github.com/captain-noob/aff11542477ddd0a92ad8b94ec75f832, Accessed 19/11/2024

CISCO (2024). Cisco Adaptive Security Appliance , https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2, Accessed 19/11/2024

IBM (2024). Security Bulletin: Multiple security vulnerabilities are addressed with IBM Cloud Pak, Available at: https://www.ibm.com/support/pages/node/7159332 , Accessed 19/11/2024

Synology (2024). Synology-SA-24:11 Synology Active Backup for Business Agent, Available at: https://www.synology.com/en-global/security/advisory/Synology_SA_24_11 , Accessed 19/11/2024

Table A.2 — Example of likelihood scale

Likelihood	Description
5 – Almost certain	The risk source will most certainly reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very high.
4 – Very likely	The risk source will probably reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is high.
3 – Likely	The risk source is able to reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is significant.
2 – Rather unlikely	The risk source has relatively little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is low.
1 – Unlikely	The risk source has very little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very low.

Table A.1 presents an example of consequence scale.

Table A.1 — Example of consequence scale

Consequences	Description
5 – Catastrophic	**Sector or regulatory consequences beyond the organization** Substantially impacted sector ecosystem(s), with consequences that can be long lasting. And/or: difficulty for the State, and even an incapacity, to ensure a regulatory function or one of its missions of vital importance. And/or: critical consequences on the safety of persons and property (health crisis, major environmental pollution, destruction of essential infrastructures, etc.).
4 – Critical	**Disastrous consequences for the organization** Incapacity for the organization to ensure all or a portion of its activity, with possible serious consequences on the safety of persons and property. The organization will most likely not overcome the situation (its survival is threatened), the activity sectors or state sectors in which it operates will likely be affected slightly, without any long-lasting consequences.
3 – Serious	**Substantial consequences for the organization** High degradation in the performance of the activity, with possible significant consequences on the safety of persons and property. The organization will overcome the situation with serious difficulties (operation in a highly degraded mode), without any sector or state impact.
2 – Significant	**Significant but limited consequences for the organization** Degradation in the performance of the activity with no consequences on the safety of persons and property. The organization will overcome the situation despite a few difficulties (operation in degraded mode).

Table A.1 *(continued)*

Consequences	Description
1 – Minor	**Negligible consequences for the organization** No consequences on operations or the performance of the activity or on the safety of persons and property. The organization will overcome the situation without too much difficulty (margins will be consumed).

5x5 Risk Matrix Example

Impact

How severe would the outcomes be if the risk occurred?

What is the probability the risk will happen?

Probability

	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

SafetyCulture

Level of risk	Risk evaluation	Description
Low (green)	Acceptable as is	The risk can be accepted without further action.
Moderate (amber)	Tolerable under control	A follow-up in terms of risk management should be conducted and actions should be set up in the framework of continuous improvement over the medium and long term.
High (red)	Unacceptable	Measures for reducing the risk should absolutely be taken in the short-term. Otherwise, all or a portion of the activity should be refused.

Domain	Number of Controls
Organisation	37
Physical	14
People	8
Technological	34

Control Type	Information Security Principles	Cyber Security Concepts	Operational Capabilities	Security Domains
• Preventative • Detective • Corrective	• Confidentiality • Availability • Integrity	• Identify • Protect • Detect • Respond • Recover	• Governance • Human Resource Security • Identity & Access Management • Asset Management • Information Protection	• Governance & Ecosystem • Protection • Defence • Resilience

Table A.10 — Examples of typical threats

Category	No.	Threat description	Type of risk source [a]
Physical threats	TP01	Fire	A, D, E
	TP02	Water	A, D, E
	TP03	Pollution, harmful radiation	A, D, E
	TP04	Major accident	A, D, E
	TP05	Explosion	A, D, E
	TP06	Dust, corrosion, freezing	A, D, E
Natural threats	TN01	Climatic phenomenon	E
	TN02	Seismic phenomenon	E
	TN03	Volcanic phenomenon	E
	TN04	Meteorological phenomenon	E
	TN05	Flood	E
	TN06	Pandemic/epidemic phenomenon	E
Infrastructure failures	TI01	Failure of a supply system	A, D
	TI02	Failure of cooling or ventilation system	A, D
	TI03	Loss of power supply	A, D, E
	TI04	Failure of a telecommunications network	A, D, E
	TI05	Failure of telecommunication equipment	A, D
	TI06	Electromagnetic radiation	A, D, E
	TI07	Thermal radiation	A, D, E
	TI08	Electromagnetic pulses	A, D, E
Technical failures	TT01	Failure of device or system	A
	TT02	Saturation of the information system	A, D
	TT03	Violation of information system maintainability	A, D
	TH01	Terror. attack, sabotage	D
	TH02	Social Engineering	D
	TH03	Interception of radiation of a device	D

[a] D = deliberate; A = accidental; E = environmental.

Table A.10 *(continued)*

Category	No.	Threat description	Type of risk source [a]
Human actions	TH04	Remote spying	D
	TH05	Eavesdropping	D
	TH06	Theft of media or documents	D
	TH07	Theft of equipment	D
	TH08	Theft of digital identity or credentials	D
	TH09	Retrieval of recycled or discarded media	D
	TH10	Disclosure of information	A, D
	TH11	Data input from untrustworthy sources	A, D
	TH12	Tampering with hardware	D
	TH13	Tampering with software	A, D
	TH14	Drive-by-exploits using web-based communication	D
	TH15	Replay attack, man-in-the-middle attack	D
	TH16	Unauthorized processing of personal data	A, D
	TH17	Unauthorized entry to facilities	D
	TH18	Unauthorized use of devices	D
	TH19	Incorrect use of devices	A, D
	TH20	Damaging devices or media	A, D
	TH21	Fraudulent copying of software	D
	TH22	Use of counterfeit or copied software	A, D
	TH23	Corruption of data	D
	TH24	Illegal processing of data	D
	TH25	Sending or distributing of malware	A, D, R
	TH26	Position detection	D
Compromise of functions or services	TC01	Error in use	A
	TC02	Abuse of rights or permissions	A, D
	TC03	Forging of rights or permissions	D
	TC04	Denial of actions	D
Organizational threats	TO01	Lack of staff	A, E
	TO02	Lack of resources	A, E
	TO03	Failure of service providers	A, E
	TO04	Violation of laws or regulations	A, D

[a] D = deliberate; A = accidental; E = environmental.

Table A.11 — Examples of typical vulnerabilities

Category	No.	Examples of vulnerabilities
Hardware	VH01	Insufficient maintenance/faulty installation of storage media
	VH02	Insufficient periodic replacement schemes for equipment
	VH03	Susceptibility to humidity, dust, soiling
	VH04	Sensitivity to electromagnetic radiation
	VH05	Insufficient configuration change control
	VH06	Susceptibility to voltage variations
	VH07	Susceptibility to temperature variations
	VH08	Unprotected storage
	VH09	Lack of care at disposal
	VH10	Uncontrolled copying
Software	VS01	No or insufficient software testing
	VS02	Well-known flaws in the software
	VS03	No "logout" when leaving the workstation
	VS04	Disposal or reuse of storage media without proper erasure
	VS05	Insufficient configuration of logs for audit trail's purposes
	VS06	Wrong allocation of access rights
	VS07	Widely-distributed software
	VS08	Applying application programs to the wrong data in terms of time
	VS09	Complicated user interface
	VS10	Insufficient or lack of documentation
	VS11	Incorrect parameter set up
	VS12	Incorrect dates
	VS13	Insufficient identification and authentication mechanisms (e.g. for user authentication)
	VS14	Unprotected password tables
	VS15	Poor password management
	VS16	Unnecessary services enabled
	VS17	Immature or new software
	VS18	Unclear or incomplete specifications for developers
	VS19	Ineffective change control
	VS20	Uncontrolled downloading and use of software
	VS21	Lack of or incomplete back-up copies
	VS22	Failure to produce management reports
Network	VN01	Insufficient mechanisms for the proof of sending or receiving a message
	VN02	Unprotected communication lines
	VN03	Unprotected sensitive traffic
	VN04	Poor joint cabling
	VN05	Single point of failure
	VN06	Ineffective or lack of mechanisms for identification and authentication of sender and receiver
	VN07	Insecure network architecture
	VN08	Transfer of passwords in clear
	VN09	Inadequate network management (resilience of routing)
	VN10	Unprotected public network connections

Table A.11 *(continued)*

Category	No.	Examples of vulnerabilities
Personnel	VP01	Absence of personnel
	VP02	Inadequate recruitment procedures
	VP03	Insufficient security training
	VP04	Incorrect use of software and hardware
	VP05	Poor security awareness
	VP06	Insufficient or lack of monitoring mechanisms
	VP07	Unsupervised work by outside or cleaning staff
	VP08	Ineffective or lack of policies for the correct use of telecommunications media and messaging
Site	VS01	Inadequate or careless use of physical access control to buildings and rooms
	VS02	Location in an area susceptible to flood
	VS03	Unstable power grid
	VS04	Insufficient physical protection of the building, doors and windows
Organization	VO01	Formal procedure for user registration and de-registration not developed, or its implementation is ineffective
	VO02	Formal process for access right review (supervision) not developed, or its implementation is ineffective
	VO03	Insufficient provisions (concerning security) in contracts with customers and/or third parties
	VO04	Procedure of monitoring of information processing facilities not developed, or its implementation is ineffective
	VO05	Audits (supervision) not conducted on a regular basis
	VO06	Procedures of risk identification and assessment not developed, or its implementation is ineffective
	VO07	Insufficient or lack of fault reports recorded in administrator and operator logs
	VO08	Inadequate service maintenance response
	VO09	Insufficient or lack of Service Level Agreement
	VO10	Change control procedure not developed, or its implementation is ineffective
	VO11	Formal procedure for ISMS documentation control not developed, or its implementation is ineffective
	VO12	Formal procedure for ISMS record supervision not developed, or its implementation is ineffective
	VO13	Formal process for authorization of publicly available information not developed, or its implementation is ineffective
	VO14	Improper allocation of information security responsibilities
	VO15	Continuity plans do not exist, or are incomplete, or are outdated
	VO16	E-mail usage policy not developed, or its implementation is ineffective
	VO17	Procedures for introducing software into operational systems not developed, or their implementation is ineffective
	VO18	Procedures for classified information handling not developed, or their implementation is ineffective
	VO19	Information security responsibilities are not present in job descriptions
	VO20	Insufficient or lack of provisions (concerning information security) in contracts with employees
	VO21	Disciplinary process in case of information security incident not defined, or not functioning properly
	VO22	Formal policy on mobile computer usage not developed, or its implementation is ineffective

Table A.11 *(continued)*

Category	No.	Examples of vulnerabilities
	VO23	Insufficient control of off-premise assets
	VO34	Insufficient or lack of "clear desk and clear screen" policy
	VO25	information processing facilities authorization not implemented or not functioning properly
	VO26	Monitoring mechanisms for security breaches not properly implemented
	VO27	Procedures for reporting security weaknesses not developed, or their implementation is ineffective
	VO28	Procedures of provisions compliance with intellectual rights not developed, or their implementation is ineffective

NOTES: All figures must be referenced				