Guidance Note.
Risk Management: What is a control?

To understand an organisation ’s problem, we need to understand how the business is managed.

- Map the process to the controls to understand how management knows business is functioning as intended
- Look for management of controls to understand impacts to intended business objectives

Example:

Business Objective: Money in the safe is secure

Business Process: CFO places cash into the safe, uses key to lock the safe, key to safe is placed with the President. To get cash into or out of the safe, the CFO must request the key from the President.

Management Control:

1. President reports to the Board of Directors (BoD) on all key requests
2. CFO reports to the BoD on all cash deposits and withdrawals
3. BoD reconciles all cash

What is a Control?

Controls are a combination of people, processes and tools that are put in place to prevent, detect or correct issues caused by unwanted events. The need is to create a carefully planned control framework that weaves the various types of controls together and protects the organisation from risks.

In short, a control design should measure in order to manage.

- What are you protecting?
- Why are you protecting?
- How are you protecting?
- How do you know your protection is working?

What is an Internal Control?

Internal Control objectives are desired goals or conditions for a specific event cycle which, if achieved, minimise the potential that waste, loss, unauthorised use or misappropriation will occur. They are conditions which we want the system of internal control to satisfy.

In short: what is measured is managed – for each and every component of the business

For each business process, support workflow, system

- What are you protecting?
- Why are you protecting?
- How are you protecting?
- How do you know your protection is working?

Types of controls

The internal control works within a business function which is designed to support internal business objectives such as client money transfers cannot be received from unapproved countries. An external control would be a regulatory requirement such as anti-money laundering laws requiring money transfers from authorised countries.

In an effective internal control system, the following five components work to support the achievement of an entity's mission, strategies and related business objectives.

1. **Control Environment.** (Integrity and Ethical Values, enforcement)
2. **Risk Assessment.** (Company-wide objectives, requirements)
3. **Control Activities.** (passwords, encryption, logging enabled)
4. **Information and Communication.** (requests, SLA)
5. (log management (Security Information Event Management system - SIEM),Service Level Agreement (SLA), breach)

Why do we need to design internal controls in the organisation ?

The control design safeguards the organisation , minimises risks, and protects assets. As you can imagine without an internal control, management receives random or unpredictable results. Design of the internal control begins with the business objectives.

How to create a control

Business states the objective and the design of who gets access to what, when, and how becomes the control. Measuring the control is reporting such as reporting on a key performance measure or risk, service, or compliance indicators.

There are six principles used in designing an internal control.

1. Establish Responsibilities.
2. Maintain Records.
3. Insure Assets by Bonding Key Employees.
4. Segregation of Duties.
5. Mandatory Employee Rotation.
6. Split Related Party Responsibility.
7. Use Technological Controls.
8. Perform Regular Independent Reviews.

Creating internal controls supports business safeguarding their assets.

ISO 9001 is one of the most well known management systems and it is process based and risk based. Consider these objectives:

Build our reputation as trusted risk partners - through people, process, technology, best practice and better use of data to provide more responsive coverage and tailored risk management insight and advice - in a way that is ‘size and sector appropriate.’

Highlight the coverage gaps, the threats and impact to intangible risks, as well as help clients to better manage complex interconnected risks (cyber, supply chain, Environmental and Social Governance (ESG) that increasingly matter in the new world order.

Move from a linear product-based approach, to offer a more client-centric, collaborative and responsive service.

ISO 9001 management system is ideal for meeting these objectives.