Annex SL – High Level Structure (HLS) Guide to Opportunities and Risks

1 Annex SL

ISO is imposing a common structure on its management system standards known as the High Level Structure (HLS) defined in Annex SL (an annex in an ISO specification document for management standards). This now applies to several management system standards including the following.

ISO 9001:2015	Quality Management System (QMS)
ISO 14001:2015	Environmental Management System (EMS)
ISO 22301:2012	Business Continuity Management System (BCMS)
ISO/IEC 27001:2013	Information Security Management System (ISMS)
ISO 37001:2016	Anti-Bribery Management System (ABMS)
ISO 45001:2018	Occupational Health and Safety Management System (OHSMS)

The alignment of ISO management system standards to Annex SL includes requirements to consider risks but these differ between standards. ISO 27001:2013 requires formal risk management that links to a set of controls specified in its Annex A. ISO 9001:2015 requires a much simpler arrangement. Annex SL introduces other new components.

Section 4 requires 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.

Sub-Section 6.1 requires an organisation to consider risks and opportunities that arise from Section 4.

2 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 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 an 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 lose your stake, i.e. the ticket price. This has a very high likelihood.

A (negative) risk usually consists of a threat and a vulnerability (a weakness that makes you susceptible to the threat). To assess the risk you must evaluate the threat and the vulnerability. To assess the possibility of a positive outcome, you must evaluate the nature of its positive influence and the extent to which it would affect the subject. The impacts of the above example are as follows.

Low Wage Worker	The possibility of a positive outcome would have a very high impact. The possibility of a negative outcome (risk) would have a low impact.
Professional	The possibility of a positive outcome would have a high impact. The possibility of a negative outcome (risk) would have a very low impact.
Head of Multinational	The possibility of a positive outcome would have a medium (or low) impact. The possibility of a negative outcome (risk) would have a very low impact.

3 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.

3.1 Simple Opportunity Assessment

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

Opportunity	Associated Risks	Decision	Outcome	Who	Start	End
What we could Choose to Pursue and What would be the Advantages.	*Risks of Pursuing Opportunity and / or Risks of Not Pursuing it.*	*Pursue Defer Ignore*	*Actions to Pursue Opportunity or Reasons Not to Pursue it.*	*Persons that do actions*	*Date actions begun*	*Date actions done*

3.2 Simple Risk Assessment

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

Threat	Vulnerability	Current Counter-measures	Risk Treatment	Who	Start	End
(What you cannot change.) What can happen and its consequences.	*(Elements under your control.) Weaknesses that make you susceptible to the Threat.*	*Existing arrangements or components that mitigate or eliminate the Vulnerability.*	*Type (Accept, Control, Avoid, Transfer) and Details of actions.*	*Persons that do actions*	*Date actions begun*	*Date actions done*

NOTE	***This method complies with the requirements of ISO 9001:2015 and ISO 14001:2015.*** It does NOT comply with the risk assessment requirements of ISO 22301:2012 – Business Continuity, ISO 27001:2013 – Information Security or ISO 37001:2016 – Anti-Bribery.
IMPORTANT	For ISO 22301, ISO 27001 or ISO 37001 (or any other management system standard that requires formal risk management) you can use this simple risk assessment table to list actual and potential risks as part of your identification of both opportunities and risks. When you have determined which opportunities you will pursue and therefore, which risks you will actually be subject to, you must manage the risks in accordance with the requirements of ISO 22301, ISO 27001 or ISO 37001 (etcetera): i.e. you must then add the (actual) risks to your risk register to manage them appropriately.