ISO/IEC 27001:2013 Information security management systems
- Information security risk treatment-

Possible options to treat risks:

- avoid the risk;
- control the risk and reduce risk level;
- transfer the risk;
- accept the risk;
- or a combination of those

The choice belongs to the organization and should be balanced taking into account resources and impact.

ISO/IEC 27001:2013 Information security management systems
- Information security risk treatment-

Statement of Applicability - SoA

“the organization shall produce a Statement of Applicability”

SoA - is the map of implementation of the ISMS.
Includes all the controls, their justification for inclusion, whether they are implemented or not and justification for excluding any controls from the Annex A (of ISO/IEC 27001).

SoA should be revised as the activities of the organization suffer changes

ISO/IEC 27001:2013 Information security management systems
- Information security risk treatment-

RiG CERT

Statement of applicability

No	Controls	Detailed	Justification for inclusion	Justification for exclusion	Implemented Y/N	Evidence of implementation
5.1.1.	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties	To define the expected levels of controls	-	Y	Documented policies - in the IS Manual Information security policy_code__ Access control policy_code, etc...
5.1.2.	Review of policies for information security		To ensure IS policies stay up to date	-	Y	The review of policies is done during management review (evidence kept in the management review minute)
14.2.6.	Secure development policy	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle	-	Our organization does not develop information systems	N	-

ISO/IEC 27001:2013 Information security management systems
- Information security risk treatment-

Risk treatment plan

The Risk Treatment Plan should include:

- the risk that is being addressed and its level according to the assessment;
- the actions proposed to treat the risk;
- who is in charge with implementing the actions;
- resources (budget);
- timeframe for implementation.

ISO/IEC 27001:2013 Information security management systems

- Information security risk treatment-

Residual risk

The remaining risk after treatment actions are applied.
Residual risk needs to be evaluated similar to the initial process to see if it falls into the acceptable category.
If not, new treatment should be decided.

Obtain the approval of the risk owners for the risk treatment plan as well as for the residual risks

Risk treatment has to be documented.