# Annex C: Surveillance Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Surveillance Plan ISO/IEC 27001:2013 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/IEC 27001:2013 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 | |  |  |  |  |
| **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 | |  |  |  |  |
| **9 Performance Evaluation** | | | | | | |
| **9.1** | Monitoring, measurement, analysis and evaluation | |  |  |  |  |
| **9.2** | Internal audit | |  |  |  |  |
| **9.3** | Management review | |  |  |  |  |
| **10 Improvement** | | | | | | |
| **10.1** | Nonconformity and corrective action | |  |  |  |  |
| **10.2** | Continual improvement | |  |  |  |  |
| **Control objectives and controls** | | | | | | |
| **A.5** | Information security policies | |  |  |  |  |
| **A.6** | Organization of information security | |  |  |  |  |
| **A.7** | Human resource security | |  |  |  |  |
| **A.8** | Asset management | |  |  |  |  |
| **A.9** | Access control | |  |  |  |  |
| **A.10** | Cryptography | |  |  |  |  |
| **A.11** | Physical and environmental security | |  |  |  |  |
| **A.12** | Operations security | |  |  |  |  |
| **A.13** | Communications security | |  |  |  |  |
| **A.14** | System acquisition, development and maintenance | |  |  |  |  |
| **A.15** | Supplier relationships | |  |  |  |  |
| **A.16** | Information security incident management | |  |  |  |  |
| **A.17** | Information security aspects of business continuity management | |  |  |  |  |
| **A.18** | Compliance | |  |  |  |  |
| **11. Additional requirements** | | | | | | |
|  | Use of Logo | |  |  |  |  |
|  | List of documents included in the audited MS | |  |  |  |  |
| **Notes and comments:** | |  | | | | |

# Annex D: Surveillance Plan

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Surveillance Plan CSA STAR Certification** | | | | | |
| **1**: Initial Audit  **2:** Surveillance 1 Audit  **3**: Surveillance 2 Audit  **4**: Recertification Audit | | **Plan** | | | |
| **1**  **(202X)** | **2**  **(202X)** | **3**  **(202X)** | **4**  **(202X)** |
| **CSA STAR Requirements Certification** | | | | | |
|  | | | | | |
| **A&A** | Audit and Assurance |  |  |  |  |
| **AIS** | Application & Interface Security |  |  |  |  |
| **BCR** | Business Continuity Management &  Operational Resilience |  |  |  |  |
| **CCC** | Change Control & Configuration Management |  |  |  |  |
| **CEK** | Cryptography, Encryption & Key Management |  |  |  |  |
| **DCS** | Datacenter Security |  |  |  |  |
| **DSP** | Data Security & Privacy Lifecycle Management |  |  |  |  |
| **GRC** | Governance, Risk Management and Compliance |  |  |  |  |
| **HRS** | Human Resources |  |  |  |  |
| **IAM** | Identity & Access Management |  |  |  |  |
| **IPY** | Interoperability & Portability |  |  |  |  |
| **IVS** | Infrastructure & Virtualization Security |  |  |  |  |
| **LOG** | Logging and Monitoring |  |  |  |  |
| **SEF** | Security Incident Management, E-Discovery, & Cloud Forensics |  |  |  |  |
| **STA** | Supply Chain Management, Transparency, and Accountability |  |  |  |  |
| **TVM** | Threat & Vulnerability Management |  |  |  |  |
| **UEM** | Universal Endpoint Management |  |  |  |  |

*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.*