

Taking a risk-based approach to internal audits

Internal audits are – or at least they should be – an important aspect of a management system. Their importance is illustrated by the fact that they are a **mandatory** activity required by standards such as ISO 9001 (Quality), ISO 14001 (Environment), and OHSAS 18001 (Health and Safety). These standards don't say 'You might want to consider doing some internal audits' – they use words like **shall**. In short, when it comes to the subject of internal audits, they mean business - and with very good reason too. For good control systems need feedback mechanisms, and internal audits are a key feedback mechanism for a management system. Internal audits offer an organized means of regularly verifying that the system is operating as intended and is achieving the desired outcomes. In the terminology of the standards referred to above, the purpose of Internal audits is to determine whether the management system 'conforms to planned arrangements' and is effectively 'implemented and maintained'.

Certification bodies also take internal audits very seriously. They have to, as the topic is a requirement for both certification and surveillance audits. Also - in an ideal world – a well-planned and executed programme of internal audits can make an external audit by a certification body a great deal easier, as to a large extent, they can simply be monitoring, reviewing, and verifying the results of the internal audits.

The current situation

In view of the above, you would be excused for thinking that organisations with management systems – particularly those that maintain certification – would plan their internal audit programme to achieve maximum benefit. Unfortunately, that is often not the case. Many a certification auditor will have visited a client to find that a series of internal audits were performed in the days immediately prior to the certification audit, and that these were tightly based on the clauses of the standard. In some cases, this may be indicative of a cynical approach whereby the organization seeks only to 'play the game' in order to maintain their certification. As part of that game, they simply go through the motions of the internal audit process in a cursory manner. However, in many cases, there is a genuine lack of understanding of how this feedback mechanism can most cost-effectively help better manage the organisation.

Lets look at how the internal audit process can provide better outcomes, while making the most efficient and effective use of resources available.

Status and importance

The standards refer to organizations varying the scope and frequency of their internal audits on the basis of status and importance – but what does this mean? Well, lets' start with the following simple explanations of frequency and scope...

Frequency – Some audits may be repeated on a more frequent basis than others

Scope - Some audits may be a cursory check while others may be a more in-depth investigation

OK, so variations to the audit schedule may allow some to be audited more often, and some to be audited in more depth – while the reverse applies to others. So far so good, but what is meant by applying those variations on the basis of status and importance? The answer to that question is of course given away in the

title of this article – it means **risk**. In essence, we can use the perception of risk as the basis for deciding the frequency and scope of our audits. The ISO 9001 standard seems determined to avoid using the term risk directly – while referring to it in round-about ways – while the term is directly referred to in other management standards.

Risk may be determined by considering both the likelihood of something going wrong, and the consequence of that happening. While there are various methods of establishing risk levels in this way, the following illustration is a popular example taken from the AS/NZS 4360 Risk Management standard. In this matrix model, where values of likelihood and consequence meet, a resultant risk level is calculated e.g. an event considered Likely to happen (B) that would have Major Consequences (4) is deemed to be an Extreme (E) Risk.

			Consequence				
			Insignificant	Minor	Moderate	Major	Catastrophic
			1	2	3	4	5
Likelihood	Almost Certain	A	H	H	E	E	E
	Likely	B	M	H	H	E	E
	Moderate	C	L	M	H	E	E
	Unlikely	D	L	L	M	H	E
	Rare	E	L	L	M	H	H

Risk level	
Code	Descriptor
E	Extreme
H	High
M	Moderate
L	Low

To be really useful, someone needs to define what constitutes these various values of Likelihood, Consequence, and Risk in the context of your audit subject matter. A tool such as this matrix may be formally incorporated into your planning process, or more loosely used as a planning guide.

Remember, internal audits may be based on a process, a contract, an event, or some other criteria. Some of the factors that might increase the risk related to those criteria are listed below. Consider whether these might affect the likelihood and/or consequence of problems:

Factors	Could affect?	
	Likelihood	Consequence
Where a new product or service has been introduced		
Where an existing product or service has changed significantly		
Where a new process has been introduced		
Where new equipment or materials have been introduced		
Where there has been a change in software used		
Where the organization has relocated		
Where there has been a change of personnel		
Where there has been a change of suppliers		
Where there has been a change in legislative / regulatory requirements		
Where there has been a significant change in organizational structure		
Where there has been a significant change in organizational objectives / targets		
Where previous internal audits highlighted problems		
Where there is a known history of problems within the organisation		
Where there are reports of problems in similar organisations		
Where a significant percentage of work is for one key customer		

Of course, this is not an exhaustive list of risk factors, but should give food for thought. Most of the examples above fall into two categories – those related to **change**, and those related to a **known history of problems**.

- For those in the 'change' category, there is typically an increased likelihood of problems – particularly in the time immediately after the change. Depending on circumstances, the consequence of problems may increase, decrease, or be unaffected.
- For those in the 'history' category, there is typically an increased likelihood of problems.
- Where a significant percentage of work is for one key customer, the consequence of any problems may be greater.

Wherever the likelihood or consequence of problems increases, this can be the trigger for more frequent or more intensive internal audits. Of course, the reverse also applies – where the perceived risk is minimal, you might consider reducing the frequency and/or scope of those audits.

In taking a risk-based approach to internal audits, you can turn what may currently be a 'necessary evil' into a very positive and cost-effective contribution to your business.



Internal Auditor Training

Qudos offers Internal Auditor Training courses for Quality and Integrated Management Systems – with sessions at customer premises, or at public sessions at our Brisbane CBD premises and other locations.

A key competitive advantage of this course is the provision of pre-course training material to each attendee on CD. This enables a basic understanding of quality systems and internal auditing to be gained **before** the class session. The course time is therefore reduced from a typical 2-day period to 1-day – saving cost and helping people to fit the training into their busy schedules. A JASANZ-accredited certification body has approved the course.

For more information on Qudos Internal Auditor training, visit:

<http://www.qudos-software.com/consult.html>

or call

(+61) 07 3010 9259

