# Annex C: Surveillance Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Surveillance Plan ISO/IEC 27034:2011** | | | | | | |
| **1**: Initial Audit  **2:** Surveillance 1 Audit  **3**: Surveillance 2 Audit  **4**: Recertification Audit | | | **Plan** | | | |
| **1**  **(201X)** | **2**  **(201X)** | **3**  **(201X)** | **4**  **(201X)** |
| **ISO/IEC 27034:2011 requirements** | | | | | | |
| **6 Introduction to application security** | | | | | | |
| **6.3** | Application security scope | |  |  |  |  |
| **6.3.1** | General | |  |  |  |  |
| **6.3.2** | Business context | |  |  |  |  |
| **6.3.3** | Regulatory context | |  |  |  |  |
| **6.3.4** | Application life cycle processes | |  |  |  |  |
| **6.3.5** | Processes involved with the application | |  |  |  |  |
| **6.3.6** | Technological context | |  |  |  |  |
| **6.3.7** | Application specifications | |  |  |  |  |
| **6.3.8** | Application data | |  |  |  |  |
| **6.3.9** | Organization and user data | |  |  |  |  |
| **6.3.10** | Roles and permissions | |  |  |  |  |
| **6.4** | Application security requirements | |  |  |  |  |
| **6.4.1** | Application security requirements sources | |  |  |  |  |
| **6.4.2** | Application security requirements engineering | |  |  |  |  |
| **6.4.3** | ISMS | |  |  |  |  |
| **6.5** | Risk | |  |  |  |  |
| **6.5.1** | Application security risk | |  |  |  |  |
| **6.5.2** | Application vulnerabilities | |  |  |  |  |
| **6.5.3** | Threats to applications | |  |  |  |  |
| **6.5.4** | Impact on applications | |  |  |  |  |
| **6.5.5** | Risk management | |  |  |  |  |
| **6.6** | Security costs | |  |  |  |  |
| **6.7** | Target environment | |  |  |  |  |
| **6.8** | Controls and their objectives | |  |  |  |  |
| **7 ISO/IEC 27034 overall processes** | | | | | | |
| **7.1** | Components, processes and frameworks | |  |  |  |  |
| **7.2** | ONF management process | |  |  |  |  |
| **7.3** | Application security management process | |  |  |  |  |
| **7.3.1** | General | |  |  |  |  |
| **7.3.2** | Specifying the application requirements and environment | |  |  |  |  |
| **7.3.3** | Assessing application security risks | |  |  |  |  |
| **7.3.4** | Creating and maintaining the Application Normative Framework | |  |  |  |  |
| **7.3.5** | Provisioning and operating the application | |  |  |  |  |
| **7.3.6** | Auditing the security of the application | |  |  |  |  |
| **8 Concepts** | | | | | | |
| **8.1** | Organization normative framework | |  |  |  |  |
| **8.1.1** | General | |  |  |  |  |
| **8.1.2** | Components | |  |  |  |  |
| **8.1.3** | Processes related to the Organization Normative Framework | |  |  |  |  |
| **8.2** | Application security risk assessment | |  |  |  |  |
| **8.2.1** | Risk assessment vs risk management | |  |  |  |  |
| **8.2.2** | Application risk analysis | |  |  |  |  |
| **8.2.3** | Risk evaluation | |  |  |  |  |
| **8.2.4** | Application’s Targeted Level of Trust | |  |  |  |  |
| **8.2.5** | Application owner acceptation | |  |  |  |  |
| **8.3** | Application normative framework | |  |  |  |  |
| **8.3.1** | General | |  |  |  |  |
| **8.3.2** | Components | |  |  |  |  |
| **8.3.3** | Processes related to the security of the application | |  |  |  |  |
| **8.3.4** | Application’s life cycle | |  |  |  |  |
| **8.3.5** | Processes | |  |  |  |  |
| **8.4** | Provisioning and operating the application | |  |  |  |  |
| **8.4.1** | General | |  |  |  |  |
| **8.4.2** | Impact of ISO/IEC 27034 on an application project | |  |  |  |  |
| **8.4.3** | Components | |  |  |  |  |
| **8..4** | Processes | |  |  |  |  |
| **8.5** | Application security audit | |  |  |  |  |
| **8.5.1** | General | |  |  |  |  |
| **8.5.2** | Components | |  |  |  |  |
| **Use of Logo** | | |  |  |  |  |
| **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.*