How to Maintain a Risk Register

Management of (negative) risks is fundamentally a simple process that consists of identifying something that can happen, what its consequences are, what your vulnerability is to it, what you already do, and what else you can do, to prevent or mitigate it.

People to Involve in Risk Assessment and Management

The correct people to involve in risk assessment and management are people with a good knowledge and understanding of the product, service, system or organisation, for which you must identify, assess and treat the risks. The most important aspect of risk management is risk identification. You can only assess and treat risks that you identify. Risk assessment and management is essentially a simple process that you and your colleagues can and should do yourselves, without outside help.

Risk Priority is Treatment Priority, not Risk Seriousness

If you must manage a substantial number of risks, it is advantageous to use a method in which you quantify the Consequence and estimate the Likelihood of each risk, from which you calculate a Risk Priority, to rank the risks. The most common method requires you to assign a value of 1 (Low), 2 (Medium) or 3 (High) to the Consequence and Likelihood, from which you calculate a Risk Priority using the following formula.

Risk Priority = Consequence x Likelihood

Alternatively, you can use the formula below, which assigns greater weight to the Consequence. This may be more suitable for Health and Safety risks, to ensure that you assess and appropriately treat risks in order of severity of injury or illness. The formula is also more suitable if it is difficult to reliably estimate the likelihood, which is frequently the case.

Risk Priority = (10 x Consequence) + Likelihood

The most important aspects of risk management are risk identification and risk treatment. If you identify 67 risks you must decide how to treat all 67 of the risks, irrespective of the order in which you list them, and even if the treatment for several is simply to accept the risk.

(1) The Risk Priority is not a measure of the seriousness of a risk. It is not expressed in any units and is based on the Consequence and Likelihood, which may only be rough estimates.

(2) The Risk Priority is a number that ranks risks, to assist you to assess and manage them. The Risk Priority puts risks in an appropriate order of priority, so that when you have a meeting to decide how to treat the risks, you have them in a list with the highest priority at the top and lowest priority at the bottom.

NOTES	(A)	Only categorise Consequence and Likelihood on a scale of 1 to 3. If you categorise them on a scale of 1 to 5 or 1 to 10 it has little effect on the order and no effect on the treatment, so it is a waste of time.
	(B)	You should review the risks as you apply treatments, so the order in which you rank them will change.
	(C)	It is more productive and effective to use your time and devote your thinking, to identify the risks and decide how to treat them (than how to rank them).

Standard Risk Assessment

This describes how to do risk assessments that satisfy the requirements of the following standards.

ISO 27001 – Information Security Management
ISO 22301 – Business Continuity Management

You can adapt it to do risk assessments for other standards, such as the following.

ISO 37001 – Anti-Bribery Management
ISO 45001 – Occupational Health and Safety Management

Risk Methodology

A variety of risk scenarios are identified and linked to specific assets. In each case the threats and vulnerabilities are identified and linked to an appropriate assessment of the consequences of the risk.

NOTE	For information security risk assessments, the assessment of the consequences of the risk is based on identification of whether confidentiality, integrity, or availability would be compromised in the scenario.

Consequence and Likelihood Grading

The **Consequence** and **Likelihood** of every risk are each assigned a value of 1 to 3, and multiplied together to give a **Risk Priority** from 1 to 9. This represents the current residual risk within the IMS.

Consequence

3	High	**Information Security** Public exposure of confidential or personal, sensitive information leading to significant embarrassment for the company, or its customers. **Business Continuity** Severe and/or long term disruption. For example: fire or structural damage to building; severe weather for a long period; serious epidemic.
2	Medium	**Information Security** Exposure of confidential or personal sensitive information to a non-authorised third-party, system downtime or data corruption, with undesirable consequences upon operations and with potential consequences upon customer(s). **Business Continuity** Temporary, substantial disruption. For example: a loss of electrical power, for several hours; severe weather for a short period, minor epidemic.
1	Low	**Information Security** Internal exposure of internally restricted information beyond authorised individuals, system downtime or data corruption, with only minor disruption to operations. **Business Continuity** Temporary, minor disruption. For example: a loss of electrical power, which resumes before our UPSs (Uninterruptible Power Supplies) cease to provide emergency power to our phone system and principal servers.

Likelihood

3	High	Likely to happen within the next 2 months
2	Medium	Likely to happen within the next 12 months
1	Low	Unlikely to happen within the next 12 months

Risk Treatment Criteria

The following table gives a recommended risk treatment plan that specifies who has the authority to accept risks at varying levels.

Risk Treatment

Risk Priority = Consequence x Likelihood		**Risk Treatment**
6 or 9	***High***	***Director reduces or accepts risk.***
3 or 4	*Medium*	*Management Review Meeting reduces or accepts risk.*
1 or 2	Low	Acceptable – Review annually.

Documentation

The risk assessments are documented in a table with the following columns.

(1) **Date Logged**

(2) **Process**

A (business or management system) Process of the operations of your organisation.

(3) **Asset**

The asset, such as the following examples.

IT Infrastructure
Sage Payroll data
Personnel (paper) files
Cisco certified staff

(4) **Type (of the Asset)**

One or more of the following five categories.

Information
Hardware
Software
Services
People

(5) **Risk Owner**

The person or entity with the accountability and authority to manage the **Risk**.

(6) **Threat (what you cannot change)**

A description of what may happen to the **Asset** (such as loss, corruption, damage, attack), how it may happen and the possible consequences.

(7) **Property (of the information Asset)**

One or more of the following three aspects of the information **Asset** that the **Threat** could influence.

Confidentiality
Integrity
Availability

Refer to the **Terms and definitions** in the following.

ISO 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary

NOTE	This column applies to any risk to (security of) information.

(8) **Consequence (1 to 3)**

A number, ONE, TWO or THREE, that represents the severity of the effect that the **Threat** could have on the **Asset**.

Refer to the ***Consequence*** table above.

(9) **Vulnerability (elements under your control)**

A description of one or more weakness(es) that make the **Asset** susceptible to the **Threat**.

(10) **Current Countermeasure(s)**

Any organisational arrangement(s) and / or component(s) of infrastructure that mitigate or negate the **Vulnerability**.

(11) **ISO 27001, Annex A, Reference(s)**

Any controls that correspond to the **Existing Countermeasure(s)**.

IMPORTANT		
	(1)	A risk may be to more than one aspect of operations, such as quality, resilience (business continuity) and (security of) information.
	(2)	This column applies to any risk to (security of) information.
	(3)	Specify all ISO 27001, Annex A, controls that apply to the risk.
	(4)	Specify any non ISO 27001 controls that you apply; either: where no suitable ISO 27001 control exists, or in addition to any ISO 27001 control(s). For example, if you implement ISO 27001 with ISO 37001, you may devise and apply controls from ISO 37001, Annex A: A.10 Due diligence; A.11 Financial controls; A.12 Non-financial controls.

(12) **Likelihood (1 to 3)**

A number ONE, TWO or THREE that represents the likelihood that the **Threat** will occur.

Refer to the ***Likelihood*** table above.

(13) **Risk Priority (= Consequence x Likelihood)**

Multiply the **Consequence** and **Likelihood** together to give the **Risk Priority** that represents the current residual risk within the ISMS.

Refer to the ***Risk Treatment*** table above.

(14) **Risk Treatment Plan**

A description of the planned treatment(s), in response to the **Risk Priority**, based on the **Risk Treatment Criteria**.

Refer to the ***Risk Treatment*** table above.

(15) **Treatment Type**

One or more of the following four categories of treatment that comprise the **Risk Treatment Plan**.

Accept
Control
Avoid
Transfer

(16) **Treatment Owner**

The person or entity that is responsible for the implementation of the **Risk Treatment Plan**.

(17) **Review Date**

The planned date of review of the implementation of the **Risk Treatment Plan**.

(18) **Desired Risk Priority (1 to 3)**

A number ONE, TWO or THREE that is an estimate of the likely long-term residual risk following the planned treatment(s).

Health and Safety

This describes a modification to the risk methodology described in the previous pages, to assess risks to health and safety. The formula **Risk Priority = Consequence x Likelihood** is appropriate for the management of information security and business continuity risks. This modification uses the following formula that assigns a higher Risk Priority to deaths and serious injuries than minor injuries, which is appropriate for the management of health and safety risks. *You may also choose to use this formula for other types of risk assessment if it is difficult to reliably estimate the likelihood.*

Risk Priority = (10 x Consequence) + Likelihood

NOTE The **Risk Priority** that this formula assigns is a two-digit number with the **Consequence** as the first digit and the **Likelihood** as the second digit.

NOTE *Use appropriate descriptions of consequences. Those listed below are suggestions.*

Consequence

3	High	Death; Permanent disablement; Loss of a limb, eye, sight, hearing; Serious or critical injury with permanent after effects.
2	Medium	Serious recoverable injury with no or superficial permanent after effects.
1	Low	Minor injury.

NOTE *Use appropriate periods (that make it simple) to estimate likelihood. The three combinations of periods (1 & 10 or 2 & 15 or 5 & 25 years) shown in the following table are suggestions.*

Likelihood

3	High	Likely to happen within the next 1 (or 2 or 5) year(s).
2	Medium	Likely to happen within the next 10 (or 15 or 25) years.
1	Low	Unlikely to happen within the next 10 (or 15 or 25) years.

NOTE *Group the Risk Priority numbers appropriately. The groupings shown below are suggestions.*

Risk Treatment

Risk Priority = (10 x Consequence) + Likelihood		**Risk Treatment**
22, 23, 31, 32 or 33	***High***	***Director reduces or accepts risk.***
12, 13 or 21	*Medium*	*Management Meeting reduces or accepts risk.*
1	Low	Acceptable – Review annually.