Implementing ISO 37001 with ISO/IEC 27001 and other Management System Standards

1 *Introduction*

*This document examines the implementation of **ISO 37001 – Anti-bribery management systems – Requirements with guidance for use** together with ISO/IEC 27001, and other management system standards. There are two reasons to consider this.*

(1) The main use of certification to management system standards is to facilitate procurement. It is inevitable that any potential customer who requires or prefers certification to ISO 37001, will also require or prefer, certification to other appropriate management system standards.

(2) Implementation of ISO 37001, in particular, together with ISO/IEC 27001, can support more comprehensive anti-corruption and anti-fraud management.

2 ISO 37001 – An Innovative Management System Standard

ISO 37001 is a management system standard that differentiates itself from others because it provides two interesting innovations.

(1) ISO 37001 Manages Something that Should Never Happen

ISO 9001 is a management system standard against which you assess management of an aspect of operations that is essential, i.e. quality of delivery of products and services and customer satisfaction. If a company does not provide its customers with products and services they are willing to pay for, it will eventually fail.

Other management system standards, such as ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001 and ISO 50001, are standards against which you assess management of an aspect of operations that may be desirable and/or associated with legal requirements.

ISO 37001 is a standard against which you assess management of an aspect of operations that should never happen, because it is a crime.

(2) ISO 37001 Invokes the Involvement of a Governing Body

Other management system standards require leadership and support from the (operational) Top Management, as does ISO 37001, Section 5.1.2.

ISO 37001, Section 5.1.1 introduces the concept of the Governing Body.

If an organisation has a Governing Body, ISO 37001, Section 5.1.1 also requires its approval and oversight.

NOTE	An (integrated) management system that complies with ISO 37001, together with one or more other management system standards, such as ISO 27001, can be implemented so that other components, in addition to its anti-bribery components, require the approval and oversight of the Governing Body, to prevent not just bribery, but also other forms of corruption and fraud.

3 ISO/IEC 27001 and Information Security

The full title of ISO 27001 is **ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements**. This implies, and unfortunately gives the impression, that it only applies to information and data held and processed by, Information and Communications Technology (ICT) systems.

The overwhelming volume of information and data is now held on ICT systems. However, the standard ISO/IEC 27001 is written so that it can be applied to any form of information and data, including paper documents and records, and even information that exists in an intangible, undocumented form, such as an employee's knowledge and experience.

The implementation of an Information Security Management System (ISMS), compliant to ISO/IEC 27001, is correctly perceived as an effective tool to assist organisations to protect information, such as personal data and card details, from threats such as cyberattacks. This unfortunately also gives the mistaken impression that the purpose of ISO/IEC 27001 is to protect and maintain confidentiality. In fact, ISO/IEC 27001 assigns equal importance to the following three properties of information.

Integrity	Information is accurate and complete.
Availability	Information is accessible and usable upon demand by authorized individuals, entities and processes.
Confidentiality	Information is not made available or disclosed to unauthorized individuals, entities, or processes.

The maintenance of security of information (in accordance with ISO/IEC 27001) is, by definition, the maintenance of all three properties. Security of information can also include one or more other properties, such as the following. [Refer to ISO/IEC 27000 (*available free of charge*) for definitions.]

Authenticity	An entity is what it claims to be.
Non-Repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities.
Reliability	Consistent intended behaviour and results.

3.1 ISO/IEC 27001, Annex A – Controls

It is straightforward to implement **ISO 37001 – Anti-bribery management systems – Requirements with guidance for use** with ISO/IEC 27001, because they share the High Level Structure (HLS) specified by Annex SL. However, ISO/IEC 27001 is in two parts. The first part is the main standard structured according to the HLS. The second part is Annex A, that consists of a set of grouped controls, of which, the following can be useful to support implementation of ISO 37001.

A.8.2 - Classification of information specifies requirements, to classify information (for example as Public, Unrestricted, Restricted, Confidential, Sensitive, Secret etcetera), and define how you label and handle information with different classifications.

A.16.1 - Management of information security incidents and improvements specifies requirements for how to manage instances where information is incomplete, inaccurate or unavailable, or where an unauthorised disclosure of confidential information has occurred.

A.18.1 - Compliance with legal and contractual requirements requires you to specify how you comply with legislation, such as data protection, bribery, money laundering, fraud and accounting regulations etcetera.

4 Opportunities and Risks

An important link to consider between ISO 37001 and other management system standards is the initial identification of opportunities and risks.

ISO 45001 A risk of bribery may be a risk to health and safety if part of the intention of the corruption is to avoid compliance with health and safety laws and regulations.

ISO 14001 A risk of bribery may be a risk to environmental impact if part of the intention of the corruption is to avoid compliance with environmental laws and regulations.

ISO 9001 A risk of bribery may be a risk to quality, for example, if there is a risk that a contract may be awarded to a supplier that does not provide optimum quality and/or part of the intention of the corruption is to avoid compliance with product or service regulations.

ISO 22301 *Most people intuitively think of events such as suspension of utility services (water and electricity), fire, flood or extreme weather in the context of business continuity. However, the departure or absence of a worker, due to resignation, illness, injury or any other reason, could cause disruption. A risk of bribery may be a risk to business continuity, because bribery may result in the arrest and detention of staff, prosecution resulting in a fine, imprisonment and the appointment of a monitor to oversee operations. All of these could (severely) disrupt the operations of an organisation.*

ISO/IEC 27001 A risk of bribery is a risk to security of information, because it is a risk to the integrity and availability of information. It is common practice to record inaccurate and incomplete financial and other records to hide or disguise the payment or receipt of a bribe. For example: a false purchase order and false invoice might be raised to facilitate payment for (1) a fictitious service such as consultancy; or (2) non-existent (or an inaccurate quantity of) goods and/or services. Information is incomplete if the offer or receipt of a bribe is not declared. Any risk of false accounting, fraud and money laundering etcetera is, by definition, a risk to security of information.

A risk of bribery may be a risk to other aspects of operations. Similarly an opportunity with respect to anti-bribery management may be an opportunity with respect to other aspects of operations.

5 Financial and Non-Financial Controls

The following two sub-sections of ISO 37001 are conspicuous by their brevity; each consists of just one sentence. They both require the implementation of controls, but specify no details whatsoever.

Section 8.3 – Financial Controls
Section 8.4 – Non-Financial Controls

The predominant anti-bribery legislation is the USA **Foreign Corrupt Practices Act (FCPA)**, which consists of the following two components.

Anti-Bribery Provisions
Books and Records Provisions

ISO 37001, Sections 8.3 and 8.4 relate to the FCPA Books and Records Provisions. Elsewhere, however, other anti-bribery legislation differs considerably. The UK **Bribery Act 2010** does not contain an equivalent component to the FCPA Books and Records Provisions. The UK has other applicable legislation such as the following.

Criminal Finances Act 2017
Money Laundering Regulations 2017

5.1 ISO/IEC 27001

The requirements to implement financial and non-financial controls effectively require an organisation to ensure that it records and retains complete and accurate monetary and non-monetary details of its commercial activities. In other words it requires an organisation to ensure integrity and availability of information, so this is really an information security problem. The most appropriate standard against which to assess this activity is ISO/IEC 27001 rather than ISO 37001.

NOTE	If, additionally, your definition of information security also includes other properties, such as **authenticity**, **non-repudiation** and **reliability**, this can further reinforce your implementation of financial and non-financial controls.

5.2 ISO 9001

Financial and non-financial controls will closely relate to and/or be an integral part of the **purchase and invoice processes**, with respect to management of quality of delivery of products and services, in accordance with ISO 9001 [Section 4.4 – Quality management system and its processes].

5.3 Ensuring Compliance – Speed Bumps and Speed Cameras

5.3.1 Speed Bumps

We live on a main road with a 30mph speed limit. However, it is a wide straight road and in the evenings many drivers feel compelled to drive at speeds close to, or even in excess of, 60mph.

However, in other nearby, quiet residential streets, drivers routinely drive at around 20mph. The reason for this lawful behaviour is quite simple: the quiet residential streets have substantial speed bumps and any attempt to drive at high speed would result in the destruction of the car's suspension.

5.3.2 Speed Cameras

Most years, during the summer, we like to go for a short holiday in Scotland. As we drive north, and reach England's most northern county, Northumberland, we notice that drivers comply with the speed limits, and drive at 60mph on single carriageways, and 70mph on dual carriageways. This cautious behaviour is also the norm in Scotland. This is somewhat different to most of England, where many drivers routinely exceed the speed limits and drive at approximately 80mph on dual carriageways.

The explanation for this lawful behaviour is quite simple: Northumberland and Scotland have more operational speed cameras than in most of England. Drivers know that if they exceed the speed limit and break the law they are likely to be photographed by a speed camera, and subsequently receive a fine, and penalty points' endorsement, on their driving licence.

5.3.3 Ensuring Compliance

Many drivers knowingly exceed speed limits if they believe that they can get away with it, and will not be apprehended and punished. These drivers will only obey the speed limit if (at lower speed) speed bumps physically constrain them to do so or (at higher speed) they are certain that they will definitely be convicted and punished if they exceed the speed limit.

The same philosophy should be applied to ISO 37001, Section 8.3 – Financial Controls and Section 8.4 – Non-Financial Controls. An organisation should implement financial and non-financial controls that record extensive details, to make it difficult to pay or receive a corrupt or unlawful payment, and/or are likely to reveal that a payment is corrupt or unlawful.

6 Raising Concerns (Whistle-Blowing)

6.1 Classification of Information (for Investigation of Concerns)

ISO 37001, Section 8.9 - Raising Concerns requires an organisation to provide arrangements for what is commonly referred to as whistle-blowing.

> This requires you to ensure confidentiality of reports and investigations. However, it is necessary to disclose some information, in order to act upon a raised concern.
>
> You must appropriately implement **ISO 37001, Section 7.5 - Documented Information** so that it is consistent with, and facilitates, the implementation of **ISO 37001, Section 8.9**.

*The control group **ISO/IEC 27001, A.8.2 - Classification of Information** requires that you define **categories** of information and specify how to **label** and **handle** each category. This can provide a clear structure to assist the implementation of **ISO 37001, Section 7.5 - Documented Information** (which you would implement together with **ISO/IEC 27001, Section 7.5 - Documented Information**).*

6.2 Alternative Options for Management of Raised Concerns

6.2.1 ISO/IEC 27001

The implementation of ISO 37001, together with ISO/IEC 27001, provides the opportunity to raise a concern, such as inadequate accounting records, as either of the following ISO/IEC 27001, Annex A controls:

(a) An information security incident, against

A.16.1 - Management of information security incidents and improvements;

(b) An unacceptable accounting practice, as a non-conformity, against

A.18.1 - Compliance with legal and contractual requirements.

This provides the option to manage a concern in a less contentious manner, as an operational or technical matter, against a procedure, rather than as malpractice, against one or more person(s).

6.2.2 ISO 9001

If ISO 37001 is alternatively or additionally implemented with ISO 9001, an issue of concern may also be managed as a non-conformity, which may be a consequence of a shortcoming of a **process** [Section 4.4 – Quality management system and its processes].

7 Auditing in Accordance with ISO/IEC 27006

One of the benefits (or disadvantages, depending upon your point of view) of implementing an Integrated Management System (IMS) in accordance with ISO/IEC 27001, together with ISO 37001, (and other management system standards such as ISO 22301 and ISO 9001 etcetera) is that the CAB will perform the certification audits of your IMS in accordance with ISO/IEC 27006 in addition to ISO/IEC TS 17021-9 (and ISO/IEC TS 17021-6 and ISO/IEC 17021-3 etcetera respectively).

In other words, your IMS will be subject to more thorough audits.

ISO/IEC 17021 Series	The ISO/IEC 17021-2, ISO/IEC 17021-3 and ISO/IEC TS 17021-4 to ISO/IEC TS 17021-9 standards, which supplement ISO/IEC 17021-1, only specify the required competences of auditors and audit teams.
ISO/IEC 27006	This, by contrast, is a more comprehensive audit standard that specifies the required competencies of auditors and audit teams, and other audit requirements, including duration of certification and surveillance audits.

8 Sub-Section 6.1 Actions to address risks & opportunities

*A component of the core text of the Annex SL High Level Structure (HLS) is **Section 6.1 – Actions to address risks and opportunities**.*

It is in accordance with the requirements of this Sub-Section 6.1, in the various management system standards, that opportunities of how to implement an effective Integrated Management System (IMS), which integrates management of two or more aspects of operations (such as quality management and information security management with anti-bribery management), should be identified and addressed.

In particular, for an IMS that integrates anti-bribery management with management of one or more other aspects of operations, it is in accordance with the requirements of this sub-section that opportunities of how to implement effective financial and non-financial controls and alternative ways to manage raised concerns should be identified and addressed.

9 Acknowledgement

*I wish to acknowledge the contribution of **Jan Branzell, CEO Veriscan**, who made an invaluable suggestion on how to improve this document.*