1. Read ISO27001 and ISO27002 and write all Annex A controls on a single page this will help you to remember controls. (Try to create your own mind map) as given on page 2 of this document. (Exercise – A)

Table

Description automatically generated

*Submitted on 16th November 2022*

Guidance document

ISO/IEC 27001 –

Annexure A (select based on Risk assessment)

5. Organizational Controls (A5.1 to A 5.37)

6. People controls (A6.1 to A6.8)

7. Physical controls (A7.1 to A7.14)

8. Technology Controls (A.81.1 to A8.34)

.

Required Clauses (to be include in ISMS Manual)

Cl.4🡪 Context of the Organization

Cl.5 🡪 Leadership

Informative clauses

Cl.1🡪 Scope

Cl.2 🡪 Normative References

Cl.3🡪 Terms and Definition

Controls

Case (Imaginary): “Rural Medical Service Centre” (RMSC) is a hospital which provide Internal Level Medial Service at affordable cost the Rural population by use of State of Art IT and Medical Equipment

*Submitted on 16th November 2022*

|  |
| --- |
| **Exercise** **-1** |

## Terms & Definitions pertaining to Information Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Term** |  |  |  | **Definition / Standard Terms** |
| 1. Base measure | I | ~~A~~ | Person or body that is recognized as being independent of the parties involved, as concerns the issue in question. |
| 2. Audit scope | W | ~~B~~ | Effect of uncertainty on objectives. |
| 3. Conformity | G | ~~C~~ | Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management risk. |
| 4. Confidentiality | P | ~~D~~ | Occurrence or change of particular set of circumstances. |
| 5. Derived measure | MK | ~~F~~ | Property being accessible and usable by an authorized entity. |
| 6. Decision criteria | Z | ~~P~~ | Property that information is not made available or disclosed to unauthorized individuals, entitles or processes. |
| 7. Event | D | ~~G~~ | Fulfillment of requirement. |
| 8. Record | N | K | Measure that is defined as a function of two or more values of base measures. |
| 9. Risk | B | ~~W~~ | Extent and boundaries of an audit. |
| 10. Availability | F | ~~J~~ | Potential cause of an unwanted incident, which may result in harm to a system or organization |
| 11. Risk communication and consultation | C | ~~M~~ | Measure that is defined as a function of two more values of base measures. |
| 12. Vulnerability | O | ~~I~~ | Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature. |
| 13. Third party | A | ~~Z~~ | Measure defined in terms of an attribute and the method for quantifying it. |
| 14. Threat | J | ~~N~~ | Document stating result achieved or providing evidence of activities performed. |
| 15. Derived measure | MK | ~~O~~ | Weakness of an asset or control that can be exploited by one or more threats. |

|  |
| --- |
| **Exercise-2** |

‘

## Auditing Information Security Principles

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Management Principle | # | Management Principle | # | Management Principle |
| **1** | **Awareness of the need for**  **information security** | **2** | **Assignment of responsibility for information security** | **3** | **Incorporating management commitment and the interests of stakeholders** |
| **4** | **Enhancing societal values** | **5** | **Risk assessments determining appropriate controls to reach acceptable levels of risk** | **6** | **Security incorporated as an essential element of information networks and systems** |
| **7** | **Active prevention and detection of information security incidents;** | **8** | **Ensuring a comprehensive approach to information security management;** | **9** | **Continual reassessment of information security and making of modifications as appropriate** |

Submitted on 16th November 2022

|  |  |  |
| --- | --- | --- |
| # | Scenario – Note > **Some scenarios may demonstrate correct implementation of one or more principle(s) OR may be violating one or more principle(s).** | **Principle**  **(Syl. #)** |
| 1 | The Data Privacy policy of the organization focusses on giving respect to privacy of all the Interested Parties and mitigation of all risks for the same | 8 |
| 2 | The process owners of the organization review their residual risks (as a disciplined activity) every six months and updates the approved residual risks | 5 |
| 3 | Five delivery executives of the online shopping portal company, do not collect the identity of the person to whom delivery made, as per delivery policy & process | 3 |
| 4 | The Housing Society declares a special Information Security awareness training to enhance the knowledge of the residents on the subject and give an idea of prioritization of risks – for the benefit of the residential colony member’s benefit | 1 |
| 5 | The school principal investigated the incident of the Artificial Intelligence examination paper of final year vanishing from his locker | 7 |
| 6 | The Car rental company collects the identity of the person hiring car without driver and in one case of Ms Jene, did not collect the driving license | 9 |
| 7 | The General Manager who also happens to be in Governance Board of the automotive company, wanted the R&D manager to give presentation on the new steering technology used for which the R&D Manager in the upcoming Tech. conference – the R&D manager refused to do so as per organization’s risk assessment control of R&D department | 3 |
| 8 | The Passenger lost his boarding pass after security clearance – wanted to go back to check-in counter to get the duplicate boarding pass – security personnel escorted to check-in counter to verify and ensure that this person is the same and boarding pass belongs to the same person | 7 |
| 9 | Incident records in the DR server got corrupted… and the main server also went down. at the same time this was already identified an approved residual risk (low probability) that both might go down at the same time | 9 |
| 10 | The incident details (including causes) were envisaged as new ones – updated into ISMS KEDB and Risk Assessments | 6 |
| 11 | The traditional way of risk assessments in Excel is replaced by locally developed tool with Risk Assessments for C, I & A done separately, as part of Board decision taken | 9 |
| 12 | The College has introduced an online training module for giving training on Information Security Management Systems (ISO 27001:2022) for benefit of college staff and students | 1 |
| 13 | The Zonal Sales Manager recommended termination of the Salesman as he stole the mobile of the Board Member visiting office for a meeting (left mobile on table before going to washroom) – entire incident was captured in CCTV | 7 |
| 14 | The Business Continuity Plan includes testing of Encrypted Data Retrieval to ensure the Data Integrity reliability – risk assessment shows the approved residual risk of the failure of the De-encryption (low possibility) | 5 |
| 15 | The organization does Gap Analysis towards GDPR compliance (as per Board Instructions) for the purpose complying to GDPR, if applicable to business | 4 |

### Exercise -3

Read the Iso27001:2022 standard and try to write down

**External and Internal Issues – list down the external and internal issues consider you company as case study for ISO27001 implementation.**

Submitted on 16th November 2022

|  |  |
| --- | --- |
| **Issues** | **Type (External / Internal)** |
| 1. Patient records not accessible due to network outage | Internal |
| 1. Governing medical body issue notice for non-compliance to applicable medical rules | External |
| 1. VIP movement is preventing paramedical staff from reaching on time for operation to operate High end and sophisticated Heart -lung machine | External |
| 1. Not able to access the Patient payment system due to power outage delay the OPD operations | Internal |
| 1. Cyber-attacks on the hospital Database server | External |
| 1. Biometric access is not implemented for Server room instead security guard is posted only during daytime | Internal |

**Exercise -4**

**List down interested parties**

Submitted on 16th November 2022

|  |  |
| --- | --- |
| **Interest parties** | **Expectation** |
| Board of directors | Provide secure, safe and affordable medical services while maintaining good financial health of the hospital |
| Doctors | IT services and medical equipment are available as need to provide medical services to patients |
| Para Medical staff (Nurses, Lab Doctors, Physio Therapist …) | Training on the effective usage IT and medical equipment. |
| Support staff (Ward boys, Technicians, front desk, Telephone operators …) | Safe working environment, training on the IT systems, clarity on role and responsibilities. |
| Partners (e.g., Pharmacy store) | Clarify on the service levels, correct and timely payment of invoices |
| Suppliers and Vendors (e.g., Oxygen suppliers, Waste management agency.) | Accurate projection of the requirement and delivery timelines, correct and timely payment of invoices |
| In-patients | Close and critical monitoring |
| Out – patients | Fast and quick Doctor consultation with correct diagnosis |

**Exercise -5**

**Write Scope statement**

Submitted on 16th November 2022

Rural Medical Service Centre is hospital which provide international level medical service at affordable cost to the Rural population by use of state of art IT and Medical equipment in a high availability mode, while maintaining compliance to the requirement of ISO27001 in term of Confidentiality, Integration and Protection of Privacy of the patient and staff and in compliance to the applicable Governmental regulation and Medial council framework

**Exercise -6**

**Write your Information security policy**

Submitted on 16th November 2022

**Introduction:**

*“Rural Medical Service Centre” (RMSC)” IT system, IT enabled equipment along with all their operation activities to provide international level medical services at affordable cost. RMSC is cognizant of the requirement of its patients to leverage RMSC IT based services for utilizing RMSC’s medial services by sharing and consuming health and other personal information in digital formats and protection of such information is an essential requirement of the RMSC.*

**Purpose:**

RMSC ISMS constitute the Management’s direction on Information security in form of ISMs policy which are available to public on our website ( <https://www.rmsc.in> ) and support buy the procedure are available to RMSC staff

**SCOPE:**

**RMSC ISMS** covers and applicable to RMSC’s staff across all department, vendors and suppliers. Patients’ co-operation is requested to follow and adhere the instructions of the RMSC staff.

**Policy statement:**

Commitment to protecting the security of Patient and staff information and the protecting the underlying IT system with special emphasis on Medical Equipment is a foundational assurance of RMSC ‘s patients, staff, vendors, suppliers and all other interested parties.

RMSC Management is committed to provide required training, support and direction to its staff members, extend required awareness to contributors such as patients, vendors, suppliers towards their role in protection information and secure usage of the IT and Medical usage. Preventive efforts shall be designed based on a continuous risk assessment and implement controls against failures of integrity or interruptions to the availability of that systems/devices and to ensure appropriate legal, regulatory compliance. Advisory and independent assessment shall be commissioned from reputed external entities shall be sought on periodic basis as an assurance not RMSC’s security posture. Specific measure shall be implemented to achieve and maintain a culture of compliance with rewards and penalty programs.

Exercise -7

**Draw Organization chart as per your company structure (only to cover information security team & concerned team)**

Submitted on 16th November 2022