# Annex C: Surveillance Plan

|  |
| --- |
| **Surveillance PlanISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO/IEC 27017:2015, and ISO/IEC 27018:2019** |
| **1**: Initial Audit**2:** Surveillance 1 Audit**3**: Surveillance 2 Audit**4**: Recertification Audit | **Plan** |
| **1****(202X)** | **2** **(202X)** | **3****(202X)** | **4****(202X)** |
| **Clauses and Controls** |
| **4 Context of the organization** |
| **4.1/5.2.1** | Understanding the organization and its context\*\* |  |  |  |  |
| **4.2/5.2.2** | Understanding the needs and expectations of interested parties\*\* |  |  |  |  |
| **4.3/5.2.3** | Determining the scope of the information security management system\*\* |  |  |  |  |
| **4.4/5.2.4** | Information security management system\*\* |  |  |  |  |
| **5 Leadership** |
| **5.1/5.3.1** | Leadership and commitment\*\* |  |  |  |  |
| **5.2/5.3.2** | Policy\*\* |  |  |  |  |
| **5.3/5.3.3** | Organizational roles, responsibilities and authorities\*\* |  |  |  |  |
| **6 Planning** |
| **6.1/5.4.1** | Actions to address risks and opportunities\*\* |  |  |  |  |
| **6.1.1/5.4.1.1** | General\*\* |  |  |  |  |
| **6.1.2/5.4.1.2** | Information security risk assessments\*\* |  |  |  |  |
| **6.1.3/5.4.1.3** | Information security risk treatment\*\* |  |  |  |  |
| **6.2/5.4.2** | Information security objectives and planning to achieve them\*\* |  |  |  |  |
| **6.3** | Planning of changes |  |  |  |  |
| **7 Support** |
| **7.1/5.5.1** | Resources\*\* |  |  |  |  |
| **7.2/5.5.2** | Competence\*\* |  |  |  |  |
| **7.3/5.5.3** | Awareness\*\* |  |  |  |  |
| **7.4/5.5.4** | Communication\*\* |  |  |  |  |
| **7.5/5.5.5** | Documented information\*\* |  |  |  |  |
| **7.5.1/5.5.5.1** | General\*\* |  |  |  |  |
| **7.5.2/5.5.5.2** | Creating and updating\*\* |  |  |  |  |
| **7.5.3/5.5.5.3** | Control of documented information\*\* |  |  |  |  |
| **8 Operation** |
| **8.1/5.6.1** | Operational planning and control\*\* |  |  |  |  |
| **8.2/5.6.2** | Information security risk assessment\*\* |  |  |  |  |
| **8.3/5.6.3** | Information security risk treatment\*\* |  |  |  |  |
| **9 Performance Evaluation** |
| **9.1/5.7.1** | Monitoring, measurement, analysis and evaluation\*\* |  |  |  |  |
| **9.2/5.7.2** | Internal audit\*\* |  |  |  |  |
| **9.2.1** | General |  |  |  |  |
| **9.2.2** | Internal audit program |  |  |  |  |
| **9.3/5.7.3** | Management review\*\* |  |  |  |  |
| **9.3.1** | General |  |  |  |  |
| **9.3.2** | Management review inputs |  |  |  |  |
| **9.3.3** | Management review results |  |  |  |  |
| **10 Improvement** |
| **10.1/5.8.2** | Continual improvement\*\* |  |  |  |  |
| **10.2/5.8.1** | Nonconformity and corrective action \*\* |  |  |  |  |
| **Control objectives and controls** |
| **A.5** | Organizational controls |  |  |  |  |
| **A.6** | People controls |  |  |  |  |
| **A.7** | Physical Controls  |  |  |  |  |
| **A.8** | Technological controls |  |  |  |  |
| **11. Additional requirements** |
|  | Use of Logo |  |  |  |  |
|  | List of documents included in the audited MS |  |  |  |  |
| **ISO/IEC 27701:2019** |
| **6 PIMS-specific guidance related to ISO/IEC 27001** |
| **6.1** | General |  |  |  |  |
| **6.2** | Information security policies |  |  |  |  |
| **6.3** | Organization of information security |  |  |  |  |
| **6.4** | Human resource security |  |  |  |  |
| **6.5** | Asset management |  |  |  |  |
| **6.6** | Asset control |  |  |  |  |
| **6.7** | Cryptography |  |  |  |  |
| **6.8** | Physical and environmental security |  |  |  |  |
| **6.9** | Operations security |  |  |  |  |
| **6.10** | Communications security |  |  |  |  |
| **6.11** | Systems acquisition, development and maintenance |  |  |  |  |
| **6.12** | Supplier relationships |  |  |  |  |
| **6.13** | Information security incident management |  |  |  |  |
| **6.14** | Information security aspects of business continuity management |  |  |  |  |
| **6.15** | Compliance |  |  |  |  |
| **7 Additional ISO/IEC 27002 guidance for PII controllers** |
| **7.1** | General |  |  |  |  |
| **7.2** | Conditions for collection and processing |  |  |  |  |
| **7.3** | Obligations to PII principals |  |  |  |  |
| **7.4** | Privacy by design and privacy by default |  |  |  |  |
| **7.5** | PII sharing, transfer, and disclosure |  |  |  |  |
| **8 Additional ISO/IEC 27002 guidance for PII processors** |
| **8.1** | General |  |  |  |  |
| **8.2** | Conditions for collection and processing |  |  |  |  |
| **8.3** | Obligations to PII principals |  |  |  |  |
| **8.4** | Privacy by design and privacy by default |  |  |  |  |
| **8.5** | PII sharing, transfer, and disclosure |  |  |  |  |
| **Notes and comments:** |  |

*For completed visits, mark “X” in the box for each clause/process covered.*

*For planned visits, mark “O” in the box for esach clause/process to be covered.*