# Annex C: Surveillance Plan

|  |
| --- |
| **Surveillance PlanISO 9001:2015, ISO/IEC 27001:2022 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)** |
| **ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 27018:2019 Clauses** |
| **4 Context of the organization** |
| **4.1** | Understanding the organization and its context |  |  |  |  |
| **4.2** | Understanding the needs and expectations of interested parties |  |  |  |  |
| **4.3** | Determining the scope of the information security management system |  |  |  |  |
| **4.4** | Information security management system |  |  |  |  |
| **5 Leadership** |
| **5.1** | Leadership and commitment |  |  |  |  |
| **5.2** | Policy |  |  |  |  |
| **5.3** | Organizational roles, responsibilities and authorities |  |  |  |  |
| **6 Planning** |
| **6.1** | Actions to address risks and opportunities |  |  |  |  |
| **6.2** | Information security objectives and planning to achieve them |  |  |  |  |
| **6.3** | Planning of changes |  |  |  |  |
| **7 Support** |
| **7.1** | Resources |  |  |  |  |
| **7.2** | Competence |  |  |  |  |
| **7.3** | Awareness |  |  |  |  |
| **7.4** | Communication |  |  |  |  |
| **7.5** | Documented information |  |  |  |  |
| **8 Operation** |
| **8.1** | Operational planning and control |  |  |  |  |
| **8.2** | Information security risk assessment |  |  |  |  |
| **8.3** | Information security risk treatment |  |  |  |  |
| **8.4** | Control of externally provided processes, products and services |  |  |  |  |
| **8.5** | Production and service provision |  |  |  |  |
| **8.6** | Release of products and services |  |  |  |  |
| **8.7** | Control of nonconforming outputs |  |  |  |  |
| **9 Performance evaluation** |
| **9.1** | Monitoring, measurement, analysis and evaluation |  |  |  |  |
| **9.2** | Internal audit |  |  |  |  |
| **9.3** | Management review |  |  |  |  |
| **10 Improvement** |
| **10.1** | Continual improvement/General |  |  |  |  |
| **10.2** | Nonconformity and corrective action  |  |  |  |  |
| **10.3** | Continual improvement |  |  |  |  |
| **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 |  |  |  |  |
| **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 each clause/process to be covered.*