Guide to Opportunities and Risks

Annex SL

Most ISO Management System (MS) standards share a common structure. This was originally the High Level Structure (HLS), published in December 2012. A revision was published in May 2021 and it is now known as the Harmonised Structure (HS). This is specified in Annex SL, which is part of a large ISO specification document. Many standards now share this structure, including the following.

ISO 9001	Quality Management System (QMS)
ISO 14001	Environmental Management System (EMS)
ISO 22301	Business Continuity Management System (BCMS)
ISO/IEC 27001	Information Security Management System (ISMS)
ISO 45001	Occupational Health and Safety Management System (OHSMS)

Strategy

The alignment of ISO management standards to this common structure includes Clause 6.1, which specifies a requirement to consider opportunities and risks to the management system.

IMPORTANT	This assessment of opportunities and risks is STRATEGIC. The purpose of this is to devise STRATEGY.

Annex SL introduces other new components. Clauses 4.1 and 4.2 require you to identify the context of your organisation and interested parties, with respect to the management system and determine its scope. These will be different, for example, for a Quality Management System (QMS) and an Environmental Management System (EMS), but if you operate an Integrated Management System (IMS) you include everything relevant to the aspects of your operations that your IMS manages.

Clause 6.1 requires you to address opportunities and risks, taking into consideration issues identified by Clauses 4.1 and 4.2. The intention is to devise strategies, comparable to a SWOT (Strengths, Weaknesses, Opportunities and Threats) Analysis: the following link provides a good explanation of a SWOT Analysis. www.quickmba.com/strategy/swot In a SWOT Analysis the opportunities and threats are principally external factors, and the strengths and weaknesses are principally internal factors. In Clause 6.1, the opportunities and risks encompass both internal and external factors.

Tactics

Some standards also separately require management of risks, to a specific aspect of operations, such as ISO/IEC 27001, which requires management of risks to information and information processing assets, and ISO 22301, which requires management of risks to continuity of business operations.

IMPORTANT	*This management of risks is TACTICAL.* *The purpose of this is to manage (routine) risks to OPERATIONS.*

ISO/IEC 27001

This contains a set of controls in Annex A, which are primarily intended for use in the tactical / operational risk assessment, in Clauses 6.1.2, 6.1.3, 8.2 and 8.3, to manage risks to information.

However, you can also select some of these (such as 5.24, 5.25, 5.26, 5.27, 5.31, 8.7 and 8.13 etc.) to control risks to the management of information security, as part of your strategic assessment of opportunities and risks in ISO/IEC 27001, Clause 6.1.1.

Opportunities and Risks – Are Separate

One problem that arises from the introduction to ISO management standards, of consideration of risks and opportunities, is confusion caused by the definition of risk. The standards define risk and state that it can be positive as well as negative. This concept is also known and referred to as upside risk and downside risk. This conflicts with the common understanding that risk is a negative phenomenon. Also, the standards do not define opportunity. This has had the unfortunate consequence that some guidance on how to address risks and opportunities erroneously equates opportunity to positive risk.

The concept of positive risk exists because in some situations it is appropriate to evaluate the possibility of associated positive and negative outcomes in a consistent manner. A typical example is a financial investment, where it is appropriate to evaluate, in a consistent manner, the probabilities that an investor will make or lose money. The term positive risk may seem counterintuitive and a contradiction in terms, but it arises from a mathematical need. One possible way to accommodate the concept is to use the word ***outcome*** instead of ***risk***, with the understanding that the possibility of a negative outcome is what is commonly understood as a risk.

You can analyse opportunities more easily, if you utilise the concept of the possibility of a positive outcome (positive risk), and consider it as separate from, and different to, an opportunity.

(1) *A (negative) risk is the possibility of a negative outcome.*
A positive risk is the possibility of a positive outcome.

(2) *A (negative) risk (possibility of a negative outcome) or positive risk (possibility of a positive outcome) is something to which you are subject, without choice.*

You may be subject to a risk as a consequence of a choice that you made.

(3) *An opportunity is something that you can choose to pursue.*

(4) *An opportunity has an associated possibility of at least one positive outcome.*

(5) *An opportunity may have associated possibilities of both positive outcomes and negative outcomes (risks).*

(6) *After you choose to pursue an opportunity, you are then subject to its associated possibilities of negative outcomes (risks) and positive outcomes.*

(7) *You may have to take or increase (negative) risks to pursue an opportunity.*

(8) *An opportunity may be something that you can pursue, to mitigate a (negative) risk.*

(9) *If you choose to pursue an opportunity, you must review your assessments of possibilities of positive and negative outcomes (risks), and opportunities, to determine:*

(a) *Additional possibilities of positive and negative outcomes (risks), which arise because you now pursue the opportunity;*

(b) *Additional opportunities that arise because you now pursue the opportunity.*

For example, the sale of lottery tickets provides an opportunity, to buy a lottery ticket. If you choose to buy a lottery ticket, you pursue the opportunity. This opportunity has an associated possibility of a positive outcome and an associated possibility of a negative outcome (risk).

The possibility of a positive outcome is that you win the lottery. This has a very low likelihood.

The possibility of a negative outcome (risk) is that you do not win and therefore lose your stake, i.e., the price of the lottery ticket. This has a very high likelihood.

How to Address Opportunities and Risks

Section 6.1 Actions to address risks and opportunities of an ISO management standard aligned to Annex SL requires an organisation to consider risks and opportunities that arise from Section 4 of the ISO management standard. An opportunity may have associated risks (of both pursuing it and not pursuing it) so it is more convenient to itemise opportunities first and then risks.

Simple Opportunity Assessment

The following table provides a simple method to assess and manage opportunities.

Opportunity (*What we could choose to pursue and what would be the benefits*)	**Risks of Pursuing**	**Risks of Not Pursuing**	**Decision** (Pursue Defer Ignore)	**Actions to Pursue**	**Who** *(Persons that do actions)*	**Start** *(Date actions begun)*	**End** *(Date actions done)*

Simple Risk Assessment

The following table provides a simple method to assess and manage risks.

Risk (*What could happen and what would be the consequences*)	**Current Actions** (*to mitigate the risk*)	**Type of Treatment** (Accept Control Avoid Transfer)	**Further Actions** (*to mitigate the risk*)	**Who** *(Persons that do actions)*	**Start** *(Date actions begun)*	**End** *(Date actions done)*

IMPORTANT The two tables above comply with the requirement to address opportunities and risks of Clause 6.1 of management system standards, such as ISO 9001 and ISO 14001. Other management system standards, such as the following, additionally require formal assessment of risks, to a specific aspect of operations.

ISO/IEC 27001 requires assessment of risks to information
ISO 22301 requires assessment of risks of disruption
ISO 37001 requires assessment of risks of bribery

The Simple Risk Assessment table above does NOT comply with the requirements that these standards specify, of how to assess risks. ISO/IEC 27001 specifies detailed requirements of how to assess risks (to information). You should implement comparable methodologies for other standards, such as ISO 22301 and ISO 37001.