**Appendix 3 – Internal Audit Checklist for ISO 27001**

\*\* FREE PREVIEW VERSION \*\*

|  |  |  |  |
| --- | --- | --- | --- |
| Clause | Requirement of the standard | Compliant Yes/No | Evidence |
| 4.2 | Did the organization determine interested parties? |  |  |
| 4.2 | … |  |  |
| 4.3 | … |  |  |
| 5.1 | Are the general ISMS objectives compatible with the strategic direction? |  |  |
| 5.1 | … |  |  |
| 5.2 | … |  |  |
| 5.2 | Is Information Security Policy communicated within the company? |  |  |
| 5.3 | … |  |  |
| 6.1.2 | … |  |  |
| 6.1.2, 8.2 | … |  |  |
| 6.1.3 | Is the risk treatment process documented, including the risk treatment options? |  |  |
| 6.1.3, 8.3 | … |  |  |
| 6.1.3 | … |  |  |
| 6.1.3, 8.3 | Does Risk treatment plan exist, approved by risk owners? |  |  |
| 6.2 | … |  |  |
| 7.1 | Are adequate resources provided for all the elements of ISMS? |  |  |
| 7.2 | … |  |  |
| 7.3 | … |  |  |
| 7.4 | Does the process for communication related to information security exist, including the responsibilities and what to communicate? |  |  |
| 7.5 | … |  |  |
| 7.5 | Are documents of external origin controlled? |  |  |
| 8.1 | Are outsourced processes identified and controlled? |  |  |
| 9.1 | … |  |  |
| 9.1 | Are the results of measurement documented and reported to responsible persons? |  |  |
| 9.2 | … |  |  |
| 9.2 | … |  |  |
| 9.3 | … |  |  |
| 9.3 | … |  |  |
| 10.1 | Does the organization react to every nonconformity? |  |  |

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here:

<https://advisera.com/eugdpracademy/documentation/iso-27001-internal-audit-checklist/>