1.1.1 RISK MANAGEMENT POLICY

Scope

The risk management framework applies to all ISO 27001 ISO 9001 risks identified as part of the strategic business planning process to enable the organisation to pursue and achieve the BMS objectives set out in the Information Security and Quality Policies.

Responsibilities

The BMS Manager shall be responsible for ensuring that the organisational risk management framework meets the requirements of top management and of identifying legislative or regulatory requirements in terms of risk management.

Policy

The organisation evaluates strategic and operational risks on an ongoing basis. This approach recognises the evolution and fast-changing nature of the business.

Risk assessments shall be conducted at regular intervals or whenever there is a significant change to the business, to the scope of the BMS or emerging threat actors not previously considered in the current risk assessment.

Risk management

Risk is the effect of uncertainty on objectives. However, for ease of use and in line with ISO 27000, the risk is defined as the combination of the likelihood of an event occurring when a threat exploits a vulnerability and the impact of such an event on the organisation.

Risk Assessment Framework (Information Security)

Identify key assets and calculate risks

Key items that are within the scope of the BMS shall be assessed for risk using suitable tooling. This shall take into consideration the confidentiality, integrity and availability and consider the impact of a loss of the attribute(s) and the likelihood of that event occurring using the below-defined algorithm and calculates the risk. This risk is compared to the acceptance threshold.

Risks that are above the threshold shall be treated as appropriate (modification, transfer, toleration or termination). Mitigating controls shall be based upon those identified in Annex A of ISO 27001. Management may elect to treat risks that are calculated as acceptable where the business case indicates such treatment is appropriate.

When identified, each risk shall be assigned a risk owner and is estimated in terms of the likelihood of occurrence and the impact that there would be on the company if the risk was realised.

The impact is based on the loss of confidentiality, availability and/or integrity of the information asset. The impact is assigned a numerical score in the range 1-5. Annex 2., below, illustrates how scores are assigned. Dependant on the type of vulnerability, the impact of the vulnerability being exploited can be financial, operational or reputational, or a combination of these. Where a combination of impacts is expected, the highest-scoring is used for the risk analysis.

Analysis and evaluation of risks shall be conducted collaboratively wherever possible so that a consensus can be agreed on the correct estimation of risk levels. Overall responsibility for the risk assessment remains with the risk owner.

The likelihood is assessed according to the probability of occurrence. A numerical score is allocated according to Annex 3. The Risk Score for each Impact-Likelihood combination is calculated using formulae:

*Risk score = (Impact * Likelihood)*

Table 1. - Risk score values

IMPACT SCORE						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		LIKELIHOOD SCORE				

Risk Assessment Framework (Quality)

Identify key assets and calculate risks

Key items that are within the scope of the BMS shall be assessed for risk using suitable tooling. This shall take into consideration the confidentiality, integrity and availability and consider the impact of a loss of the attribute(s) and the likelihood of that event occurring using the below-defined algorithm and calculates the risk. This risk is compared to the acceptance threshold.

Risks that are above the threshold shall be treated as appropriate (modification, transfer, toleration or termination). Management may elect to treat risks that are calculated as acceptable where the business case indicates such treatment is appropriate.

When identified, each risk shall be assigned a risk owner and is estimated in terms of the likelihood of occurrence and the impact that there would be on the company if the risk was realised.

The impact is based on the loss of confidentiality, availability and/or integrity of the information asset. The impact is assigned a numerical score in the range 1-5. Quality - Risk Based Thinking (Risk Assessment), below, illustrates how scores are assigned. Dependant on the type of vulnerability, the impact of the vulnerability being exploited can be financial, operational or reputational, or a combination of these. Where a combination of impacts is expected, the highest-scoring is used for the risk analysis.

Analysis and evaluation of risks shall be conducted collaboratively wherever possible so that

a consensus can be agreed on the correct estimation of risk levels. Overall responsibility for the risk assessment remains with the risk owner.
The likelihood is assessed according to the probability of occurrence. A numerical score is allocated according to Quality - Risk Based Thinking (Risk Assessment). The Risk Score for each Impact-Likelihood combination is calculated using formulae:

*Risk score = (Impact * Likelihood)*

Table 1. - Risk score values

IMPACT SCORE						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		LIKELIHOOD SCORE				

Assess the risks

The impact that might result from each threat-vulnerability is defined as part of the risk assessment methodology as the value of the asset which the threat-vulnerability combination would exploit and this figure is held for each attribute.
The realistic likelihood that each of these failures might occur shall be assessed using the likelihood scale from the risk assessment framework.
The risk levels are then automatically calculated, for each risk, and shown as risk rating value.
The initial risk score represents the risk level prior to treatment i.e. inherent risk. The Board has determined that within this assessment model, the risk levels are categorised as follows:

- Risk scoring 1 – 4 – Minor risks – acceptable risk without further treatment
- Risk scoring 5 – 14 – Moderate risks – acceptable, but not desirable risks. Risks evaluated at this level are selected for risk treatment (on a high priority) to attempt to reduce the level of risk.
- Risk scoring - 15 - 25 – Severe risks – treat immediately upon completion of risk assessment/risk discovery.

All risks which score above 4 shall be entered into the risk treatment plan (described below)

for further analysis for risk treatment.
The risk assessor for the management system shall identify risks to its management systems and shall determine risk treatment options in consultation with risk or asset owner:

- Eliminating the risk by removing the activity affected by the risk
- Accepting the risk to pursue an opportunity
- Removing the source of the risk
- Changing the likelihood of the risk coming to pass
- Changing the consequences of the risk coming to pass
- Sharing the risk with another party or parties (such as via suppliers, insurance or other third parties).

The risk assessor shall create a risk treatment plan providing the following information:

- The reasons for selected treatments, including expected benefits
- Those responsible for approving the risk treatment plan
- Those responsible for implementing the risk treatment plan
- Proposed actions
- Resource requirements and contingencies
- Treatment performance measures and limitations
- Requirements for reporting and monitoring
- Timing and schedule for the risk treatment
- The risk treatment plan is agreed with the risk owners.

The risk treatment plan shall be implemented in accordance with organisational processes and the risk treatment plan itself. Treatment options shall be identified for each of the assessed risks; whether the risk is acceptable or if it must be controlled in line with criteria established in the risk assessment framework.
Appropriate control objectives and controls shall be selected from those listed in Annex A of ISO 27001. Residual risk shall be estimated once all controls have been identified and implemented.
The final residual risk will then be shown in the risk assessment table for the threat-vulnerability combination. The risk assessor then summarises all the selected control objectives and controls into the Statement of Applicability, which can then be drawn up together with the justification for inclusion or exclusion of each ISO 27001 control.
A risk treatment plan is produced identifying the controls to mitigate risk, the risks being addressed (or areas) with the actions to mitigate risk, priority and responsibility. This risk treatment plan may be divided into sections or work patterns as appropriate.
Much of the mitigation of risk is defining and documenting the practices currently in place to assist their suitability and accountability. Key risks or risk areas may be summarised in a short-form summary to aid management planning and prioritisation.
The risk treatment plan shall be reviewed and accepted by top management. The risk treatment plan shall be updated as appropriate.
The risk treatment plan is drawn up after the initial risk assessment and shows how the controls are implemented. The result of implementing these controls is re-assessed as the

residual risk.
The risk treatment report as output from the risk assessment tool is reviewed manually and from this, the summary risk treatment plan report is derived. This shows the key areas that require additional actions over and above documentation.
The risk treatment plan is derived by inspection and review of the risk assessment and is reviewed and updated until all relevant risks have been suitably addressed.
The risk assessment is reviewed upon significant change and at least annually.

Edocuments Limited, Unit 32 Waterhouse Business Centre,
Chelmsford, Essex, CM1 2QE
Company Number: 04236508

www.edocuments.co.uk
info@edocuments.co.uk
T: +44 (0)1245 330010