STATEMENT OF APPLICABILITY

Commented [27A1]: To learn how to fill out this document, and to see real-life examples of what you need to write, watch this video tutorial: "How to Write ISO 27001 Statement of Applicability".

To access the tutorial, choose one of the following options (depending on how you received the document):

a) For document(s) delivered via Conformio: log into Conformio, click "Helpful materials" in the top menu, choose your language, and open the folder "Video tutorials."

b) For document(s) delivered via email: in your inbox, find the email that you received at the moment of purchase - there, you will see a link that will enable you to access the video tutorial.

Commented [27A2]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [27A3]: To learn how to write the Statement of Applicability, read this article:

The Importance of Statement of Applicability for ISO 27001
https://advisera.com/27001academy/knowledgebase/the-importance-of-statement-of-applicability-for-iso-27001/

Commented [27A4]: The document coding system should be in line with the organization’s existing system for document coding. In case such a system is not in place, this line may be deleted.
### Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Created by</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td></td>
<td>27001Academy</td>
<td>Basic document outline</td>
</tr>
</tbody>
</table>

### Table of contents

1. PURPOSE, SCOPE AND USERS .................................................................................................................. 3
2. REFERENCE DOCUMENTS .......................................................................................................................... 3
3. APPLICABILITY OF CONTROLS ................................................................................................................. 3
4. ACCEPTANCE OF RESIDUAL RISKS ............................................................................................................... 21
5. VALIDITY AND DOCUMENT MANAGEMENT ............................................................................................. 21
1. Purpose, scope and users

The purpose of this document is to define which controls are appropriate to be implemented in [organization name], the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all controls listed in Annex A of the ISO 27001 standard. Controls are applicable to the entire Information Security Management System (ISMS) scope.

Users of this document are all employees of [organization name] who have a role in the ISMS.

2. Reference documents

- ISO/IEC 27001 standard, clause 6.1.3 d)
- Information Security Policy
- Risk Assessment and Risk Treatment Methodology
- Risk Assessment and Risk Treatment Report

3. Applicability of controls

The following controls from ISO 27001 Annex A are applicable:

<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/ non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.5</td>
<td>Information security policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.5.1.2</td>
<td>Review of the policies for information security</td>
<td></td>
<td></td>
<td>Each policy has a designated owner who has to review the document at planned interval</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Controls according to ISO/IEC 27001</td>
<td>Applicability (YES/NO)</td>
<td>Justification for selection/non-selection</td>
<td>Control objectives</td>
<td>Implementation method</td>
<td>Status</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------</td>
<td>------------------------</td>
<td>------------------------------------------</td>
<td>--------------------</td>
<td>-----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>A.6.1.1</td>
<td></td>
<td></td>
<td>Responsibilities for information security are listed in various ISMS documents. If required, [job title] defines additional responsibilities</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Commented [27A10]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

Commented [27A7]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

Commented [27A8]: To learn more about control objectives, read this article: ISO 27001 control objectives – Why are they important? [link]

Commented [27A9]: Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma ",", this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

Commented [27A6]: Based on risk assessment results, contractual and legal obligations.

Commented [27A11]: If business continuity is not included in the ISO 27001 project, replace this text by specifying who is responsible for the contact with the police, fire department, etc.

Commented [27A12]: Different interest groups may be assigned to different job functions, depending on specialization of work.

A.6.1.5 Information security in project management

A.6.2 Mobile devices and teleworking

Project manager is required to include applicable information security rules in every project.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability [YES/NO]</th>
<th>Justification for selection/non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.6.2.1</td>
<td>Mobile device policy</td>
<td>[IT Security Policy] / [Mobile Device and Teleworking Policy], [Bring Your Own Device (BYOD) Policy]</td>
<td>[Executive Summary, P. 1 of 65]</td>
<td>[Executive Summary, P. 1 of 65]</td>
<td>[Executive Summary, P. 1 of 65]</td>
<td>[Executive Summary, P. 1 of 65]</td>
</tr>
</tbody>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. “Planned,” “Partially implemented,” “Fully implemented.”

Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article: ISO 27001 control objectives – Why are they important? [https://advisera.com/iso27001academy/blog/2014/04/10/iso-27001-control-objectives-why-they-important/](https://advisera.com/iso27001academy/blog/2014/04/10/iso-27001-control-objectives-why-they-important/)

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign “/”, this means you should choose either the first or the second document. If two documents are mentioned with comma “,” this means you should implement both documents for a particular control.

The document called “List of documents” lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection (non-selection)</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.7.2.1</td>
<td>Management responsibilities</td>
<td></td>
<td></td>
<td>Management actively requires that all ISMS rules be implemented by all employees, suppliers and outsourcing partners</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.7</td>
<td>Termination and change of employment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.7.3.1</td>
<td>Termination or change of employment responsibilities</td>
<td></td>
<td></td>
<td>All agreements with suppliers and partners contain clauses that remain valid after the termination of employment, as well as the [Confidentiality Statements] signed with employees.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Commented [27A10]:** Indicate the status of implementation – e.g. “Planned,” “Partially implemented,” “Fully implemented.” Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

**Commented [27A8]:** To learn more about control objectives, read this article. ISO 27001 control objectives – Why are they important? [https://advisera.com/27001academy/blog/2014/04/10/so-27001-control-objectives-why-are-they-important/](https://advisera.com/27001academy/blog/2014/04/10/so-27001-control-objectives-why-are-they-important/)

**Commented [27A9]:** Implementation method – specify document, technical control, or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign “/,” this means you should choose either the first or the second document. If two documents are mentioned with comma “,” this means you should implement both documents for a particular control.

The document called “List of documents” lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.8.1.2</td>
<td>Ownership of assets</td>
<td></td>
<td>[Inventory of Assets], [IT Security Policy]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.8.1.3</td>
<td>Acceptable use of assets</td>
<td></td>
<td>[IT Security Policy]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.8.2.2</td>
<td>Labeling of information</td>
<td></td>
<td>[Information Classification Policy]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.8.3.2</td>
<td>Disposal of media</td>
<td></td>
<td>[Security Procedures for IT Department] / [Disposal and Destruction Policy]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.8.3.3</td>
<td>Physical media transfer</td>
<td></td>
<td>[Information Classification Policy]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.9.2</td>
<td>User access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Commented [27A10]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

Commented [27A7]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Commented [27A8]: To learn more about control objectives, read this article.

Commented [27A9]: Implementation method - specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

Commented [27A6]: Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/ non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.9.2.5</td>
<td>Review of user access rights</td>
<td></td>
<td></td>
<td>[Access Control Policy]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.9.2.6</td>
<td>Removal or adjustment of access rights</td>
<td></td>
<td></td>
<td>[Access Control Policy]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.9.3</td>
<td>User responsibilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.9.4.3</td>
<td>Password management system</td>
<td></td>
<td></td>
<td>[Access Control Policy] / [Password Policy]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.9.4.4</td>
<td>Use of privileged utility programs</td>
<td></td>
<td></td>
<td>Only [job title] has the right to use privileged utility programs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

**Commented [27K8]:** To learn more about control objectives, read this article: ISO 27001 control objectives - Why are they important? https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/

**Commented [27A9]:** Implementation method - specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma ",", this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.11</td>
<td>Physical and environmental security</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.11.1</td>
<td>Secure areas</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.11.1.1</td>
<td>Physical security perimeter</td>
<td></td>
<td></td>
<td>Areas with sensitive information are protected [describe how – walls, etc.]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Commented [27A10]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

Commented [27A7]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

Commented [27A8]: To learn more about control objectives, read this article. ISO 27001 control objectives – Why are they important? [https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/](https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/)

Commented [27A9]: Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma ",", this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

Commented [27A6]: Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.11.1.6</td>
<td>Delivery and loading areas</td>
<td>[describe how], and delivery and loading areas (specify which) are controlled [describe how]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.11.2</td>
<td>Equipment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article:
ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.
This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.
If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with commas ",", this means you should implement both documents for a particular control.
The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/ non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article:
ISO 27001 control objectives – Why are they important? 
https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma ",," this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection / non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article:
ISO 27001 control objectives – Why are they important? [https://advisera.com/27001academy/blog/2014/04/10/so-27001-control-objectives-why-are-they-important/](https://advisera.com/27001academy/blog/2014/04/10/so-27001-control-objectives-why-are-they-important/)

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma ",", this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.

**Commented [27A13]:** If necessary, a technical description of how these environments are separated may be added; criteria used for transfer from development to test environment and from test to operational environment may also be described.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. “Planned,” “Partially implemented,” “Fully implemented.” Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article: ISO 27001 control objectives – Why are they important? [https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/](https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/)

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign “/”, this means you should choose either the first or the second document. If two documents are mentioned with comma “,” this means you should implement both documents for a particular control.

The document called “List of documents” lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.

**Commented [27A14]:** If necessary, add cryptographic protection, access restriction in accordance with the Access Control Policy, etc.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/ non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

**Commented [27A8]:** To learn more about control objectives, read this article: ISO 27001 control objectives – Why are they important? [https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/](https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/)

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma "," this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."
Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.
Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article:
ISO 27001 control objectives – Why are they important?
https://avisera.com/27001academy/blog/2014/04/01/iso-27001-control-objectives-why-are-they-important/

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.
This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.
If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma ",," this means you should implement both documents for a particular control.
The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/ non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article:
ISO 27001 control objectives – Why are they important? [Link]

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma "," this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.

©2019 This template may be used by clients of Advisera Expert Solutions Ltd. www.advisera.com in accordance with the License Agreement.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability [YES/NO]</th>
<th>Justification for selection/non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article: ISO 27001 control objectives - Why are they important? [https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/](https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/)

**Commented [27A9]:** Implementation method - specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma ",", this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability [YES/NO]</th>
<th>Justification for selection/ non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

**Commented [27A8]:** To learn more about control objectives, read this article: ISO 27001 control objectives - Why are they important? [https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/] (external link)

**Commented [27A9]:** Implementation method - specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control, if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma ",," this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.

**Commented [27A15]:** Write this only if business continuity management is included in ISO 27001.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
</table>

---

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

**Commented [27K8]:** To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important?
https://advisera.com/27001academy/blog/2014/04/10/iso-27001-control-objectives-why-are-they-important/

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma "," this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
<table>
<thead>
<tr>
<th>ID</th>
<th>Controls according to ISO/IEC 27001</th>
<th>Applicability (YES/NO)</th>
<th>Justification for selection/ non-selection</th>
<th>Control objectives</th>
<th>Implementation method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Commented [27A10]:** Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented." Leave blank if the control is marked as inapplicable.

**Commented [27A7]:** They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A. Leave blank if the control is marked as inapplicable.

**Commented [27A8]:** To learn more about control objectives, read this article:
ISO 27001 control objectives – Why are they important? [Link]
https://advisera.com/27001/academy/blog/2016/04/10/iso-27001-control-objectives-why-are-they-important/

**Commented [27A9]:** Implementation method – specify document, technical control or describe the process. Leave blank if the control is marked as inapplicable.

This table lists documents from this Toolkit relevant for each control; if there are no documents relevant for the control, a suggested description of the process is given.

If two documents are mentioned with the slash sign "/", this means you should choose either the first or the second document. If two documents are mentioned with comma "," this means you should implement both documents for a particular control.

The document called "List of documents" lists all the documents from the Toolkit together with a note whether such document is mandatory according to the standard or not.

**Commented [27A6]:** Based on risk assessment results, contractual and legal obligations.
4. Acceptance of Residual Risks

Since not all risks could be reduced in the risk management process, all residual risks are hereby accepted:

1. 
2. 

[Complete the table with data on all individual risks which are not acceptable – use the Risk Treatment Table as the source.]

<table>
<thead>
<tr>
<th>No.</th>
<th>Name of asset</th>
<th>Asset owner</th>
<th>Threat</th>
<th>Vulnerability</th>
<th>New impact</th>
<th>New probability</th>
<th>Residual risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year, and immediately after risk assessment review and updates to the Risk Assessment Table and Risk Treatment Table.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- [Job title]
- [Name]
- [Signature]