**The CIA Triad**

A diagram of information security

Description automatically generated with low confidence

|  |  |
| --- | --- |
| Confidentiality |  |
| Integrity |  |
| Availability |  |
| Information Security Triad |  |

**Common Security Standards and Frameworks**

A picture containing text, screenshot, font, rectangle

Description automatically generated

|  |  |
| --- | --- |
| ISO27000 family of standards |  |
| NIST Security standards & guidelines |  |
| Common Criteria |  |
| ENISA standards |  |
| Critical infrastructure standards |  |
| General Data Protection Regulations |  |
| BSI Standards |  |
| Industry-specific standards |  |
| COBIT infrastructure framework |  |
| PCI DSS |  |
| COSO framework |  |
| SOC for cybersecurity |  |

**Components of an ISMS**

A picture containing text, screenshot

Description automatically generated

|  |  |
| --- | --- |
| Systems, tools for ISMS implementation and management |  |
| Policies and controls |  |
| Supply chain management systems and tools |  |
| Implementation resources |  |
| Continual improvement resources |  |
| Communication and engagement resources |  |

**ISMS Scope Scenarios**

A picture containing text, screenshot, font, number

Description automatically generated

|  |  |
| --- | --- |
| Organization |  |
| ISMS scope |  |
| ISMS A |  |
| ISMS B |  |
| ISMS C |  |
| The ISMS scope covers the entire organization |  |
| The ISMS scope covers part of the organization |  |
| There are several ISMSs in the same organization (A, B, C) |  |

**Example Organization Structure Reflecting ISMS Scope**

A picture containing text, screenshot, font, line

Description automatically generated

|  |  |
| --- | --- |
| Board of directors/CEO |  |
| Finance & administration |  |
| Sales & marketing |  |
| Technology |  |
| Engineering |  |
| Internal audit |  |
| Production |  |
| R&D |  |

**PDCA Model and ISMS**

A picture containing text, screenshot, font

Description automatically generatedX

|  |  |
| --- | --- |
| Plan |  |
| Design the ISMS |  |
| Do |  |
| Implement the ISMS |  |
| Act |  |
| Maintain and adjust the ISMS |  |
| Check |  |
| Monitor and check the ISMS |  |

**Risk Management Process**

A diagram of a risk assessment

Description automatically generated with low confidence

|  |  |
| --- | --- |
| Establish context of the organization (internal and external) |  |
| Monitor & review (clause 5.6) |  |
| Treat the risks (clause 5.5) |  |
| Communicate & Consult (clause 5.2) |  |
| Identify risks (clause 5.4.2) |  |
| Analyze risks (clause 5.4.3) |  |
| Evaluate risks (clause 5.4.4) |  |
| Risk assessment (clause 5.4) |  |

**Risk Matrix Example in MS Excel**

A picture containing text, screenshot, number, font

Description automatically generated

|  |  |
| --- | --- |
| Impact |  |
| Likelihood |  |
| Insignificant |  |
| Minor |  |
| Moderate |  |
| Major |  |
| Severe |  |
| Almost |  |
| Certain |  |
| Likely |  |
| Possible |  |
| Unlikely |  |
| Rare |  |
| Medium |  |
| High |  |
| Very High |  |
| Low |  |

**Developing a Communication Plan**

A picture containing text, screenshot, circle, font

Description automatically generated

|  |  |
| --- | --- |
| Step |  |
| Define communication objectives |  |
| Assign roles and tasks |  |
| Identify most important commnications messages |  |
| Carryout target group analysis and determine appropriate media |  |
| Define communication objectives |  |

**Continual Improvement of the ISMS Using PDCA**

A picture containing text, screenshot, font, logo

Description automatically generated

|  |  |
| --- | --- |
| Plan |  |
| Design the current state. Formulate target state |  |
| Do |  |
| Implement the described measures |  |
| Check |  |
| Check if the planned target had been achieved |  |
| Act |  |
| Adapt goals based on the check |  |

**Continual Improvement Plan Tracker Template**

A picture containing text, screenshot, line, number

Description automatically generated

|  |  |
| --- | --- |
| Sr. No |  |
| Date Submitted |  |
| Description |  |
| Priority |  |
| Responsible Person |  |
| Due Date |  |
| Date of Completion |  |
| Progress Description |  |
| Status |  |

**ISO/IEC 27001 Control Domains**

A picture containing text, font, logo, screenshot

Description automatically generated

|  |  |
| --- | --- |
| Organizational controls |  |
| People controls |  |
| Physical controls |  |
| Technological controls |  |