# A picture containing text, clipart Description automatically generatedRisk Assessment & Treatment Methodology

Table of Contents

[1. Purpose 1](#_Toc94210249)

[2. Risk identification 2](#_Toc94210250)

[3. Adding and updating risks 2](#_Toc94210251)

[4. Assessing risks 3](#_Toc94210252)

[5. Treating risks 5](#_Toc94210253)

[6. Risk acceptance criteria 6](#_Toc94210254)

[7. Closed Risks 7](#_Toc94210255)

[8. Opportunities 7](#_Toc94210256)

[9. Applicable legislation & regulation risk assessment 8](#_Toc94210257)

[10. Alignment with other important risk-based processes 9](#_Toc94210258)

## Purpose

The purpose of this document is to set out our approach to risk assessment and treatment in regard to compliance with ISO 27001: 2013 and other standards as required. It also draws on practices within risk management focused ISO 31000.

The policy reflects how we run our normal day-to-day business from a risk perspective, using the Risks & Treatments tool.

Clause 6.1 of ISO 27001: 2013 is very clear that the approach towards addressing risks and opportunities is about information security. As such, our approach incorporates a more holistic perspective, which is described in detail further in this methodology and summarised in the image below.

Monitoring

and

review

Risk assessment internally and externally

Risk analysis

Risk identification

Risk evaluation

Risk treatment

Communication and consultation

Establish context

## Risk identification

Identification and initial triage

4.1 External and internal issues

4.2 Interested parties

4.3 Scope

Annex A controls

In terms of risk identification and initial inputs into the risk analysis we do the following:

1. Consider the organisation and its context including 4.1 External and internal issues
2. Understand the needs and expectations of 4.2 Interested Parties taking their importance into account
3. Consider any A.18.1.1 Applicable legislation, regulations or contractual requirement
4. Consider 4.3 Scope of the system
5. Consider ISO 27001 Annex A policy and controls areas to help stimulate further identification of risk in the above areas
6. Also consider any additional compliance regimes adopted within the organisation

***Tips***

*The risk identification work may be achieved through brainstorming / workshop facilitation, desktop research and business plan review, asset inventory, existing process documentation review etc. Initial ideas may also be stimulated by the Risk Bank.*

## Adding and updating risks

Having identified a risk using the process above, the risk is added to the Risks & Treatment tool within ISMS.online.

The following principles apply:

* Risks are relevantly described along with their potential consequence
* Risks are categorised as being internal, external or both
* Each risk has one overall owner. Individual treatment actions can be created as To-Dos and tracked and managed within that risk
* All work around risks is audited. The risk owner must demonstrate enough evidence to auditors and internal stakeholders that appropriate action has been taken
* Risks can be identified, added and updated within the tool at any time by any member of the ISMS board
* Risks are reviewed at varying intervals based on their position on the map or any other change (eg: to regulations, external or internal issues etc) as appropriate
* All changes are visible to all ISMS board members via the Risks & Treatments tool
* New risks are assessed as they become known e.g. through project work in accordance with A.6.1.5 Information security in project management, management reviews, or other interactions with Interested Parties or general research

## Assessing risks

A defined process of likelihood and impact analysis is considered for risk assessment. It takes into account the potential loss of confidentiality, integrity and availability of information for the impact assessment.

**Likelihood**

|  |  |
| --- | --- |
| **Level** | **Description** |
| Very low | No history of occurrence and the event may only happen in exceptional circumstances with a high level of investment and or specialist skills |
| Low | The event has not occurred before but could do so without exceptional circumstances being needed or high level of investment and or specialist skills |
| Medium | The event has occurred in the past and could recur again without exceptional circumstances being needed or high level of investment and or specialist skills |
| High | The event will occur at some point and may be a repeat of past events |
| Very High | There is a history of regular reoccurrence |

**Confidentiality and Integrity Impact**

|  |  |
| --- | --- |
| **Level** | **Description** |
| None | The risk does not affect this area |
| Insignificant | (i.e. Very Low) - negligible or no damage to business operation and reputation with no costs or consequences |
| Minor | Low damage to business operation or reputation with negligible costs or consequences |
| Moderate | Some damage or loss to business operation or reputation with some cost exposure but not affecting future prospects |
| Major | Serious but not complete damage to business operation or reputation with large cost exposure and affecting future prospects |
| Severe | Severe damage to business operation or reputation with very large cost exposure and leaving no future prospects |

**Availability Impact**

|  |  |
| --- | --- |
| **Score** | **Description** |
| None | The risk does not affect this area |
| Insignificant | Can be absorbed and shows no measurable impact - no service disruption |
| Minor | Work distraction; minor increases in support or costs - low disruption to service |
| Moderate | Work delays; noticeable impact to costs and productivity - short disruption to service |
| Major | Work interruption; business commitments delayed with serious costs |
| Severe | Work stoppage and extended service closure; substantial support costs |

***Confidentiality***

Information is not made available or disclosed to unauthorised individuals, entities, or processes, i.e. it means ensuring that information held is only accessible to those who are authorised to see it (within a defined group of users).

A breach of confidentiality is where the information concerned is disclosed, maliciously or accidentally, and can be assumed to come into the hands of unauthorised persons. This also encompasses accidental misrouting to an unintended party.

***Integrity***

Safeguarding the accuracy and completeness of information. Ensuring it is a sound representation of authorised business processes or persons. Integrity addresses the following aspects: completeness, accuracy, validity, maintenance of stored information including timeliness of updates.

A breach of integrity is where the information concerned is deliberately or accidentally altered; it has arrived out of sequence or its integrity has otherwise been compromised during the course of transaction; or it has been duplicated or deleted.

***Availability***

Being accessible and usable upon demand by an authorised entity, i.e. meaning ensuring that information and/or service is available when required for business operations.

A breach of availability is the inability to transact in expected or contracted time-scales due to flaws in the process or due to the effects of a disaster or failure.

## Treating risks

The Risks & Treatments tool within the ISMS.online uses a 5 x 5 grid. Once assessed each risk is placed on the map in a position based on its likelihood and impact. Each position has a unique number for easy identification.

The higher the number, the greater the overall risk; with impact being considered more important than likelihood. Frequency of monitoring is determined by the overall risk level indicated by the coloured squares on the map with reviews taking place:

* For positions 1 to 5 in the green, at least annually
* For positions 6 to 14 in the yellow, at least every six months
* For positions 15 to 20 in the red, at least quarterly
* For positions 21 to 25 in the black, at least monthly

These timelines are suggested automatically by the Risks & Treatments tool and can be overridden if more frequent review is required. The risk owner will be prompted in advance of the review date to review the risk.

The risk owner is responsible for identifying the appropriate treatment and considering the criteria for accepting (tolerating) the risk as follows:

* **Terminate** - the aim being to remove the risk entirely
* **Treat** - the aim being to reduce its impact and/or likelihood to more acceptable levels
* **Transfer** - the aim being to transfer or share the risk e.g. to or with a supplier
* **Tolerate** - to accept the residual risk (*see risk acceptance criteria in section six*)
* **Combination of actions** - taking more than one of the treatment options above

**Closed Risks**

Risks are only closed once they are deemed Terminated (See Above) or are no longer a threat to your organisation.

Examples of when risks may be closed:

* If we were to change a key software provider for our business processes, the risks associated with the old software would not be present. However, it would still be documented that the risks were addressed whilst they were present and open.
* Risks linked to older legislations which are no longer applicable would also be deemed as closed.

**NOTE: If an Annex A control is mitigating a risk, it is likely this risk will still be open, as there is still a chance the risk can occur.**

***Tips***

*Treatments are documented as required in terms of free text notes, tasks, discussions or documents, including where appropriate linked work to relevant policies or controls in the wider ISMS.*

If there are conflicts in the assessment, treatment or managing of risks, the following priority order will be used (with i. the highest priority)

1. Customer and user confidence in the Confidentiality of their data
2. The Integrity of the information
3. The Availability of the information (e.g.: if we found something that made information available but where its confidentiality or integrity were at unacceptable risk then we would choose not to make that information available)
4. Any legal, regulatory or contractual requirement identified from a risk perspective would trump any desire for internal business improvement or further growth
5. Where one or more parties are specifically impacted by a potential conflict in risk management, we may choose to take that to the relevant party and consider appropriate courses of action with them.   
     
   As part of that process, risk treatment may involve them accepting that risk or helping us treat that risk e.g. by transferring it, sharing it or co-operating on the removal of it

## Risk acceptance criteria

In general, we are happy to accept risks shown in the green area on the Risks & Treatments map. As the risk position increases into the yellow, red and black areas the less likely we are to accept the risk without further treatment.

The final risk acceptance criteria are determined by the risk owner, but should take into consideration the following:

* The level of residual risk to be accepted
* Any legal, regulatory or contractual obligations
* Business objectives and internal compliance requirements
* Other conflicting risks that may be introduced or changed from further treating the risk being considered (this may include e.g. risks to resourcing levels and/or financial implications)

The residual risk being tolerated (i.e. the risk remaining after acting) is demonstrated from its position on the risk map and this position will also determine how often the risk is to be reviewed (see above).

## Closed Risks

Risks are closed once they are deemed Terminated (See Above) or are no longer a threat to your organisation.

Examples of when risks may be closed:

* A change to a key supplier takes place. Any risks specific to the old supplier would no longer be present. By closing the risk, you can retain the audit trail of actions and decisions you took while the risk was open.
* Risks linked to older legislation, regulation or contractual requirements which are no longer applicable could also be closed if no longer relevant.

**NOTE**: If you are using a control to mitigate a risk, then generally the risk should remain open as a residual risk, rather than closed. As there is still a chance (however diminished) that the risk can occur.

## Opportunities

The standard requires the identification of “risks” and “opportunities”. The Risks & Treatments tool within the ISMS.online platform can be used to record and assess both.

The descriptions in the impact and likelihood tables in section 4 are used when conducting are written from the perspective of threat-based risks. Opportunity risks, when considered, are simply to be viewed through the mirror of the threat-based descriptions below e.g. where it says damage/consequence it may be a benefit instead.

## Applicable legislation & regulation risk assessment

ISO 27001 does not require the assessment of risks relating to each individual piece of legislation, regulation or contractual requirements. That said the use of the ISMS.online Applicable Legislation tool to record these enables this additional assessment to take place as follows.

1. Identify applicable legislation and regulation affecting the organisation
2. Add the applicable legislation and regulation into the Applicable Legislation tool within ISMS.online
3. Describe its applicability and relevance to your organisation (keeping it simple)
4. Conduct a likelihood and impact analysis on the risk for the organisation considering the following;
   1. Likelihood is the likelihood of a breach affecting compliance with the legislation, regulation or contractual compliance including how likely it is that the legislation will change
   2. Impact is the impact of a breach of the legislation and the effects of that legislation coming down on you (or your interested parties because of your behaviour) such that your business has negative consequences
   3. Risk acceptance criteria and risk review periods based on map position are the same as for information security risks detailed above

**Likelihood:**

|  |  |
| --- | --- |
| Score | Description |
| Very low | The legislation has relevance for you or interested parties who rely on your services to ensure compliance. Having complied, the legislation and controls to meet it are unlikely to change or influence daily business. It has very low day to day management and monitoring. |
| Low | The legislation has relevance for you or interested parties who rely on your services to ensure compliance but having complied, the legislation and controls to meet it are unlikely to change or influence daily business. It has low day to day management and monitoring. |
| Medium | The legislation has relevance for you or interested parties who rely on your services to ensure compliance. Having complied, the legislation and controls to meet it are unlikely to change or influence daily business but could do so given their nature. It has medium attention for management and monitoring. |
| High | The legislation has relevance for you or interested parties who rely on your services to ensure compliance. Having complied, the legislation and controls to meet it are highly likely to change or influence daily business given their nature. It has high attention for management and monitoring. |
| Very High | The legislation has relevance for you or interested parties who rely on your services to ensure compliance. Having complied, the legislation and controls or practices to meet it are very highly likely to change or influence daily business given their nature. It has very high attention for management and monitoring. |

**Impact:**

|  |  |
| --- | --- |
| Score | Description |
| Very low | Negligible or no damage to business operation and reputation with no costs or consequences. |
| Low | Low damage to business operation or reputation with negligible costs or consequences. |
| Medium | Some damage or loss to business operation or reputation with some cost exposure but not affecting future prospects. |
| High | Serious but not complete damage to business operation or reputation with large cost exposure and affecting future prospects. |
| Very High | Severe damage to business operation or reputation with very large cost exposure and leaving no future prospects. |

## Alignment with other important risk-based processes

<ADD OR REMOVED AS REQUIRED>