OXEBRIDGE
QUALITY RESOURCES INTERNATIONAL LLC

Oxebridge Guidance Document Compendium

Ver.1

A full collection of the free Guidance Documents originally published on the Oxebridge website.

www.oxebridge.com

Introduction

Since 1999, Oxebridge has been offering free consulting, guidance and training, as well as *pro bono* assistance in resolving problems with registrars and accreditation bodies worldwide.

We've published dozens of free Guidance Documents on the Oxebridge website, but it was becoming unwieldy to find them easily. To make things easier, here is a compendium of all the best Oxebridge Guidance Documents, up to date for the latest ISO 9001:2015 and AS9100 Revision D standards.

Remember that in addition to this free Compendium, Oxebridge offers a totally free set of QMS template documents for both ISO 9001 and AS9100. We think template kits suck, but free template kits suck less. We urge you to approach such kits with caution, but if you want to try and save thousands of dollars by creating your own QMS, these kits are a great place to start.

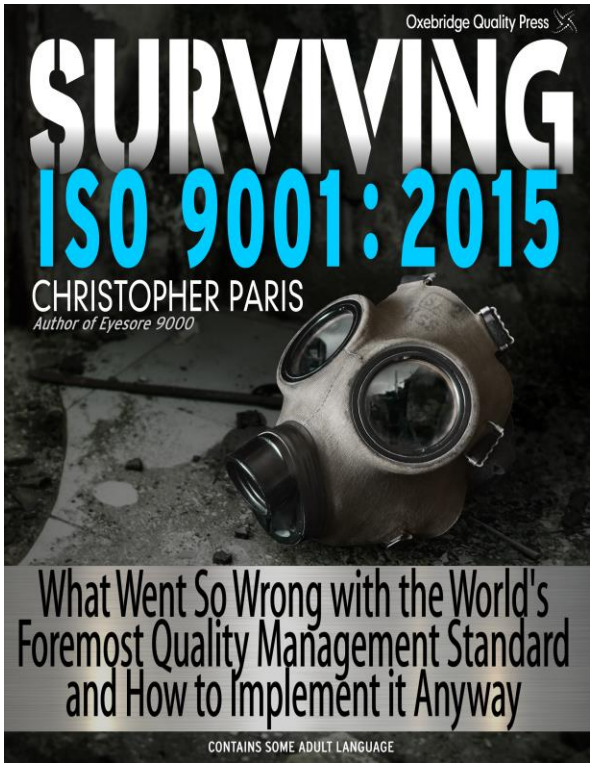
You can grab the ISO 9001 kit here, and the AS9100 kit here.

Surviving ISO 9001

Oxebridge VP and Founder Christopher Paris – the author of the Guidance Documents found herein – has written the first honest book on ISO 9001, ***Surviving ISO 9001:2015 – What Went So Wrong with the World's Foremost Quality Management Standard, and How to Implement It Anyway.***

Christopher Paris presents a fantastic, one-of-a-kind insight into how the latest version of the world's foremost quality management standard got so wildly off the rails, and then provides unique implementation guidance for those companies that find they have still to implement it, whether to meet a customer mandate or simply to keep their QMS up to date.

Surviving ISO 9001 features all the humor and hard-hitting satire of Eyesore 9000, and comes with an adult language warning for occasional "sixteen-letter, four-letter words," but despite the jokes, presents an incredible insight into how the standard was made, and how to interpret it for everyday use.



Broken into three sections, Part 1 discusses how the standard came to be, and reveals the political infighting and backbiting that resulted what many see as ISO's worst standard ever. Part 2 discusses step-by-step how to implement ISO 9001, using proven, real-world examples and advice. Part 3 then provides a handy checklist that puts the implementation steps in an easier order than if you follow the ISO 9001 clause sequence itself.

You can purchase the Surviving ISO 9001:2015 e-book by visiting ***http://www.survivingiso9001.com***.

Table of Contents

The articles included in the Compendium are presented in no particular order.

Implementing the ISO 9001:2015 "Process Approach"

The "process approach" to QMS management has been around since the 2000 edition of ISO 9001, but it's confused everyone to no end. Making matters worse, the new ISO 9001:2015 standard rewrote the language surrounding the requirements, making it ***less*** clear, rather than clarifying it. As I've argued elsewhere, this is because the authors of the new version were comprised of mostly private consultants who have since tried to make a fortune on deciphering the garbled text they created.

So it behooves us to revisit the process approach or, for new users, take a look at how it can be implemented for the first time.

Inconsistent Usage of Terms

First, understand that the ISO 9001 authors did not include actual process engineers. Again, they were mostly private consultants and registrar representatives, with no background in actual process design or process management. Then, ISO fails to employ a "final edit authority" in its standards development, to ensure that language and terms are used consistently throughout a given document. This is why through the first half of clause 8.5 the authors used the words "product or services" and in the second half, they used the word "output"; different authors wrote the two halves, and ISO didn't enforce a final editor to clean up the disparity.

This is also why the word "process" is used willy-nilly in the standard, without concern for the confusion or impact. For example, in clause 9.2.2 bullet point (a) the standard calls internal auditing a "program," and just two sentences later, bullet point (c) it refers to it as a "process." Then, in bullet point (f), it's back to a "program" again. An editor would have caught this, but ISO can't be bothered with things like editing when it has money to make by rushing things to print.

Next, some of the usages of the word "process" within the text ***contradict*** other areas of the very same standard. For example, clause 8.3 demands you implement "design ***processes***," apparently demanding there be more than one process related to design. This violates clause 4.4.1 which says, "*the **organization** shall determine the processes needed for the quality management system*" — so the organization (you) decide what processes exist for your QMS, not anyone else. The ISO 9001 standard cannot dictate your QMS processes, and yet the text of some sections appears to do just that. Neither can ISO 9001 tell you to split a process into multiple processes (plural) if you don't want to, but that's exactly what 8.3 is doing.

So you have to ignore any instance of the word "process" ***except*** in clause 4.4, where the "process approach" requirements reside. Don't let the other text confuse you.

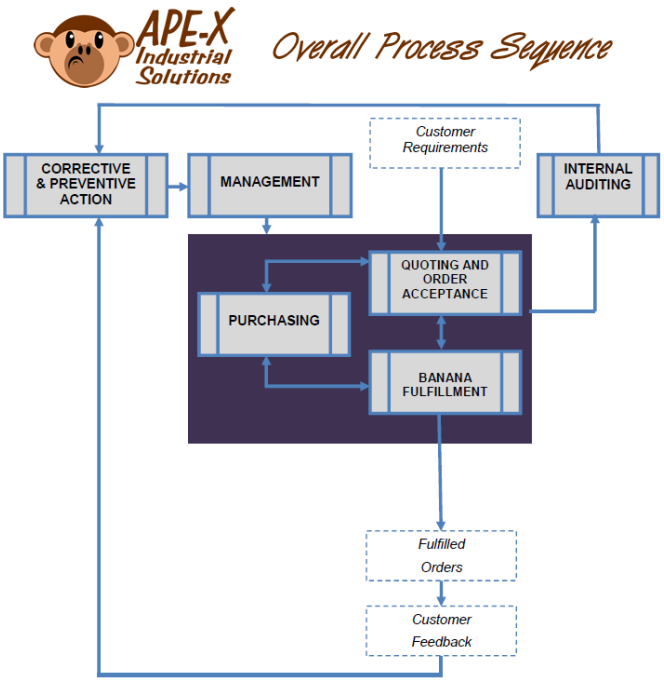
Identifying Your QMS Processes

Ignoring ISO's ever-changing definition of the word "process" (trust me, ignore it), understand that a process is an activity that converts inputs into outputs. Every human activity is a process: eating, breathing, walking, etc. This also means that everything — everything! — your company does is a process: from answering phones to sorting files to manufacturing airplane parts to serving lunch to the employees. Which makes things insanely difficult to manage, obviously.

Knowing that the process approach is defined in clause 4.4, you thus only want to use the word "process" when defining an activity you intend to manage under the requirements defined in bullet points 4.4.1 (a) through (h). Anything you ***don't*** want to manage under those rules, well, call them something else: "activity," "workstep," "operation," "sub-process" — make up a word if you have to. Just ensure that even if ISO 9001 is confused about how to use the word, in your QMS (including the documentation) ***you only use the word to describe activities you intend to manage per 4.4.*** And remember, the second sentence of 4.4.1 gives you this right: "*the **organization** shall determine the processes needed for the quality management system.*"

So what are those requirements? They're not particularly complicated to understand, but ISO jumbled them up sequentially, making it confusing. So we can better understand them if we look at them logically, rather than in exact sequence:

- ***"b) Determine the sequence and interaction of these processes."*** Here you have to develop an overall process flow, typically presented as a diagram or flow chart, of the sequence of the processes. For example, "Order Intake" usually precedes "Shipping." The typical approach here is to make a single "overall process flow chart" that shows this flow, and shove it in the quality manual somewhere. An example of such a flow diagram appears below, or can be found here. If you have a small to medium company, this might seem blindingly simple, and that's normal.



- ***"a) Determine the inputs required and the outputs expected from these processes."*** Next, start to define each individual process you've selected by identifying what its inputs are (required information, personnel, equipment, materials, etc.) and then what their final output should be (finished product, completed service, etc.) People use Turtle Diagrams for this, which I have written are entirely stupid, but if you like them, go for it. I use a "Process Definition" approach which eschews dumb graphics for a more thoughtful text-based description, and you can find a

sample here. This also captures some of the information required for the other bullet points herein.

- ***"d) Determine the resources needed for these processes and ensure their availability."*** Now define — perhaps in that Process Definition — what personnel, equipment and facilities are needed for the process.
- ***"e) Assign the responsibilities and authorities for these processes."*** Now define — perhaps (again) in the Process Definition — who is responsible for not only "owning" the process, but carrying out its related activities.
- ***"c) Determine and apply the criteria and methods (including monitoring, measurements and related performance indicators) needed to ensure the effective operation and control of these processes."*** Here is where things get tricky. You must develop process measurements — some call these KPIs (key performance indicators) — for each of your identified processes. I discuss this further in this article, below.
- ***"g) Evaluate these processes and implement any changes needed to ensure that these processes achieve their intended results."*** Now that you've established the measurements, start actually measuring them, and report the data to management; typically this is done in real time, daily, and then re-examined more formally during your regular management review per clause 9.3.
- ***"f) Address the risks and opportunities as determined in accordance with the requirements of 6.1."*** The analysis of the measurement data will likely highlight problems, which can be converted into risks which you then analyze per 6.1. Likewise, the data may identify opportunities. But you should also conduct a per-process review of possible risks and opportunities prior to, or outside of, any process measurement data collection. See my series of articles on "*Practical Implementation of Risk-Based Thinking*" available here.
- ***"h) Improve the processes and the quality management system."*** Finally, use the data and your corrective action system to improve the processes when they don't meet process objectives, or any other time you want to improve them.

So as we can see, that's a lot to do, and you wouldn't want to do all that for an activity as mundane as "shredding files" — unless, of course, your company offers professional file shredding services, in which case that might be your primary process! So every company will be different. My experience tells me most small to medium sized companies (1000 employees or less) have under a dozen activities they label as core QMS processes. For example, a typical small manufacturing shop usually has the following processes:

- Quoting & order entry
- Purchasing & receiving
- Manufacturing (including QA)
- Packaging

- Shipping

Depending on your company's size and complexity, you may separate these further. For example, some companies separate Purchasing and Receiving into two processes, while other smaller companies keep them together as one. Others putting Shipping and Receiving together. Often, companies won't have a single "Manufacturing" process, but instead a handful of individual manufacturing processes, such as "cleaning," "milling," "sawing," etc. Again, that depends on their size and complexity, and what they want to measure. If measuring "manufacturing" as a process isn't useful, because it's too vague, then you would label the individual activities as processes, and measure those.

Often, the processes will align to some degree to company departments, but you shouldn't use departments as the sole guide when dividing your company into processes.

You're also going to add a few administrative processes, which I will discuss shortly.

Assign ISO 9001 Clauses

It's not in the ISO 9001 standard itself, but to properly implement a process-based QMS which, itself, must comply with ISO 9001, you should ensure that your set of processes also encompasses all the ISO 9001 clauses. This will make sense in a minute, but for now trust me; make a table of each of your processes and assign the ISO 9001 clauses that are applicable to that process, until all the clauses are assigned somewhere. For example, a "Purchasing" process would be assigned clause 8.4, and your "Design" process would be assigned clause 8.3.

What you will find is that a lot of the ISO 9001 clauses other than those in 8 don't fit anywhere. This is why you have to develop a few additional QMS oversight processes. These will then cover clauses 4, 5, 6, 7, 9 and 10 which are typically not covered by your product or service related processes.

I usually suggest a single "QMS Administration" process which covers all of management activities for clauses 4, 5 and 7. Then a "Resources" process to cover clause 7, and an "Improvement" process to cover 9 & 10. Some companies keep Internal Auditing as a separate process, which makes auditing easier (more on that coming up), and others with huge documentation libraries and complex configuration management activities may break out "Document Control" into a standalone process. It's entirely up to you, but I urge companies to keep their top-level processes to a minimum, because it can get out of hand quickly. Again, even with a few QMS management related processes added, most companies have a set of about a dozen processes when done.

Again, each of these QMS management processes would need be measured, too. To measure the "Resources" process, for example, you might measure employee turnaround, or equipment downtime, etc. To measure the "QMS Administration" process, you might measure overall compliance to ISO 9001, or how effective all the other processes are; after all, if the other processes are ineffective, then it's likely a management issue.

In such a case, the process list from the example I made above might grow a bit, to look like this when done:

- QMS Administration
- Improvement

- Internal Auditing
- Quoting & order entry
- Purchasing & receiving
- Manufacturing (including QA)
- Packaging
- Shipping

Here is an example of what your process listing vs. ISO 9001 clauses might look like for a company that conducts both design and field service, alongside manufacturing (click here for a PDF version.)

Process	Applicable ISO 9001:2015 Clauses
Management System Administration	4.0 Context of the Organization (all)
	5.0 Leadership (all)
	6.0 Planning (all)
	7.0 Support (all)
	8.1 Operational planning and control
	9.0 Performance evaluation
	10.0 Improvement
Business Development and Sales	8.2 Requirements for products and services
Engineering	8.3 Design and development of products and services
Procurement	8.4 Control of externally provided processes, products and services
Production	8.5 Production and service provision
	8.6 Release of products and services
	8.7 Control of nonconforming outputs
Field Service	8.5 Production and service provision
	8.6 Release of products and services
	8.7 Control of nonconforming outputs

Process Objectives

Recall that clause 4.4.1 bullet point (c) requires you to "*determine and apply the criteria and methods (including monitoring, measurements and related performance indicators) needed to ensure the effective operation and control of these processes."* This means each process should have at least one measurement.

The clause on quality objectives (now residing in 6.2 of the latest standard) is just an update of original language that has existed since the 1987 initial release, and has never been properly aligned with the process approach; this was a pretty significant error made in the 2000 version, which was never corrected in any version since; again, this is because there are no actual process engineers in the ranks

of the ISO 9001 authors. But process engineers understand that each process has objectives, and these are almost always redundant — or much better — than simple "quality objectives."

"Quality objectives" in the oldest sense meant simple things like scrap rates, yield, on-time delivery, etc. (AS9100 still adheres to this thinking, in fact.) But under a true process-based QMS, such objectives are meaningless because they don't tell you where problems with scrap rates, yields or OTD come from; by this I mean which process ***caused*** the problem. Without knowing that, the data is meaningless since it makes it difficult to know where (which process) to apply corrective action.

So I recommend combining the concept of "quality objectives" from clause 6.2 with the "process performance indicators" required by 4.4.1. To do this, you assign at least one objective/metric pairing to each process, and ensure these include metrics suitable for measuring product or service conformity. I take an unconventional interpretation here, as follows:

- "**Objective**" should be a prose (text) description of what the process intends to achieve. Each process must have at least one such objective, but may have more than one. For example, the objectives of a "Purchasing" process may be "*to ensure high quality raw materials are used*" and "*to ensure excellent performance by our selected suppliers*." These are simple statements of the obvious.
- "**Metric**" is the means of measuring each objective statement; some objectives may have multiple metrics. For example, the Purchasing objective of "*to ensure excellent performance by our selected suppliers"* (from above) may have two metrics: measurement of supplier on-time delivery, and measurement of quality acceptance of received raw materials.
- "**Goal**" or "**target**" is then the actual measurement you want to achieve for each metric. For example, your goal for supplier on-time delivery may be "*95% on time delivery for all items received in the last 6 months*." Always make sure you have a time period included in the goal, unless it's a running total. Goals are set by top management.

Again, each process must have at least one objective; each objective must have at least one metric (sometimes more) and each metric must have a goal, set by management. You will find that your traditional quality objectives, such as yield, scrap rate, etc., "fit" somewhere into the process objectives, probably for your manufacturing-related processes. Now, when you have a poor yield, you know which process is likely responsible, and thus where to apply corrective action.

I suggest making a table of the entire thing, that looks like this:

Top-Level Process	Quality Objective(s)	Metric(s) / KPIs	Current Standing	Goal/Target	Goal Met? (Y/N)

Obviously, you will fill this in accordingly, leaving the columns “current standing” and “goal met?” blank — those are used later, during management review.

Process Auditing

Finally, if you like (it’s optional) you can audit by processes. Despite common belief, there’s no such thing as process-based auditing, and anyone telling you otherwise just made it up. It’s not defined in the auditing standard, ISO 19011, not mentioned anywhere in the registrar accreditation rules, and there’s no consensus on what it actually means. That hasn’t stopped a host of consultants and auditors from telling you it’s mandatory, and then giving their ideas (or selling their books and seminars) on how to conduct process-based audits anyway. They also invent a false dichotomy, saying that process auditing is the opposite of clause-based auditing, which is also utterly untrue. In fact, ISO 9001 clause 9.2 requires you to audit the ***clauses***, (“*the requirements of this international standard*“) and not the QMS processes, so when someone tells you otherwise, you know they have no idea what they’re talking about.

Having said that, conducting internal audits by processes is a ***good idea***, as it makes audits more manageable, and then results in audits that can highlight process inefficiencies or problems. But, as I said, you still have to audit the clauses in some fashion. If you make audit checklists based on the processes, and include only questions related to the ISO 9001 clauses you identified for that specific process (as above), then you’re on your way. There are additional things you should do beyond ***just***checklist auditing, but that’s out of scope for this article.

But this is also why you want to have some processes dedicated to the QMS administrative clauses, like 4 and 5, to ensure they get audited, and that they are measured as part of your processes. It is also why some companies elect to have “Internal Auditing” as a standalone process, since you have to audit your internal audits (yes, really), and having them separate makes that activity easier, since you can assign the “process audit of the Internal Audit process” to someone objective, who wasn’t involved in all the ***other*** process audits. Makes sense!

Risk & Opportunity

I've indicated you should read my article series on Practical Implementation of Risk-Based Thinking, so I won't reiterate it here, only to say that as part of your day-to-day work, you should be identifying risks and opportunities not only related to products or contracts or customers, etc., but also related to your top-level processes. If you use my COTO Log, then that covers you here, too.

Management Review of Process Effectiveness

Finally, you will assess the performance of each process, based on its objectives and measurements, in real time as needed. But you must then report this to management during your periodic management review; ISO 9001 clause 9.3.2 bullet (c)(3) says that the review must include "process performance," and this satisfies that.

Prior to any management review activity, I recommend alerting the process owners to submit their most recent process objectives data, so that the table I presented above can be filled in with the "current standing." For example, if your Purchasing objective's goal is "*95% on time delivery for all items received in the last 6 months,"* then you indicate what is the actual data showing ***right now***, which may be "*98% OTD by suppliers in the last six months*" or it might be something terrible like "*25% OTD by suppliers in the last 6 months*."

Then, during management review, have the process owners present their data to top management, and if the goals are not met, then management may elect to either change the goal or request corrective action. Whatever happens, if a goal is not met, something ***must*** be done, and this should be captured in the records of management review.

Likewise, you will report on the internal audit results, by processes. In fact, the entire management review should be structured around an analysis of each process (its objectives/performance, internal audit results, resource needs, staffing levels, etc.) When done, your top management will know which processes are operating effectively, which are not, and thus be able to make informed decisions aimed at correcting or improving some processes, while leaving the high-performing processes alone to carry on.

Conclusion

Remember that a quality management system is just that: a ***system***; and a "system" is a set of processes. The system cannot operate well if one or more of the major processes is stumbling. By adopting a truly robust process approach to the QMS, this enables management to manage by processes, which simultaneously captures the performance against ISO 9001 clauses and other requirements.

Last tip: our totally free ISO 9001 QMS Documentation template kit is still available, constantly updated, and includes sample documentation based on the process approach methods defined herein. Like I said, it's totally free, so click here to download it (or click here for the AS91900 version.)

I also urge you to consider buying my, umm… "controversial" book on this whole thing, called ***Surviving ISO 9001: What Went So Wrong With The World's Foremost Quality Management Standard, and How to Implement It Anyway.*** This is the only book on ISO 9001 that goes behind the scenes to detail the

politics, backstabbing and skulduggery that caused the latest version of ISO 9001 to be so terrible, but then provides proven, real world guidance on how to implement each clause. You can grab it by visiting www.survivingiso9001.com. (Adult language is used, so fair warning; as I said, the new standard is pretty terrible, and it deserves a few f-bombs.)

Practical Implementation of "Risk Based Thinking" – Part 1

The COTO Exercise

I've made it clear I am no fan of the vague, peyote-sourced "risk based thinking" (RBT) language that TC 176 added to ISO 9001:2015, nor its clearly non-consensual "include risk or else" origins from a mandate by overcaffeinated ISO executives. The thing is, we're stuck with it, and no amount of garment rending will undo it. I know, since I've rended all my garments, and am typing this naked.

Moving past *that* mental image (you're welcome), if we *must* adopt RBT then it behooves us to figure out just how to do it in the best practical way possible, without falling into one of two traps:

1. We don't want to let the vague language of RBT in ISO 9001 translate into doing ***nothing***
2. We don't want to let the growing chorus of ill-informed CB auditors have us ***overdo*** it, and apply FMEA to everything

Instead, the text of ISO 9001 tells us that it's entirely up to the ***company*** to decide what level of risk consideration to adopt. And that's great. But before we can do that, we have to tackle an entirely different clause of ISO 9001:2015 first, and it's also new. This is the clause related to "context of the organization" (which I'm calling "COTO", an abbreviation I am shoving the Oxebridge flag in so years later you know who invented it.) Anyone jumping into the risk clause without tackling COTO has missed an important step. This also proves how those FMEA-addicted auditors have no clue what they are talking about, since COTO will drive the decisions on which risk treatment methods to select.

COTO en Toto

Why COTO first? If we look at the first requirement in clause 6.1.1 related to risk, we find it pushes us back to COTO:

> *"When planning for the quality management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2…"*

What this means is that prior to doing any work on the RBT requirement, you have to first conduct what I call the "COTO exercise." This is an activity that will take a little bit of time the first time, and then just gets updated periodically (perhaps annually) later on. So, just to repeat myself and see if my blog can still handle red bold italics, let me reiterate:

You cannot address risk-based thinking properly without considering the context of the organization first.

Fortunately, the COTO exercise is simple. This requires identification of four things:

1. Identify your interested parties – who they are and what are their requirements and expectations
2. Identify internal and external issues – based on # 1 above
3. Define the scope of the QMS – based on # 1 and # 2 above
4. Identify your processes within the QMS

Now a strict reading of the COTO clauses (4.1 through 4.4 of 9001:2015) has them in a different sequence. This is because TC 176 is dumb; they would have you identify the external issues first, and then identify the external stakeholders — which in the exact opposite of the way you would do this in real life. So I've re-ordered the steps, ignoring 9001:2015's clause sequence.

Fight For Your Right to Party

Following these steps, you have to first identify stakeholders ("interested parties") who either have an interest in your products or an interest in your quality system. This is a great addition to ISO 9001, the previous versions of which obsessed almost entirely with customers, but ignored almost anyone else who might care about your products of services. For example, many B2B companies sell products to another company, but the end user may actually be the public; under 9001:2015 we get to consider the end users, and not just the paying customer.

I recommend creating a simple table and then populating it, with the help of the senior management team and other company propellorheads. The table should look like this:

Interested Party	Internal or External	Reason for Interest

You will then think of all the groups of people who may be directly or indirectly impacted by your product or service, as well as those that have a direct or indirect impact on your QMS. For each identify whether they are internal (work for the company) or external (third parties.) Then define why those groups might have an interest.

Like much of ISO 9001, ***you get to decide who an interested party is***. The only expected party would be your customers, and everything beyond that is entirely up to you.In most cases, however, this is going to include:

Internal Interested Parties

- Employees
- Other divisions of the company
- Departments that may be outside of the QMS (legal, finance, etc.)

External Interested Parties

- Customers
- Suppliers / Vendors

- Regulators
- The public
- Other end users of your product/service
- Certification bodies
- Competitors

Doing so, your list might start to look like this:

Interested Party	Internal or External	Reason for Interest
Customers	External	Direct recipient of our products.
Employees	Internal	Responsible for realization of our products.
End users	External	Our products may be resold by our direct customers to other end users, who are directly impacted by the quality of our products.
Suppliers	External	Provide supporting services or raw materials
Regulators	External	Dictate controlling regulations that impact on the management system and our products.
Public	External	While a low risk, failure of our products could impact on public safety.
Certification Bodies	External	Assess conformity of the company against ISO 9001 and so must be kept notified of changes to the QMS.
Competitors	External	Provide challenges to our ability to provide products to customers.

Once you have your interested parties identified, you can start to think about what each of those cares about, which brings us to the next step in the COTO exercise.

We've All Got Issues

Using the list above, you will then identify internal and external "issues." These are concerns that the interested parties may have that directly or indirectly impact on your products, services and/or QMS. Again, a simple table is a great way to start:

Internal or External	Type	Issue	Bias

(By the way, you can create a single spreadsheet that includes all of this in a sortable file. I'm just proposing these tables because it's easier to discuss in a blog article.)

You would then begin the mental exercise of identifying the issues of concern. The good news is that ISO 9001:2015 gives us some pointers on where to start. The Notes in clause 4.1 provide the following suggestions:

Internal Issues

- values
- culture
- knowledge
- performance

External Issues

- legal
- technological
- competitive
- market
- cultural
- social
- economic

Once again, these are optional… ***you*** decide the issues of concern, not anyone else. Just try to imagine, however, what your interested parties might consider an issue of concern.

When you're done, your table might start to look like this:

Internal or External	Type	Issue	Bias
Internal	Technological	The company currently has adequate technological resources to consistently produce its products	Positive
Internal	Employee base	Availability of skilled workforce in the area remains high	Positive
Internal	Employee base	Employee turnover is low	Positive
External	Supply Chain	Quality issues pertaining to raw materials or critical services may not be addressed properly when using sole source or limited-source suppliers	Negative
External	Competition	The company does not have significant competition in this market at this time.	Positive
External	Society & Culture	Our products do not present any particularly controversies that would result in negative reactions from society or the public.	Neutral

So why did I add a column for "bias?" After all, that's not mentioned at all in the standard. The answer is simple: this will help you identify risks and opportunities later, as part of the risk-based thinking (RBT) exercise. So remember that point, because we will come back to it later.

Scope, Processes & Strategic Direction

The next two requirements for COTO are two that you've probably already done, if you had implemented ISO 9001 prior to the 2015 release. These are (1) defining the scope of the QMS, and then (2) defining the QMS processes. If you haven't done this before, well, they are not terribly complicated exercises, but far beyond the scope of this article. If you've identified interested parties and issues of concern, you have enough to begin taking a bite out of risk-based thinking. Your QMS scope and QMS processes will help in this regard.

From all of this information — stakeholders, issues, scope and processes — you now can do a few things. One of these will be to define the "strategic direction" of the company (see new clause 5.1.1 as well as a few others). This is also out of scope for this article, but if already done would further assist in the RBT exercise; if the company hasn't yet defined its strategic direction, don't worry: it's not a showstopper for RBT.

But relative to RBT, the COTO information will allow you to make informed decisions on the risks to consider in your organization, the risk tools to use for assessment of each, and the risk treatment methods.

Practical Implementation of "Risk Based Thinking" – Part 2

Defining Risk and Opportunity

From the information you have derived from the COTO exercise, you now have a better understanding of the company, it's stakeholders, internal and external issues of concern, and other factors which will build the framework for your thinking about risk.

You will also realize that because the information derived from the COTO exercise will be different for every company, the risks will also be different for every company. This means ***no auditor can tell you what your risks are.*** (Of course they are going to anyway, but you have to push back.) ***You*** decide which risks are going to be managed… no one else. This is explicitly hard-coded into the standard, which says:

> *"6.1.1 When planning for the quality management system, the **organization** shall … determine the risks and opportunities that need to be addressed."*

In the AS9100 scheme, which has had requirements for risk management since 2009, we have seen auditors come on site and try to dream up risks during the audit, and then play "gotcha" with the client. Despite being presented with formal risk registers, they will stroke their chin and muse on things you've missed: "well, did you think of whether or not a meteor will strike your HR manager on her way to work?" or "did you assess the risk of a zombie apocalypse?" Now, under 9001:2015, you get to tell them to STFU and look at the risks you've addressed, to stop auditing by fantasy, and for God's sake, stop stroking their chin.

Re-Defining Risk and Opportunity

So the next step is to "determine" your risks. Unfortunately, we have another slight speedbump: ISO has completely mucked up traditional concepts of risk. The reasons for this are complicated and political, and not at all universally agreed-upon. There are two camps: one that thinks "risk" is neutral, and thus can be either negative or positive (thus defying the dictionary) and the other that believes risk is solely negative. The "positive risk" crowd has won over the ISO Technical Management Board and the authors of ISO 31000 on risk management, but did not win over TC 176. In fact, the "positive risk" debate is one of the main sticking points for ISO 9001 ratification across the world.

Why does this matter? Wouldn't it be nice to let ISO have their fight and watch from the sidelines? Well, this has a real-word impact on you right now. You see, normally you work to mitigate risk — meaning ***minimize*** it — because it's bad. If you suddenly treat risk as "positive" then you would want to ***maximize*** the possibility of the risk, right? But you can't use the same tools to both minimize and maximize something at the same time. SWOT comes close, but other traditional tools like FMEA focus only on reducing risk, understanding that risk is inherently bad. Other tools might work to maximize opportunities (such as expanding business development leads) but these wouldn't work for reducing negative risk.

The Silver Lining Theory

The "positive risk" camp tends to defend its view using what I have dubbed the "Silver Lining Theory" — this is where they paint risk as being positive only because there may be an accidental benefit of an otherwise disastrous thing. The example I often hear is the "hurricane" scenario: a hurricane is a bad

thing because it causes damage. The "Silver Lining" crowd says that a hurricane is also positive, since the destruction it leaves behind becomes an opportunity for those in the construction industry.

The reason the Silver Lining Theory fails is when you try to apply it in a practical way. Remember, for negative risk we work to minimize the likelihood and severity; so companies must reduce the risks associated with hurricane damage by having business continuity plans in place, escape routes, shelters, data backups. etc.

Remember too that positive opportunities must be managed to increase their likelihood and maximize the benefits. However, those in the construction industry cannot increase the likelihood of a hurricane, and cannot maximize the damage (which to them is a benefit) unless they hire hordes of looters to tear the city apart, which they can rebuild later. Not a great business plan.

The best a construction company can do is plan to have additional resources ready (reconstruction teams, hardware, etc.) in the event there is damage they can repair. But that's not the same as risk management since mere planning does not increase either likelihood or severity. And, in fact, they may expend money to have those resources ready and it be all for naught, if the hurricane doesn't make landfall at all. In which case, they've created a problem (now they're broke) and not achieved any opportunity. Not to mention they need to do all of this while mitigating their own exposure to the damage of the hurricane, like making sure the people they have on standby don't get killed themselves. None of this magically turns a hurricane into a good thing; it just tries to examine the "silver lining" behind an overwhelmingly bad thing.

(The most ghoulish explanation I've heard is related to cancer. A few "positive risk" advocates claim that cancer is good because it creates jobs. They ignore the fact that those jobs are seeking to eradicate cancer, an admission that cancer researchers never view cancer as an "opportunity" but as a risk that must be eliminated.)

A "pure" positive opportunity exists, first and foremost, as an opportunity; it is not an accidental positive side effect of a bad thing, it is inherently good to start with. For example, a positive opportunity might be that the government puts a $5 Billion contract out for bid, and it's something your company is qualified in. Another opportunity might be you find $100 on the street, or prices drop on a critical raw material, or that nerdy engineer who works in the lab and smells like tuna fish accidentally invented antigravity. All these things are positive first; they may have hidden negatives (a "tarnished silver lining" if you will) but they are primarily opportunities. You work to exploit them, not run from them.

The Uncertainty Battery

So what you have is the reality that ***uncertainty is neutral***, while "risk" and "opportunity" are the negative and positive aspects of uncertainty. If you imagine a battery is, itself, neutral and only the poles have a charge, then you begin to understand the true nature of uncertainty:

So the Oxebridge view is that ***uncertainty*** is neutral; risk is the ***negative effect of uncertainty***, and opportunity is the ***positive effect of uncertainty***. This interpretation has the benefit of (a) complying with English dictionaries and (b) actually making sense. I strongly suggest you adopt this view to proceed, but if you do, you may need to indicate this in your QMS documentation somewhere. Auditors may come in and disagree, depending on which ISO school of thought they were trained in, but ***you*** get to define concepts for your QMS, not them.

The ISO 9000 Problem

An aside: some will say that ISO 9001 calls out the definitions in ISO 9000 as a "normative reference" which thus makes the definition of "risk" from ISO 9000 a mandatory requirement. This is not true, and you must be ready to defend yourself against this argument as well. Here are the talking points for your defense:

- ISO 9000's definition is not universally adopted within ISO itself, which has 40 different and often contradictory definitions of the term "risk".
- ISO 9000's definition of "risk" has been viewed as controversial and may be changed or revoked, and you don't want to hold your QMS hostage to something that could change easily.
- ISO 9000's definition of risk is impossible to implement in a practical way, since negative risks must be managed differently than positive opportunities, so the definition needed "tailoring".
- The tailored definition doesn't inherently contradict ISO 9000's definition anyway, they merely provide greater context.

As we will see, having this definition in place will become necessary to continue.

Practical Implementation of "Risk Based Thinking" – Part 3

RBT in Practice

To recap, so far we've conducted a COTO (context of the organisation) exercise which helped us better understand our company, its stakeholders and the things they may find important. We then tailored our understanding of the concepts of "risk" and "opportunity" to something that makes practical sense. Finally, we will use this information to determine the risks facing the company and how to manage them.

One important thing to consider: the ISO 9001:2015 standard specifically uses the phrase "determine" your risks. Many CB auditors and pundits have already misinterpreted this as saying you must "document" or "record" them; but "determining" is not equal to "documenting", so they are wrong. If TC 176 had wanted you to document them, they would have said so; instead they did include the word "thinking" however, so in the strictest sense you can "determine" your risks merely by thinking about them. Yes, it's insane, but it's literally true.

What does this mean in a practical sense? This means ***you*** also get to decide how to "determine" the risks. This article just presents one possible way, and it doesn't pretend to be the ***only*** way.

Converting Issues to Risks and Opportunities

Risks are everywhere, and naming every one of them is like naming all the stars in the sky. So what risks do you consider? The standard does give some pointers, thankfully. Clause 6.1.1 says you must "*determine the risks and opportunities that need to be addressed to:*

- *give assurance that the quality management system can achieve its intended result(s);*
- *enhance desirable effects;*
- *prevent, or reduce, undesired effects;*
- *achieve improvement*

But those are vague concepts in and of themselves, so they are only hints. You are going to have to take those hints, run them through the filters of the COTO exercise outputs, and come up with actual risks you can take a bite out of.

I like tables, so I am going to recommend another table; I call this an "Issues Log." It may look like a traditional risk register, but it's not, at least not yet; if you elect to create a risk registry later, you can cut and paste data from this table into it. You can download a free, customizable version of this table (MS Excel 2013 format) here.

Line #	Interested Party	Int / Ext	Issue of Concern	Bias	Processes Affected	Prioritiy	Treatment Method	Record Reference
1								
2								
3								
4								
5								
6								
7								

Using this table, you will copy the information from your previous exercises into it. The Excel version provides drop-down lists for most of the columns to make filling it in a bit faster. A few explanations:

"Bias" refers to whether the issue is inherently negative (a risk) or positive (an opportunity.) Now you see why re-defining "risk" (as we discussed in Part 2) is important.

"Processes Affected" refers to the key (core processes in your organization which you should have already identified. The RBT activities should become part of your process approach, so tying each issue to at least one related process is important.

"Priority" allows you to prioritize the issues; this might then carry over into any prioritization used in the risk treatment itself.

"Treatment Method" would be a reference to the preferred method used to process the issue. For many negative risks you may opt for FMEA, but for others you would not. The Excel file provides a drop-down list of about 30 different risk treatment methods, from ISO 31010 *Risk Management – Risk Assessment Techniques;* you can likewise add your own.

"Record Reference" would be where you indicate the associated records or files related to the risk treatment; this could be a CAR number, a FMEA reference number, a report number… whatever. But the Issues Log should link to where the user can find more information.

To fill this out, you go down your COTO tables and copy the data into this new Issues Log. Once you are done, you can then add additional risks and opportunities that you think of outside of the COTO exercise. In fact, I recommend you hold a special management-level meeting to help populate this Issues Log.

Once it's complete — and keep in mind, this is a living document that will be updated as conditions change — you can then use this to drive a number of ISO 9001 related activities:

- Use the information to update the company's Strategic Direction
- Use the information to update the internal audit schedule
- Use in Management Review as an overall risk thinking tool
- Use to populate a formal risk registry

You may wish to upload this to a central server so that employees can add to it as they like; this encourages participation by your staff in the risk thinking activities.

On its own, however, the Issues Log doesn't fully meet all the requirements of RBT. Instead, it has helped you "determine" the risks and opportunities as required by ISO 9001:2015.

Risk Based Vaporware

Once you've identified your risks, ISO 9001 then goes on to require the following:

> *6.1.2 The organization shall plan:*
> *a) actions to address these risks and opportunities;*

> *b) how to: integrate and implement the actions into its quality management system processes [and] evaluate the effectiveness of these actions.*

The first in that list (take "actions to address" the risks) is ISO's way of saying you need to conduct some form of assessment and treatment; but ISO didn't want to use those words, lest they be seen as prescriptive. Formal risk assessment and risk treatment is not required, but you have to do ***something***.

This is where the 9001:2015 standard fails: it wants to have its users adopt risk management, but is so terrified (and ignorant) of formal risk management, it tries to avoid using the terms directly. (There were also a lot of politics in play, and TC 176 didn't want to step on the toes of TC 262 on risk management, the guys who publish ISO 31000.) The end result is a vague set of words that actually mean nothing, and provide no direction whatsoever on how to meet the requirement. I call this a "required non-requirement" in that it requires something, but says nothing.

So, in a practical sense, you have to do some "action" that — for the purposes of this article, anyway — we will call "risk assessment" and "risk treatment." But these activities may not always look like the traditional assessments and treatments, and may not be applicable to all the risks or opportunities you identified.

Risk-Based Fortune Telling

I hate that I have to use the term "risk assessment" because ISO 9001 doesn't officially require this, but lacking any other term, it will have to do. As you will see, I am not suggesting the full gamut of formal risk assessment methods commonly used by risk management professionals. If you like, we can call it "risk evaluation" or "risk consideration." Maybe "risk divination." I don't care.

The dirty secret in the risk management profession is that it's all based on guesswork. Any risk assessment is just making guesses and then assigning numbers to make it look like science. It's closer to Tarot card reading than physics, but no risk manager will ever admit it.

So here's what we do, in the real world. Taking your Issues Log, you will determine the best risk treatment method for the given risk or opportunity and apply it.

- If the risk treatment is FMEA (or similar), then this method includes the risk assessment within the treatment. Run the FMEA and you're done.
- If the risk treatment method is something else, this may require two steps: first, evaluate (assess) the risk in some way and then determine the course of action to take. This may mean simply writing the evaluations and actions in a simple text document and filing it, or it may require more formal activities and records — you get to decide.

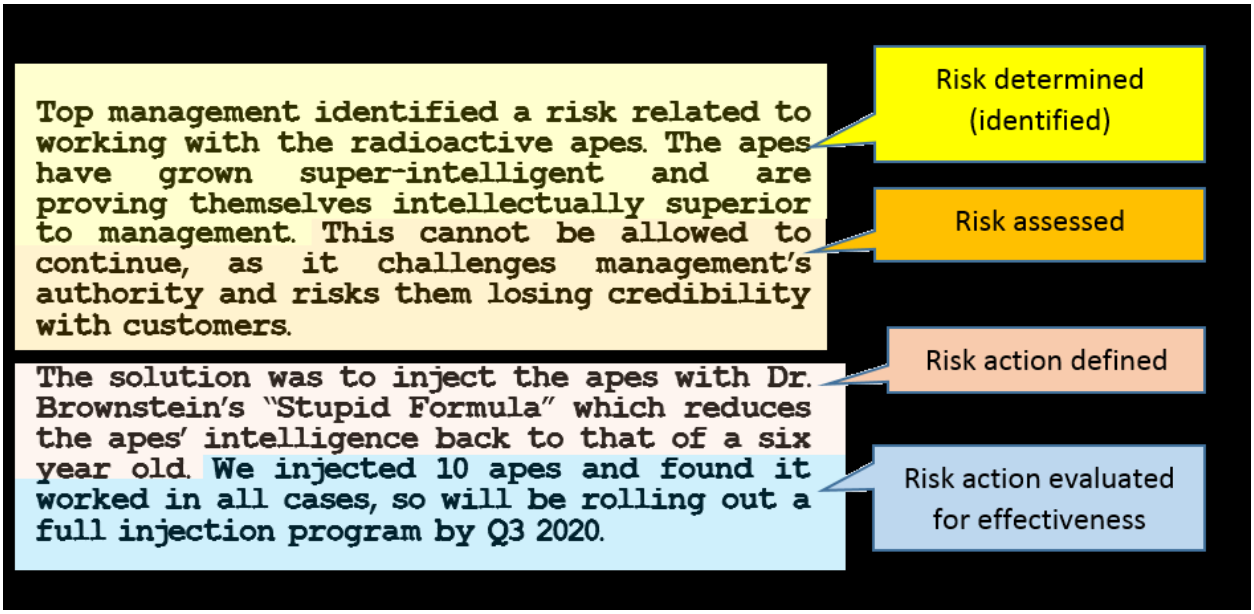
I'm no fan of FMEA when using it for every type of risk, but if you want something that is a bit more flexible, but which still looks like an FMEA, consider downloading this free Excel file. (Right click, and select "Save As.") This also acts as a risk registry of sorts (and that's what it's called.)

Whatever method you use, it has to comply with the next "required non-requirement" of ISO 9001, which says the you must

> *… integrate and implement the actions into its quality management system processes [and] evaluate the effectiveness of these actions.*

If you have used a traditional, formal tool (like the FMEA or any of the treatments listed in ISO 31010), your job is done; these tools effectively meet this requirement.

But if you've elected to use a nontraditional method, or simply are explaining your actions in a prose text file, then just be sure the text explains clearly (1) identifies the risk, (2) evaluates the risk, (3) defines a risk action and (4) evaluates the actions taken. Here's what that might look like in a simple typewritten example:



This meets all the requirements of ISO 9001:2015's risk-based thinking without using a single spreadsheet, complicated FMEA or any other traditional method, and can he upheld during audits if you clearly point out the four elements.

Managing Opportunities

Opportunities are the alleged positive side of risk, as we discussed. They are not managed to mitigate (minimize) them, but instead the opposite — you want to ***maximize*** the likelihood and impact of opportunities. Therefore while you can use all the same steps in RBT, when you reach the treatment step you will have to select different tools or approaches. Often the "prose" format is best, otherwise you will have to create a risk register that calculates opportunities in the ***opposite*** manner of risks, ranking them based on how well you can exploit the opportunity, as opposed to how well you can minimize the risk. Another great option for managing opportunities is SWOT, but it is not easy for the beginner.

Recap and Moving Forward

So, to recap, you use the COTO exercise to identify your stakeholders and their issues. You use this to help identify your risks and opportunities, and then collect them into some format to assess them. That assessment should include the determination of a risk treatment method specific to that risk, since no

one tool can be used in all cases. Then you take actions to reduce the risk, evaluate the actions, and keep a record of the whole thing to prove it later.

The flexibility of the vague language of ISO 9001:2015 can be used to your benefit, allowing you to do whatever you like to meet these requirements. But at the same time, this will cause headaches for CB auditors who are expecting to see the same thing from one client to another. Be prepared to defend your interpretations, definitions and approaches. While the standard doesn't officially require records of risk actions, you should maintain them for your own internal reference, but also to prove to the CB auditor that you've actually done something.

Like this topic? Book Christopher Paris for a speaking event at your organization on ***Practical Implementation of Risk-Based Thinking.*** *Click* here *for more details.*

How to Audit "Risk-Based Thinking"

The future of how certification bodies (CBs) will audit the new ISO 9001:2015 "risk based thinking" language is already setting, like a wet clay in the oven. In short, they are going to default to traditional risk management techniques and impose FMEA on their clients. It won't matter if you are making tanks for the military or muffins in a bakery, you are going to be doing FMEA because they auditor's don't know any other way. That contradicts what ISO 9001's authors intended, but it's what is going to happen.

But if the CBs are wrong, then what is the ***right*** way to audit something like RBT, which doesn't actually have any requirements? How do you audit "thinking"? Some have argued it's impossible, but it's not; it's just challenging. Let's take a look.

The Audit Process

First, let's understand what auditors are supposed to do. They are supposed to gather objective evidence to assess the conformity of a company against ISO 9001 requirements. That means there needs to be two inputs into the audit process: requirements and evidence.

Let's take that in reverse order and understand what "objective evidence" is. In short, objective evidence is evidence that is gathered independent of the auditor's opinions and biases, and which can be confirmed at a later date by any third party. For decades, auditors have been trained to believe that the only acceptable forms of evidence are documents and records. This is not true. Other forms of objective evidence include:

- Direct observation of work by multiple parties
- Direct observation of work by a single party (when a job is only performed by one person)
- Gathering of intellectual evidence (i.e., conversations)
- Sounds, smells, tactile evidence
- … and so on.

When auditing RBT it will be imperative for CB auditors to ***avoid*** the reliance on documents, records and procedures since the standard specifically does NOT require them. Auditors who demand to see such documentation because "I can't audit otherwise" should be shown the door. And I mean that in the Old Western saloon bar fight way.

So the second input is the requirement itself. For RBT, as I said, there are no firm requirements for documents, records, processes or resources. One need merely "think" about risk when crafting and managing a QMS. The idea behind this approach was to, according to one TC 176 representative, *"address risk according to the context of the organization":*

> *"Some organizations might be required to take a heavy, formal approach in order to provide the necessary level of confidence in their ability to provide consistent conforming product. In the automotive context, design and process FMEA would be expected, and possibly other risk-based things like sampling criteria etc. In the Food context we have HACCP; and so on. Clearly though, it wouldn't be appropriate for a small mom & pop store selling innocuous hardware products to*

have to go through a full FMEA. So we came up with the "risk-based thinking" phrase as a way of diluting the push for out-and-out risk management.

OK, that's simple enough. But what does ISO 9001 actually require? From this standpoint, the 9001:2015 DIS calls out the need to assess risks in the following areas:

- Determining the context of the organization
- Determining the processes needed for the QMS
- Risks associated with assuring product or service conformity
- Post-delivery risks

There's also a general theme running that risks should be considered throughout the QMS regardless of whether it's specifically called out in a clause or not. It appears, then, that we have very loose, vague language defining how RBT is to be implemented, and (again) that's by TC 176's design. The intent was for the ***company*** to determine the level of rigor to be used.

So that leaves us with the need to find "hard" evidence of a "soft" intangible. Impossible? Only if you are one of those badly trained auditors who probably should have retired 10 years ago.

The Good

Instead, this is a situation that requires gathering of intellectual evidence, typically through conversations. Auditors, we find, actually don't know how to document a conversation, so here is what an audit report might look like:

Re: risk based thinking, held interviews with Bob J. the VP Engineering and Jim S. the President. Management indicated that during the development of the QMS risks specific to customer product requirements, local labor force availability and previous issues with utilities were taken into account. This, they reported, resulted in the current process set and related objectives. For example, the "Maintenance" process was formerly embedded in production, but now is a standalone process in order to better manage utilities.

In that example, the names of the people interviewed ("Bob J. and Jim S.") are the objective evidence, since they can be confirmed later by a third party. The rest of the notes are the supporting evidence to show what they said, and to give some idea that it was acted upon. There's no risk registry, no procedure, no records to prove it. Nothing that approaches any common approach to "risk management." And none would be required, yet the company complies with risk-based thinking just fine.

The Bad

So what might a ***nonconformance*** look like in such a scenario? In real life we can expect to see all sorts of nightmarish NCs written up, as auditors go nuts trying to invent risks from thin air and then play "gotcha!" with the client by writing them up for not thinking of them; or worse, for not completing an FMEA on each risk. None of that is required, but some evidence or risk-based thinking must be present, or a nonconformity can be issued. Here's an example:

Re: risk based thinking, held interviews with John D. the CEO and Fester B. the President. There was little understanding of risk and management admitted it did not consider risk when developing the QMS. The management could not name any risks it might face, nor any actions it took to address those risks.

What we see is that you have to be pretty ignorant of risk to get such a finding. Which is also by TC 176's design; they didn't intend for companies to be written up for having a different view of risk than their auditors, but they did intend a ***complete absence*** of any risk-based thinking to be noncompliant. That's good news for users, since you don't have to do too much to comply with RBT, especially since TC 176 says it's been "implicit in ISO 9001" all along. But for companies that ignore it entirely, blow it off, or fail to execute something, it will be a nonconformity. And it should be.

The Ugly

So, to recap, here's how it should work:

1. Determine how the company has interpreted the requirements for risk-based thinking.
2. Determine how the company has implemented risk-based thinking
3. Conduct interviews with key management to confirm; capture names and discussions as evidence.
4. ***If available***, capture documents and records to support. If not, stop at # 3.

This idea of auditing intangibles may be frustrating, and yes, ISO 9001's risk-based thinking is a mess. But it's not un-auditable, and auditing it doesn't require imposing specific solutions on clients simply because an auditor lacks the imagination to audit something other than a document or record.

And the thing is, auditors have already been doing this, without a peep. In the 2000/2008 versions of 9001, the standard required the management to show "commitment" and "a customer focus," neither of which are tangible things. Auditors typically relied on documentation to check these off, and if the words were on paper, that satisfied them. They were idiots, of course, and should instead have done the same thing I am suggesting here: have conversations with management and key staff, and document that as the evidence.

So we find that auditing RBT isn't the great mystery that many are claiming. If auditors can stop trying to be consultants, stick to the rules, and understand that they should stop their fixation on auditing documents, we might see some benefit from this after all.

At least when RBT hits the fan, we know who to blame.

How to Respond to an Invalid Audit Nonconformity From Your ISO 9001 Registrar

Unfortunately, the ISO certification scheme does not enforce good training on auditors working for CBs (certification bodies), and does not have high standards for the requirements for such auditors either. The result is that sometimes auditors write nonconformities that are invalid — in the US we call them "bogus" — but which nevertheless have to be responded to.

(Note: while this article refers to ISO 9001, the information herein works equally well for AS9100, ISO/TS 16949 and most other management system certifications.)

Common Reasons for Invalid Findings

Typically, these write-ups are invalid because of three common errors:

- **No objective evidence.** Without objective evidence indicated in the finding, the client cannot take immediate "containment" and fix whatever the auditor happened to be looking at. That's critical first step, and has to happen before the company takes any long-term corrective action. For example, an auditor may say *"purchase orders lack approval signatures"* but without indicating ***which exact*** purchase orders the auditor looked at, the finding is invalid (vs. ISO 17021-1) since the client cannot fix the purchase orders. It also makes it impossible for the client to physically verify what the auditor was looking at, in case the auditor made a mistake (for example, perhaps the purchase orders *were* signed, but simply on the back side of the paper, and the auditor hadn't noticed.) Then, the finding could be reversed easily, and no one is harmed.

- **No ISO 9001 citation.** Without citing the exact clause which is alleged to be in violation, the client (again) cannot take proper corrective action because they don't know what is actually wrong. Citing the clause in violation is also an accreditation rule requirement, so any finding that doesn't indicate an exact clause can be thrown out, or the CB must amend the finding to include the proper clause. Be cautious, too, when CB auditors cite clauses or documents other than ISO 9001, such as internal CB documents, "IAF guidance documents" or anything else the auditor may have seen on the internet. Audit findings can only be written against the standard you are being audited against, and that's a firm contractual requirement.

- **Invented requirement.** This is the most common problem, where auditors — after years of auditing against their past employer's QMS, rather than the ISO 9001 standard — come to assume that requirements exist in the standard when they actually do not. Search the ISO 9001 standard for "training matrix," "annual management review meetings" or "preventive maintenance records" and you can see how much of a problem this is (none of those are actually required, but nevertheless routinely mandated by CB auditors.) And, again, if there is no clear citation of an actual ISO 9001 requirement, the client cannot possibly take proper corrective action. Worse, if the client does act on the finding, they are essentially allowing the CB auditor to ***build*** their quality system based on the auditor's personal whims and expectations, so that afterwards the auditor is essentially auditing their own work… a serious violation.

There are many other reasons why a finding might be invalid, as well, but these are the most common.

ISO 17021-1: The Other Guy's Playbook

One of the best ways to ensure you can identify an invalid finding, and then challenge it properly, is to understand the accreditation rules under which all accredited ISO 9001 registrars must operate. These are found in the standard ISO 17021-1**.** All accredited CBs ***must*** comply with this standard lest they be de-accredited, and denied the right to issue ISO 9001 certificates. The enforcement of ISO 17021-1 is done by the Accreditation Body (AB) utilized by the particular registrar; common ABs include ANAB in the US, and UKAS in the UK. You've seen their logos next to the CB logo on your ISO 9001 certificate.

ISO 17021-1 is a dull document, moreso than ISO 9001, but it's a treasure trove of rights and privileges that you never even knew you had. It defines your rights, as well as the rules that restrict auditors from writing bogus nonconformities. I can't stress enough how beneficial it is to purchase a copy of the standard, read it and understand it. The clauses you will want to focus on are 9.4 (Conducting the Audit), 9.7 (Appeals) and 9.8 (Complaints.) It's worth the effort if you are plagued with suspicious nonconformities.

(I hope to be working with Praxiom on a helpful guide "ISO 17021-1 in Plain English" soon.)

The Fear of Appeals

Companies resist filing an appeal because they believe a number of myths, or hold on to some irrational fears. These are sometimes spread by the CB auditors themselves, in an attempt to get clients to accept all audit findings without question; heck, one registrar trains their auditors on how to hypnotize clients without their knowledge, to make them less resistant to their auditors!

Unfortunately, the timidity of clients to challenge CBs creates a self-inflating problem in the industry: the less clients contest bad findings, the more bad findings the auditors write up, since they have no feedback telling them they are wrong. It's therefore imperative that clients push back against invalid findings, not only to ensure the health of their QMS, but to ensure that ISO 9001 certificates worldwide remain trusted and respected.

The most common myths and fears are:

- **If contested, the auditor can take away my ISO 9001 certificate.** This is untrue, since auditors cannot take anyone's certificate away. Those decisions are made by an internal committee within the registrar, *not by the auditor*, and they will not de-certify a client because the auditor is being spiteful. You are guaranteed the right to contest nonconformities under ISO 17021-1, and the auditor cannot arbitrarily violate these rules because his ego has been bruised.
- **If contested, the auditor will escalate the finding to a major nonconformity.** Also untrue, for the same reasons. The definitions of "major" and "minor" nonconformities are defined in ISO 17021-1, and nonconformities don't magically increase in severity because a client questions them.
- **If contested, the auditor will come back angry, and our next audit will be hell.** Typically an auditor won't even remember the issue by the next audit, but even if they do, their behavior is governed by ISO 17021-1, and they cannot begin issuing "spite findings" out of anger. If they do,

those *new* findings can then me challenged, too, and are more likely to be thrown out since they won't be based on reality, but instead on emotions.

- **Challenging a registrar is expensive.** Not true, and technically it's free, other than the cost of the time needed to send the emails. In fact, challenging a registrar can ***save*** the company a tremendous amount of money, by avoiding costs associated with changing the QMS to suit an auditor, or by eliminating the need for an expensive "Nonconformity Follow-Up" audit by the registrar.

- **We hate conflict.** Some companies simply hate conflict, and do anything to avoid it. Unfortunately, at times professional and courteous conflict is a necessary part of doing business, such as pushing back against customers who refuse to pay their bills, or having to fire employees who are insubordinate. If your organization is so conflict-averse as to allow ISO 9001 registrars to do whatever they like, this is an indicator of an entirely different problem, and ISO nonconformities are the least of your worries. Ultimately, companies must remember that the registrar is a vendor, and that you are their customer, and that dynamic grants you certain rights and privileges.

- **Top management doesn't care, they just want the cert on the wall.** This is more common than it should be, and often middle managers tasked with defending the QMS find themselves ordered by their bosses to accept the findings, no matter what, just to keep the cert on the wall. It's a phony argument, since appealing a certificate doesn't de-certify a company, but if the boss is that worried about it, there's little you can do other than find a new employer.

- **Our certificate will expire while waiting for the appeal to be resolved.** This one has some merit, but you should clearly communicate to the CB that you expect the appeal to be resolved by them in a timely manner that does not impact on your certification. There are a lot of minor tweaks the CB can do to ensure your cert does not expire, but clearly they should simply prioritize the issue so that this doesn't even become a risk. If they don't, you have an entirely different complaint you can levy against them.

Steps to Contest a Finding

Contesting a finding is incredibly simple, and should be done in the following order. In all cases, the challenge must be made in a manner that is polite, firm and based on evidence. Let's take a look:

1.) Confirm that the nonconformity is, in fact, invalid. Many clients don't like nonconformities, and want to oppose them, but if the nonconformity is valid, there is no amount of arguing that can reverse it. If it's a valid finding, it's better to work to correct the problem than argue for the sake of arguing.

2.) Don't worry about the closing meeting. Many clients feel that because they have signed the auditor's nonconformance report, and held a closing meeting, that this means the finding has been accepted by the company. This is not true, although some CB auditors will lie and say so. Instead, all you are signing for is ***receipt*** of the nonconformity, not acceptance of it. You are granted the right to go back, after the audit, and study the nonconformity in greater detail. Even if during the closing meeting every nodded their heads in agreement, you are allowed to change your mind once you study the

finding in detail; that is why you do a root cause analysis, after all. So don't feel obligated to accept the finding as valid if it is not, even if you signed for it and agreed to it verbally during the audit itself.

3.) Gather your facts. Next, you have to be 100% absolutely sure the finding is invalid. You will want to put together internal notes on why the finding may be wrong, such as *"auditor didn't cite a requirement"* or *"he didn't indicate what he looked at"* or *"I can't find a requirement anywhere in ISO 9001 that requires this."* If you have purchased ISO 17021-1, go over clause 9.4 to find where the auditor may have violated the accreditation rules, which will help your case. Keep copies of any emails from the auditor, as well as copies of the audit report and nonconformity.

4.) Craft your argument. Using the information, put together a strong argument as to why you think the finding is invalid. For now this is an internal discussion only, so you can be as forceful as you like in your internal notes. Be sure your argument clearly describes what the problem is, and why you cannot take corrective action with the finding written in the way it is.

5.) Send an informal email to the auditor. The best first alert to the auditor is a casual email, written in a friendly manner, but which captures — in broad strokes — what your concern is. In the email, you would ask (*politely*!) that the auditor consider re-wording the finding to address your concerns or ask that they consider withdrawing the nonconformity altogether. Here are a few examples:

> *Dear Joe,*
>
> *As part of our root cause analysis of your finding, we are having trouble coming up with a proper response. We found that as it is written right now, there is no specific ISO 9001 clause cited, and we cannot find where in the standard there may be a violation. Can you help us by rewording the finding by citing the clause you are concerned with, and perhaps explaining better how you feel the clause was violated? If there was an error in the finding and it's not associated with an ISO 9001, we would then ask that perhaps you could withdraw it. Thanks so much.*

Or:

> *We noticed in your finding that you did not indicate the objective evidence you looked at during our audit. As a result, we cannot take immediate containment, since we don't know for sure what to fix. I understand that indicating the objective evidence is a requirement, so could you amend the nonconformity with an indication of what exact evidence you looked at? That would help us greatly. If not, we would ask that you withdraw the nonconformity, since we are unable to take proper corrective action with the problem as written. Thanks so much.*

Now you will notice that both samples are extremely polite and quite cool-headed. Unfortunately. because receiving a challenge is a rare thing for many auditors, they may react with some level of hostility. (Recently, one auditor with registrar SRI threatened to a defamation lawsuit after a mild challenge to a finding!) So you should be prepared for an irrational response, but you must remain professional and calm no matter what.

You should also not let fear of a possible irrational reply dissuade you from pursuing your concern. Eventually it all blows over and everything returns to normal, so if you do get a heated email or phone call from the auditor, just assure them it's nothing personal and you are only trying to do what's best to improve your QMS.

Alternatively, you may get a completely professional and polite reply; so don't assume things will go south just yet.

If you don't get a satisfactory result from the auditor through an informal email, you have to make a formal appeal.

6.) File a formal appeal. This is a formal request for the nonconformity to be reviewed by the registrar's internal committee (not the auditor him/herself). This is a right which is guaranteed to you under ISO 17021-1, and which the CB cannot refuse. To file this, you simply send an email to your registrar's sales contact, and cc a copy to the auditor. Ask that they forward it to the appropriate appeals body within the registrar.

The appeal should more formally state the reason you are requesting the nonconformity to be withdrawn, and should include a copy of the nonconformity, along with specific citations of ISO 17021-1 (if you have purchased it — don't worry if you do not.) You should politely but firmly request the finding be withdrawn or amended, and specifically request the CB take "appropriate corrective action."

Typically, the CB office will then attempt to resolve the problem over the phone, so you may get a call from the home office. ***Resist this***, as it means they are trying to avoid having an official, written record of the issue. This is a risk because they could later change their mind, reverse their position, and you would have no documentation to prove it. Worse still, it keeps the appeal off the record; CBs like to do this so they can hide these from their accreditation body (ANAB, UKAS, etc.) and later claim "we never get any appeals or complaints." Instead, be sure you ask the registrar rep to follow up in writing, with formal corrective action. Keep notes of any phone calls received, and keep copies of any emails received on the matter.

In 90% of the cases that go to appeal, the internal body will side with the client and withdraw the nonconformity. This is true because of two primary reasons: first, the internal committee discovers the finding was, in fact, bogus and agrees with the client. Second, the CB home office does not want of risk losing you as a client, so they would rather throw out the finding, rather than lose your annual revenue. So you stand a very good chance of having the nonconformity dropped entirely.

If not, continue…

7.) Assess the registrar's response. If the registrar has provided a reason as to why the nonconformity should stand, be sure to assess that response in an objective, open-minded manner. It could be they have a very good argument that you did not consider previously, and the finding ***should*** be upheld. If so, write to the CB and alert them that you agree with their result, thank them for it, and proceed with your appropriate corrective action. If the response is lacking, and it's clear the CB is merely "digging in" because they want to remain inflexible,then push forward…

8.) File a formal complaint. If the appeal goes south, and you are ***absolutely certain*** you still have a valid argument, you would then file a complaint with the registrar, and cc their accreditation body. Oxebridge has a separate article on filing complaints here. Once again, however, be sure you remain professional and courteous no matter what. Do everything in writing, and keep records of any and all communication regarding the complaint. CC the registrar's Accreditation Body as well, which will typically shake up the CB so they take your complaint more seriously.

As I said, typically at least 90% of all contested findings are withdrawn, usually just because the CB wants tokeep your business. But if the CB feels they have a valid finding, and especially if there's a direct risk that you are releasing defective product in the market, you may not have a good standing, and should probably accept the finding and make the appropriate corrective action.

As always, if you find yourself in a real bind with your CB, we can help with filing appeals, complaints, or simply counseling you on whether the finding is, in fact, valid. Check our page on Audit Defense Services, or post your problem on The O-Forum.

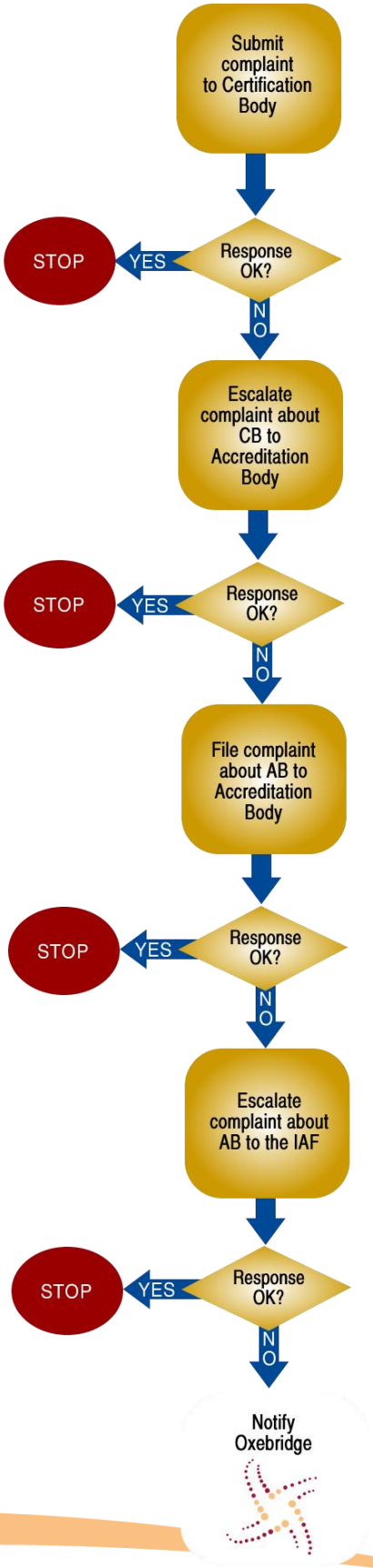
How to File a Complaint Against Your Registrar or Accreditation Body

The following represents necessary steps when filing a complaint against an accredited Certification Body, or an IAF-signatory Accreditation Body. It does not apply to filing complaints against unaccredited, or self-accredited, certificate mills.

This procedure is not to be used for contesting an audit finding or nonconformance. In such cases, you file an appeal by emailing your rationale as to why you feel the nonconformance is invalid; see this helpful article on how to challenge a invalid finding from your registrar. If that fails, ***then*** you may file a complaint.

To process a complaint against a CB, and possibly escalate it to higher bodies, you must follow this order. If you skip any step, the particular party will just throw it back until you follow the sequence.

- You must first submit the complaint directly to the CB. Do not send to a sales representative, but try to find out the proper person within the CB responsible for processing complaints. You can call the CB to find this out, but resist their requests for information on the complaint, as they will try to resolve it over the phone to avoid a formal record. Simply ask for the contact name, and thank them.
    - Submit the complaint in writing. Email is fine, but maintain records of all your communications. Consider using this helpful template (.DOCX file, right click and save to your local drive.)
    - Request that the CB acknowledge receipt, and wait.
    - Resist all attempts by the CB to resolve the problem over the phone or in person. Ensure that the problem is resolved in writing, and that the CB is using their official corrective action process to investigate. You must ensure they maintain a record. If they demand a phone call, record it; but you must tell them in advance that you intend to do so.



  - If the CB reacts with hostility, or with threats of litigation, end the contact. Coordinate with your internal Legal Department.
  - Allow proper time for the CB to investigate and respond.
  - Do not assume you are right; your case may not be as strong as you think. The CB may have a very valid reason for the problem, and their response may be entirely acceptable. Make sure you assess any response with an open mind.
- If the response is inadequate, write back and tell them so. You may give them another chance to clarify things, but it's optional.
- If you are certain you have a firm complaint and the response was inadequate, you may now escalate to the Accreditation Body.
- Find out which AB is responsible for the accreditation of the CB in your region. This will usually be the AB whose logo appears on your ISO certificate. You may also check by verifying the CB's website. Find out the appropriate contact within the AB with whom to file complaints. For ANAB, the complaint portal may be found online, at this link.
- Write the complaint again, but this time reword it as a request for the AB to investigate the CB.
- Obtain acknowledgement of receipt, and wait.

1. If the AB's response is inadequate, you have to file a complaint against the AB itself for improper complaints processing. You will reference the original complaint, but now the focus is on the AB, requesting it investigate itself and taken internal corrective action.
2. If the AB's response to this complaint is inadequate, escalate the complaint to the International Accreditation Forum (IAF). Submit this to secretary@iaf.nu and frame the complaint as one against the AB for two concerns: (1) failing to adequately address the original complaint against the CB, and (2) failing to properly process a complaint lodged against the AB itself.
3. If you still do not get an adequate response, contact Oxebridge for what other options you may have.

How To Ensure Your Registrar Uses the Right Industry Codes, and Why It's Important

An arcane detail that nearly every ISO 9001 certified company misses is the assignment of industry codes to your QMS scope by your Certification Body (CB, or "registrar.") These are typically expressed as a set of SIC and NACE codes, and are then used to determine which IAF Code your QMS falls under. The IAF is the International Accreditation Forum, and oversees the overall accreditation scheme for ISO 9001 and other management system certifications; they also establish some of the rules governing your registrar. The IAF Codes are used to "hone in" the scope of your company's business, so a registrar auditor with appropriate experience can be assigned to your company. If you develop software, than an auditor who only has experience in woodworking is not supposed to be assigned; usage of the IAF Codes helps ensure this.

The IAF Codes are, however, largely a joke. Whereas the world has developed the SIC (Standard Industrial Classification) system, comprised of over 2,300 industry classifications, and the NACE ("*nomenclature statistique des activités économiques dans la Communauté européenne*") system, comprised of about 1,000 codes, the IAF codes total …. get ready … 39. As in thirty-nine. One less than forty. Three niner. The age you still tell people you are. You get the picture…

To some extent, the IAF can be excused for dumbing this down, since had they attempted to create a system which matched auditors and clients by SIC or NACE alone, it would be nearly impossible; some generalization had to be done. But the reduction of all human endeavors to less than forty codes is somewhat ludicrous, and as a result a veterinary doctor who worked on farm cows can audit medical facilities and psychologists' officers under IAF Code 38 "Health and Social Services." Anyone involved in any aspect of anything having to do with technology can audit under IAF Code 33 "Information Technology," meaning a guy who designed HTML 1.0 websites using GeoCities back in 1998 is fully qualified to audit a company developing targeting software for jet fighters in 2017.

But let's assume for a minute that the IAF Codes are acceptable; there are still significant problems lurking, and as usual, the Certification Bodies (CBs, or "registrars") are to blame.

Send In The Clowns

The accreditation rules require, as I said, that auditors be assigned only when they have relevant industry experience and/or training within the industry served by the client. To do this, CBs are supposed to request the SIC and/or NACE codes from the client during intake; typically your accountant has these, since they impact on accounting and taxes. Then, the CBs use the official IAF ID1:2014 guide to convert SIC or NACE to the appropriate IAF Code. Once they have that, they can assign a Lead Auditor who has the IAF Codes under his or her qualification.

(Note: that IAF guidance document applies to QMS and EMS audits, so this article is equally applicable to users of ISO 14001.)

Naturally, the CBs can't even get that right. Because auditor pools are shrinking, and they refuse to pay auditors well enough to refill the ranks, your CB is unlikely to have a robust population of auditors eligible for each IAF Code. Even if they do, many of the auditors are overbooked, and not available. So

the CBs have to assign whomever happens to be breathing at the moment, and that means they need to fudge the IAF Codes.

So what you're likely to see — or ***not*** see, rather — is that they have assigned the SIC and NACE codes ***for you***, and from that they determined an IAF Code that matches whatever auditor they had already determined was available for your contract, whether or not that auditor is qualified for your actual industry. Then you're surprised when the drooling clown shows up and can't speak your industry's language, and nearly explodes the building when trying to use the hand dryer in the bathroom.

Do Your Own Heavy Lifting

To keep tabs on this, you must take some really simple, basic steps. If you're a new client, then as part of the CB's client intake, you should be sure to provide your registrar with the SIC and NACE codes that apply to your industry. If you want to be really clever, then check the table below (derived from IAF ID1:2014) and supply them the IAF Codes as well. Then, be sure those numbers are entered into the CB's records, which you can usually confirm by checking your "Client Information Sheet" the CB will maintain for you. They always have some record like this, and it may have a different name, but it's in your file somewhere because the CB has to produce it when ***they*** get audited by their Accreditation Body.

If you're a ***current*** CB client, then ask your CB rep what IAF codes have been assigned to your company, and compare them against the table below. If something looks wonky, then ask them to change their records, and provide them the right SIC/NACE/IAF combination. Be prepared: this may trigger a change in which auditor is assigned to you. That may be a good thing, or a bad thing. But if you're having problems with an incompetent auditor, having your IAF Codes properly assigned may fix the problem for you.

It's also important to point out that the CBs must use NACE ***2.0*** codes, and not the obsolete NACE 1.1 codes. As recently as this week, I caught a CB still calculating an IAF code based on NACE 1.1 codes, which have been obsolete for over a decade. For a listing of NACE 2.0 codes, click here. The IAF document specifically mandates that CBs use NACE 2.0, and not 1.1, but that doesn't stop them from forgetting to update their procedures.

For a listing of SIC codes, click here.

If you see a CB using ***NAICS*** codes, be sure not to confuse them with NACE. These are, instead, from the North American Industry Classification System, and are occasionally used by some registrars; you can find a list of NAICS codes here. There is no matrix of IAF to NAICS codes, so you may have to do a few jumps (calculate NAICS to SIC, then SIC to NACE, then NACE to IAF.) Still, it should take all of five or ten minutes.

As usual, the accreditation bodies like ANAB could catch these problems in a few minutes, simply by checking if a CB's clients had the proper NACE and IAF codes they assigned to them; it took me all of five minutes to find that the CB from this week had improperly assigned an auditor because they used an obsolete NACE 1.1 code, and wound up with the totally wrong IAF code. It defies explanation that CBs can be so routinely wrong about this basic task, but we can't rely on the Accreditation Bodies to do the

only job they have, so you'll have to do it for them. That means, as I said, double checking to ensure all the right codes are assigned, and if not, having them corrected.

Here's a table of the IAF Codes, and their NACE 2.0 equivalents:

IAF Code	Description of economic sector / activity	NACE 2.0 Equivalent(s)
1	Agriculture, forestry and fishing	01, 02, 03
2	Mining and quarrying	05, 06, 07, 08, 09
3	Food products, beverages and tobacco	10, 11, 12
4	Textiles and textile products	13, 14
5	Textiles and textile products	15
6	Textiles and textile products	16
7	Pulp, paper and paper products	17
8	Publishing companies	58.1, 59.2
9	Printing companies	18
10	Manufacture of coke and refined petroleum products	19
11	Nuclear fuel	24.46
12	Chemicals, chemical products and fibres	20
13	Pharmaceuticals	21
14	Rubber and plastic products	22
15	Non-metallic mineral products	23, except 23.5 and 23.6
16	Concrete, cement, lime, plaster etc	23.5, 23.6
17	Basic metals and fabricated metal products	24 except 24.46, 25 except 25.4, 33.11
18	Machinery and equipment	25.4, 28, 30.4, 33.12, 33.2
19	Electrical and optical equipment	26, 27, 33.13, 33.14, 95.1
20	Shipbuilding	30.1, 33.15
21	Aerospace	30.3, 33.16
22	Other transport equipment	29, 30.2, 30.9, 33.17
23	Manufacturing not elsewhere classified	31, 32, 33.19
24	Recycling	38.3
25	Electricity supply	35.1
26	Gas supply	35.2
27	Water supply	35.3, 36
28	Construction	41, 42, 43
29	Wholesale and retail trade; Repair of motor vehicles, motorcycles and personal and household goods	45, 46, 47, 95.2
30	Hotels and restaurants	55, 56
31	Transport, storage and communication	49, 50, 51, 52, 53, 61
32	Financial intermediation; real estate; renting	64, 65, 66, 68, 77
33	Information technology	58.2, 62, 63.1
34	Engineering services	71, 72, 74 except 74.2 and 74.3
35	Other services	69, 70, 73, 74.2, 74.3, 78, 80, 81, 82
36	Public administration	84

IAF Code	Description of economic sector / activity	NACE 2.0 Equivalent(s)
37	Education	85
38	Health and social work	75, 86, 87, 88
39	Other social services	37, 38.1, 38.2, 39, 59.1, 60, 63.9, 79, 90, 91, 92, 93, 94, 96

Using Indented Lists to Present Audit Evidence

Internal ISO 9001 or other QMS audits are always better when the reports include clear and accurate objective evidence; for external audits, this is actually mandatory. The reason objective evidence is important is twofold: first, it allows someone to verify the audit details at a later date. More importantly, however, it provides the auditee with critical information on what specifically was examined when a nonconformance is issued. Without indicating the evidence of what was found, the auditee can't perform containment or proper correction of any problems identified.

Most auditors will complete their audit reports in a modern word processing app or program, like MS Word, but this following approach even works if you're still filling out audit reports by hand. The method here relies on indented or "bulleted" lists to organize the evidence in a simple, yet powerful, way that keeps an auditor's thoughts organized, and allows the auditee to read the data in an orderly fashion later.

Now here's the thing: I like to record a ***lot*** of objective data, and I always advocate this for my clients or students. But you can tailor this to whatever level of data you intend on recording. This approach assumes there is space on your audit report form to record the data; if not, yo umay want to add a "Notes Page" or append a separate file with the data. Whatever works.

Organize your data by the process you are auditing or (if you're hardcore oldschool) by clauses. No matter what proponents of either approach say, both work.

Then, begin to layer in your evidence starting with a master bullet that says what the subsequent bullets will be regarding. Below this top bullet, indent once and begin to add what you verified. As you read this, you will see I use the word "verified" a lot; it hammers home that the audit verified evidence, and didn't just *obtain* the evidence. It's also a practice that slowly trains your brain to reject any subjective opinions, and to spot areas where you didn't actually "lay eyes" on evidence. Also, always be sure to indicate *who* you spoke with, as conversations are another form of evidence — not all forms of evidence are documents and records. My personal preference is to reference people by their titles, since some people feel nervous if their name appears in an audit report.

So we might begin to see something like this:

- **Re: Purchasing process:**
    - Interviewed Purchasing Manager
    - Verified Purchasing procedure rev 3
    - Verified procedure requires Approved Vendor Database entry
    - Verified Approved Vendor Database screens in the Purchax 3000 ERP system

Below that, layer in additional details of the specific evidence. When you have a finding of nonconformity or an opportunity for improvement, indicate them here. I like to add yellow highlighting to those, as it will help draw the eye to them.

- **Re: Purchasing process:**
    - Interviewed Purchasing Manager
    - Verified Purchasing procedure rev 3

    - Verified procedure requires Approved Vendor Database entry
    - Verified Approved Vendor Database screens in the Purchax 3000 ERP system
        - Verified entry for APE-X Company, compared vs. PO # 3453 – entry OK
        - Verified entry for Landlubber Rubber Scrubbers, compared vs PO # 4500 – entry OK
        - PO # 5544 was issued to Toxico Baby Wipes, for raw material P/N 400-876353, but Toxico is not listed in the Approved Vendor Database.
        - Verified Approved Vendor Database is on a server subject to backups
        - OFI: consider improving field size of the Approved Vendor Database data entry fields, as some Purchasing staff reported it is too small and data entry errors are not easily spotted
- **Re: Customer Service process:**
    - Interviewed Customer Service Manager
    - Verified procedure SOP 99-43 rev A
    - Verified Customer Complaint Log, live data with entries as of today

And so on. You will eventually build up a long list of evidence, but one that is easily navigable and read by the auditee and top management.

Regarding the findings of nonconformity, which (again) I highlighted: when you are recording your evidence, you can do so in a free-form manner. Later, when you want to write these as formal findings, you will want to re-write them to provide the three minimum required elements of a nonconformity: the objective evidence, the requirement, and an explanation of the disconnect between the two. On some audit reports, this is entered elsewhere on the form, so your free-form notes, presented in the bulleted list, may not represent the final language of the “official” finding — and that’s fine.

Do It Yourself "Rapid ISO 9001" – Ten Quick Pointers

Recently, a fellow posted a question on LinkedIn asking for tips on how to implement ISO 9001 quickly. Like a batsignal going up, I was compelled to reply. I came up with a list of 10 — okay, 11 — points that summarized what I have been saying for years now. I thought I'd reproduce my response here.

In no particular order (and not meant to be comprehensive by far):

1.) Avoid "steering committees." These are invented to offload responsibility of the consultant, or internal ISO guy, onto a group of people who he can later blame everything on when it stalls. You've heard the joke that a camel is a horse designed by a committee. There is no need whatsoever for a steering committee unless you are implementing ISO 9001 in an organization with thousands of employees over many, many sites. These committees inevitably slow the process down. Instead, assign the roles to a few key individuals, and have signoff responsibility for procedures and tools per my next suggestion, # 2.

2.) Don't have everyone sign off documents. Have ONE key subject matter expert (SME) or top manager sign off on top-level procedures, and only a ONE SME sign off on anything of a lower level. As soon as you add a second signature, you invite delay, disagreement, egos, and trouble.

3.) Read the standard and interpret it how you see fit for your organization. You can listen to, but not rely solely, on the experiences of others from other companies. How they did it at AirBus isn't going to be useful if your company only has ten employees. Keep it simple, keep it customized, keep it organic to your company and its philosophy. If your intent is to get the company certified later, then make the certification auditor understand your interpretation.

4.) Avoid document numbering. Not required by the standard, and it only increases the chances of nonconformities due to mis-typed references to numbers, and makes for a hellish editing experience if you ever change a number. Refer to documents by titles. After all, you don't buy a book at the book store by ISBN number.

5.) Keep tools simple. Document control can be done entirely in your computer's operating system without buying any third party software. Calibration can be managed with a simple spreadsheet. Record control can be a simple table written in Word. The approved vendor list probably already resides in your accounting software.

6.) Enforce quick approval of documents. The biggest delay in any implementation is the document approver(s) dragging their feet. Have top management force the issue. If it takes more than a few days to get a document approved, something is really wrong.

7.) Develop your program, and procedures, based upon what you do NOW. Then fill in the gaps or change things only where they clearly conflict with the standard. Don't reinvent fire.

8.) Avoid the temptation to improve the entire company as a part of your ISO 9001 implementation. I've seen downtrodden quality guys try to use ISO 9001 as a hammer to "finally get what I've wanted for years" and try to pin everything on the certification, as a threat to management. "If you don't buy me a new CMM, the auditor will flunk the company!" ISO 9001 provides for improvement, you don't have to have a perfect company in order to implement it from the start.

9.) Don't use boilerplate documents you buy online. Yes, the temptation for this easy approach is very strong. Yes, the sales guys for these sham products will tell you anything. Giving you my experience as both a consultant AND an auditor for registrars, I can assure you that using boilerplate documents will cause nothing but problems. If your intent is to certify the company, this will likely cause major nonconformities. I've spent weeks trying to clean up companies that used these things, and it just added a huge amount of time and expense. This sounds counter-intuitive, but It is FASTER and CHEAPER to write custom documents that suit your unique organization than it is to cut and paste your company name over someone's generic procedure. *(If you really **must** use a template kit,* download our free one*. Yes, template kits suck, but free ones suck less.)*

10) If you hire a consultant, make sure he or she doesn't suggest doing any of the things I just warned you about. If you are vetting consultants and they mention "steering committee", remember rule # 1, and don't sign the contract. Bad consultants make money by padding their contracts and intentionally stretching out the time for implementation, because they don't have other clients waiting to fill their calendars. Don't buy into consultants who make claims of "guarantees" for certification (if certification is your goal) as it usually means they are (a) neophytes who don't know that nothing during an ISO 9001 audit is guaranteed, or (b) they have a "backdoor deal" with a specific registration auditor who has promised them a favorable audit in exchange for leads (as soon as the registrar sends a different auditor, you are hosed.) A good consultant can work quickly and efficiently, reducing your costs. Anyone who says otherwise is scamming you.

After this, the original poster asked about buying a pre-assessment from a registrar, so I added an 11th point:

11) Don't buy a pre-assessment audit from your registrar. I can do that for you for free, right now: ***"Your organization does not comply with ISO 9001. Please implement it***." There, I just saved you a few thousand dollars! Pre-assessments are a waste of time and money (again, the auditors out there will disagree with me, but I've been on the Advisory Boards of two registrars and can tell you, even they know it's a scam.) You shouldn't audit anything until you have your system almost fully implemented. Then conduct a round of *internal* audits, which you have to do anyway to comply with the standard, and use that to identify remaining gaps.

Configuration Management for the Small Machine Shop

(Note: this article discusses AS9100, but is equally valuable for some ISO 9001 users, where configuration management may be important, even if ISO 9001 does not have a clause on it.)

AS9100's requirements for configuration management (CM) are well understood by the massive aerospace primes, but can present overkill and confusion for small downstream suppliers. Fortunately, for the small machine shop, the configuration management requirements can be easily met.

Normally, there are two types of machine shops: those with design responsibility, and those which merely manufacture products per the customer's design. This article will discuss the approaches for both.

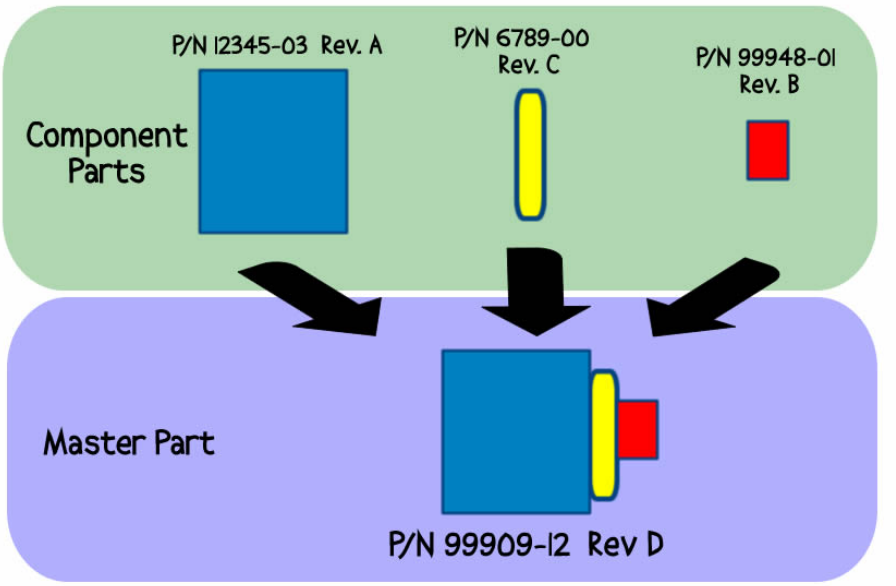
Let us start by reviewing the CM clause within AS9100 revision C:

> ***7.1.3 Configuration Management***
>
> *The organization shall establish, implement and maintain a configuration management process that includes, as appropriate to the product*
>
> *a) configuration management planning,*
>
> *b) configuration identification,*
>
> *c) change control,*
>
> *d) configuration status accounting, and*
>
> *e) configuration audit.*
>
> *NOTE See ISO 10007 for guidance.*

Configuration management is defined by ISO 10007 as *"coordinated activities to direct and control the interrelated functional and physical characteristics of a product [as] defined in the requirements for product design, realization, verification, operation and support."* That is quite a lot to manage, so a shorter definition might be "managing the components of a product."

For the machine shop, such "management" generally falls into two areas of focus: document control and product identification. The document control aspect is concerned with the identification of design data (drawings, for example); the product identification aspect is concerned with ensuring the revision level of parts is verifiable when looking at physical parts. As the 7.1.3 clause indicates, this activity is limited to CM "as appropriate to the product." Therefore CM does not need to be applied to setup tooling or equipment; doing so is optional. Also, each bullet point in clause 7.1.3 may or may not be applicable to your particular product; not all requirements are mandatory.

Configuration management is necessary when products are comprised of various levels of parts that come together to form a final, complex assembly. For the purposes of this article, we will simplify this to two levels: the **master part**, which is then comprised of **component parts**. See below.



For such assemblies, not only must the master part be identified with a part number and revision level, each component part must also be identified by part number and revision level. The print for the highest level master part must include an indication (normally a list) of the components including – again – their revision levels.

Configuration Management Planning

The first requirement is for "configuration management planning." In the typical machine shop, this is easily accomplished by developing a single Configuration Management Procedure. This can be included in your Quality Manual, or made as a separate document. Generally, this procedure would only be a few pages long, and define the overall methods for configuration management that you implement. It will include the two aspects I mentioned: document control and identification of configuration items. It's best to proceed through the other requirements to understand how you might implement CM, and then you can write your procedure based on that, at the end. So we will revisit this in a moment.

Configuration Identification

The second requirement is for "configuration identification." The goal of configuration identification is to consistently ensure that product is properly identified not only with its current part and revision status, but that we know for sure that it is comprised of the proper sub-components, each at *their* current part and revision status.

In the typical machine shop, this is accomplished as follows:

- **Conceptual identification:** when designing parts, these must be assigned both a part number and a revision level. This would then be captured in the associated design data (drawings, solid models, etc.) A method must exist to be able to identify which sub-components are used to form the higher-level assembly; again, this may be a "Master Data List" (MDL) of associated component parts within the master part's design data, or it may be done through a numbering scheme which identifies the master part for which all component parts are associated. For

machine shops with design responsibility, this applies; for machine shops without design responsibility, the shop must ensure it obtains the proper design data from the customer.

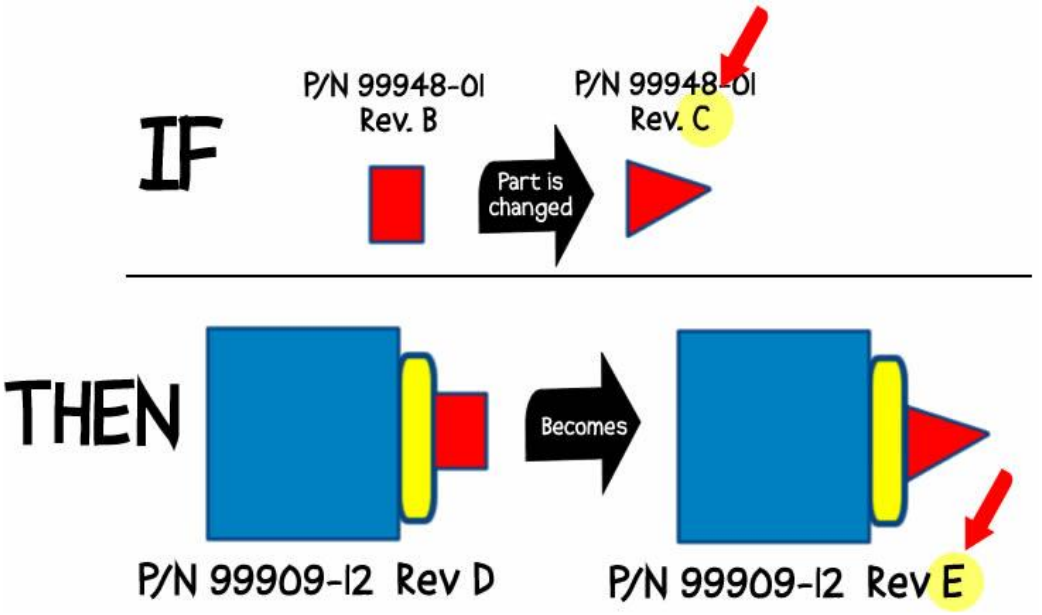
- **Physical identification**: physical products must be identified with the part number and revision. (***Both are required***; one without the other fails basic CM expectations.) Such identification can be a physical marking/tagging on the part, or merely having paperwork nearby when marking or tagging is not possible (such as when a part is going through a furnace, or being plated.)

Work orders or travelers should also reference the proper configuration (part number and revision level) of the referenced part(s).

Configuration identification applies to raw materials, in some cases. This is true when a sub-component is a purchased part. In such cases, the part itself must be ordered by part number and revision, which may be defined by the manufacturer or distributor; if so, the design documentation will reference these numbers, unless a company part number is created. If the latter, a matrix of company part numbers and manufacturer part numbers must be maintained. Then, when the purchased parts are received, the part's identification must include that part number.

Configuration Change Control

The third requirement is for "configuration change control." This is an important requirement aimed at ensuring the known configuration identification is maintained when the part's design is changed. The changes may occur from two directions: a change to the master part, which impacts on one or more of the sub-components; or a change to one of the sub-components, which thus changes the master part.



For machine shops that design parts, the design change process (often via an Engineering Change Order) must include updating related parts at the higher and/or lower levels. A change to a component will *always* necessitate a change to the highest level master part, for example, since the master part's revision level is always reflective of a specific set of components, each of a specific revision level themselves.

For machine shops that do not design parts, but merely manufacture parts designed by their customer, the only requirement would be to maintain the configuration of the customer. This means not altering the design of the product, and ensuring the parts produced always match the design data provided. When the customer changes the design, there must be a method to ensure the changes are implemented as directed by the customer; this could be purging of the old parts, or using up the existing stock and applying the change only to new orders, etc.

Configuration Status Accounting

The next requirement is for "configuration status accounting" (CSA). This terms confuses a lot of folks, but it helps if you shuffle the words as follows: "accounting ***of the*** configuration status." ISO 10007 defines this as including the *"recording and reporting of product configuration information, the status of proposed changes and the status of the implementation of approved changes."* It merely means maintaining knowledge of the product's configuration, even when it changes.

For large design and manufacturing houses, CSA can be complicated. Imagine an aircraft manufacturer: they must account for the configuration of all parts at all levels of the aircraft, from the very first bolt produced, through to the final aircraft itself, which may be comprised of hundreds of thousands of part numbers. A robust CSA program helps keep all this on track.

For machine shops, however, the activities associated with part identification and change control comprise CSA, and therefore no additional effort is required. However, your configuration plan document (from the first requirement, above) should clearly indicate this.

Configuration Audits

The final step is for "configuration audit" (CA). Again, for large manufacturers this can be an incredibly complex activity; imagine auditing the final aircraft to ensure that all the installed parts are at their correct revision levels.

For machine shops solely manufacturing parts to customer prints, CA does not apply at all. Remember, AS9100 says that these requirements are to be applied "where applicable to the product." For machine shops *with* design responsibility, the final inspection of products should include a step that ensures the final assembly is comprised of all appropriate sub-components, and all revision levels match the approved design (prints). So final QA inspection can count as a configuration audit. Once again, this should be defined in the configuration plan document, so this is clear. But no massive, complex "configuration audits" would be required.

Configuration Management Planning (Redux)

Coming back to the Configuration Management Plan document, as we said, a procedure would suffice for small machine shops. Beyond the typical header and introductory material, the content should look like this:

- **Scope of CM activities**: a description of how much CM the company is responsible for, whether the shop is design responsible or not, and the role the customer may play in any of the CM steps.

- **Unique definitions:** any company specific CM-related definitions that may differ from those in the industry.
- **Configuration identification:** define how the company creates part numbers, how part revisions are assigned, how design data (drawings, models, etc.) include this data, and how product (including purchased parts) are physically identified.
- **Configuration change control:** define the methods for changing product design data, including how revisions are advanced, and how such changes are approved. This may be included in related design procedures, so referring to these may be sufficient.
- **Configuration status accounting:** include an explanation that the activities for identification and change control (above) constitute CSA, and that work orders or travelers will monitor the configuration status throughout production.
- **Configuration audits:** include an explanation that configuration audits are not required "due to the limited CM requirements applicable to the company." Then, explain that final QA inspections will "audit" the configuration of the finished product before delivery, and that signoff of QA shall constitute a record of a successful configuration audit.

Your mileage will vary with the effectiveness of this approach. Some small machine shops may nevertheless have significant design responsibility, or may work on very complex products, so a more robust process may be required. But for the majority of small shops, this approach will be sufficient to both meet AS9100 as well as ensure good configuration control to ensure the quality of finished products.

Process Audits for ISO 9001 Made Blindingly Simple

So many are confused by process auditing, it's become a virus in the industry. Let's inoculate.

Rememebr that there's no formal thing such as "process audits." It's not defined anywhere, and anyone telling you how to conduct process-based audits just made it up. Just like I did. This article is just my own made-up approach.

A process audit shifts the focus from the product to the process, and examines each process' ability to produce a product that meets the requirements for that process. You are still looking at products, but not solely at them. Here's how it's done in ridiculously simple terms:

1. **Get a list of the processes**. If this hasn't been done, ***stop now***. You can't proceed.
2. For each process **determine the product**. Experts like to call these "outputs" – don't get confused. It's the product of that process. Simple.
3. **Review the documentation** for the process. Assess general compliance against ISO 9001 and internal requirements. Write up any findings as part of the document review.
4. **Go where the process is conducted** (shop floor, office, etc.) Examine multiple products as they pass through the process. If only one product is running at that time, go back and look at records of other products done in recent history.
5. **Assess the end result of the process** and compare against the expected end results. If they don't match, the process isn't working. Write a finding.
6. Go back to step 3 and repeat for each remaining process.

Forget about "inputs" and "outputs" and "process owners" and those ridiculous Turtle Diagrams. They are not required. Assess each process to see if it can produce a product that meets the requirements.

Where it Gets Complicated – Only A Little

Here are the problems you can expect to find:

- **Processes are not identified.** Too many companies have failed to identify their processes, because of unclear language in ISO 9001 since the 2000 revision. If the processes are not known, you cannot audit against them.
- **The "product" of a process is not clear.**For manufacturing processes, the intended end result is simple: its a physical product. For other processes, or for service industry processes, this can get tricky. But it's just an intellectual game once you get the hang of it. Here are some examples:
    - If the company has identified "Purchasing" as a process, then the "product" of that process might be purchase orders.
    - For a "Sales" process the product might be "signed contracts" or "customer orders."
    - For a "QMS Management" process, the product might be a measurement, such as reduction in customer complaints.

But every process is done for a reason, and is done to generate something. Identify that "something" and you have the "product" for that process.

- **The product requirements are not clear.**Every process generates a thing, and that thing must meet certain requirements. In our examples above:
    - Purchasing's purchase orders must be complete, signed off, and accurate.
    - Sales' contracts must be comprehensive, reviewed, approved and signed by both the customer and the company.
    - QMS Management's reduction in customer complaints must be measurable, and actually measured.

If you encounter any of these problems, you must stop and issue a nonconformity against ISO 9001:2015 clause 4.4. You can't go any further until these are addressed, and everything is properly defined.

Another problem is when a process is not active at the time of audit; for example, a production line is temporarily down, or only processing one type of product. In this case, you must audit records of recent process activities, to ensure the product was measured and met requirements.

Nonconformities

There are multiple aspects that can result in nonconformities:

- **The company hasn't identified** the process, the products of the processes, and/or the requirements for the process. Nonconformity against clause 4.4.1 3rd paragraph.
- **The company has identified everything, but isn't measuring it**. You have no way to ascertain if the process is effective. Nonconformity against clause 4.4.1 bullet point G.
- The company is measuring each process, but the **evidence shows the process isn't meeting the requirements**. If the company has identified the problem, and is working on corrective action, then there is no nonconformity. If no corrective action is in the works, a nonconformity can be issued against 4.4.1 bullet point H.

There may be other findings that emerge (out of control documents, lack of training records, etc.) but these are *in addition to* process-based findings, and not necessarily indicative of a process failure.

Where Auditors Screw Up

Because process auditing is not well defined, it's left to auditors' imaginations — and whatever they may have read on some forum somewhere. As a result, we have an entire generation of auditors who over-complicate process auditing and demand to see evidence of things that are not specifically called for in ISO 9001. This includes:

- **Demanding that process owners be defined.** Nice, but not required.
- **Demanding that proper resources be allocated.** Entirely subjective; an auditor cannot determine the resources, so therefore cannot determine if they are not fulfilled. Only in extreme

cases (e.g., the company doesn't have anyone on staff to run the machines) can a finding be written here.

- **Demanding process improvement**. Entirely subjective; improvement can take months or decades, and an auditor cannot assign an arbitrary due date for process improvement.
- **Demanding process map.** Not required.
- **Demanding Turtle Diagrams.** No…. not required. Just stop. Go home. Switch to decaf.
- **Demanding procedures to support the process.** Not required.
- **Jumping to root cause.** When a process deficiency is identified, the auditor should usually stop and write the finding. Too many auditors jump to a pre-emptive, on the spot, knee-jerk root cause analysis and write the finding against that. (For example, jumping to a conclusion that training was insufficient.) Root cause is for the ***company*** to conduct after the audit is over, not for the auditor to do during the audit.

Auditors waste time looking for process-related aspects that are not required, when this time would be better spent obtaining a greater sample of process data to determine if the process can meet the requirements.

There you go. Process auditing in six easy steps.

Selecting a Registrar (Certification Body)

If you choose to have your management system certified by a third party, there are some important realities to consider. Unfortunately, turmoil in the market has led to some confusion, much of it intentionally created by unaccredited "certificate mills" who are trying to steal market share. You're going to spend a lot of money on your registrar, you need to make the right decision. Here's a handy guide on selection of your third party Certification Body (CB), or "registrar."

Accreditation is King

Be sure your certification body is accredited by an IAF-signatory body. In the US this is ANAB, although you may on occasion see one accredited by UKAS from England. Hiring an unaccredited "certificate mill" is like buying a diploma from a website in Slovakia. Your customers will reject it when they find out, forcing you to just get an accredited cert anyway, making you look like the guy who got his medical degree from Colombia… the country, not the university.

The growth of unaccredited "cert mills" has exploded in recent years, and they have learned a new trick: to claim accreditation with an equally bogus "accreditation body" that either doesn't exist at all, or is merely the same guy using a different logo. So to check if a Certification Body is legitimately accredited, you have to conduct two steps:

First, check if the certification body is listed as accredited by ANAB; their searchable database can be found here. Alternatively, you can search the UKAS website here. If you find a listing, be sure it is the exact registrar you are considering, by carefully checking the name and home office address. Cert mill operators are famous for creating fake registration companies with slightly-off spellings. If they check out on ANAB or UKAS, then you can stop and don't have to go to step two.

If the registrar is not listed, ask they why not. If they claim to be accredited by a body other than ANAB or UKAS, get the name, and then search the IAF members list to see if their accreditation body is legitimate. It could be the registrar is accredited in another country, other than the US or UK, and it's perfectly legitimate. Or it could be that the accreditation body is as fake as the registrar.

Contrary to their claims, there is little difference in pricing, so you won't save much on hiring a certificate mill, and you will save yourself a lot of embarrassment, or accusations of fraud.

Here are some examples of "fake" certificates (meaning not accredited to ISO 17021) and a legitimate one.

Fake

QSRD-International

Certificate Of Registration

This is to certify that:

[redacted]

At the following Location(s):

[redacted]

Operates a

Quality Management System

Which complies with the requirements of:

ISO 9001:2008

For the following scope of Registration:

Precision Casting, Machining, Fabrication and Assembly

Certificate Number:	2062-QSRD-150223	Original Certification Date:	7/28/10
Audit Number:	11226	Current Certification Date:	10/31/2011
Date of Issue:	10/31/2011	Expiration Date:	10/31/2014

QSRD Certification Manager

This certification remains the property of QSRD, 15400 Easudes Road, Ann Arbor, Michigan. It may be recalled for cause at any time. The above listed company is responsible for maintaining this certification through periodic audits conducted by QSRD. For questions regarding the validity of this certificate call the certification manager at 734.678.9747.

The fake certificate above can be identified by its lack of an accreditation logo. Only the logo of the "certification body" is shown. Legitimate certificates must have two logos: one for the CB and one for the accreditation body.

Fake

QualityMasters

QualityMasters verklaart hierbij dat

[redacted]

Beschikt over een managementsysteem welke in overeenstemming is met de eisen van de norm

NEN-EN-ISO 9001:2008

Voor het toepassingsgebied(scope)

Inkoop, import, verkoop en distributie van bevestigingsmaterialen of verwante producten conform klantspecificatie, D.I.N., I.S.O. of andere internationaal geldende kwaliteitsnorm.

Datum van uitgifte 27-05-2010
Geldig tot 27-05-2013
Certificaatnummer NL 5092

QualityMasters
Daggelderweg 10
3449 JD Woerden
[t] (0031) (0)348 430425
[e] info@qualitymasters.com
[w] www.qualitymasters.com

Namens Stichting QualityMasters,

N.B. Het niet nakomen van de voorwaarden zoals gesteld in de certificatie overeenkomst en/of het niet voldoen aan de eisen van de betreffende norm en/of richtlijnen kan leiden tot het opschorten en/of intrekken van het certificaat.

Dit certificaat blijft eigendom van Stichting QualityMasters.

This certificate mill document also lacks an accreditation body logo. This is a fully ***un***-accredited certificate.

Fake

Certificate of Registration

[redacted]

G-PMC, LLC issues this certificate to the firm named above,
Having assessed and approved the firm's quality management system and finding the system conforms to the standard(s) of:

ISO 9001:2008

The quality management system is applicable to the following:

Specializing in the Precision Machining & Manufacturing of Parts from Metallic & Plastic Materials for the Military, Biotech, Power, Aerospace, Medical & Commercial Industries.

This approval has been assessed and approved by G-PMC, LLC against the provisions of ISO 9001:2008. The system will be monitored by G-PMC, LLC. In the issuance of this certificate, G-PMC, LLC assumes no liability to any party other than the firm named above, and then only in accordance with the agreed upon Quality System Assessment Agreement.

OFFICIAL SEAL — INDUSTRIAL LEADERS GROUP — ACCREDITED

American Raw Materials — An ARM Certified Co. — Seal of Approval

G-PMC, LLC — Value Added Registrar

Certification Number: GPMC-122211-1
Original Approval: December 22, 2011
Date of Issue: December 22, 2014
Date of Expiration: December 22, 2017

ABAC

Jim Davidson

Jim Davidson
Credentialing Director, Director Auditor Programs
INDUSTRIAL LEADERS GROUP-
E-mail: jim.davidson@industrialleaders.com

Certificate G-PMC, LLC — ISO9001 — Of Registration

This cert mill slathers on logos, confusing things further. Verifying the IAF website reveals that none of the logos actually mean anything, as none of the alleged "accreditations" are internationally recognized. In addition, the accreditation body "ABAC" doesn't really exist, and is merely a website operated by the same consultant/auditor who issued the certificate. This is a case of "self-accreditation," another mark of the fraudulent certificate mills.

Legitimate

EAGLE Registrations Inc.
SERVICE • INTEGRITY • VALUE
123 Webster Street, Suite 360 | Dayton, OH 45402 | USA
www.eagleregistrations.com

ANAB
ACCREDITED
Accredited by member of the IAF MLA for QMS

Certificate No. 3729 (Recertified September 16, 2013-2 Copies)
October 12, 2013 through October 11, 2016

Certificate of Registration

This is to certify that the Quality Management System of

BELDEN

2500 Braga Drive, Broadview, Illinois 60155

Has been assessed by EAGLE Registrations Inc. and conforms to the following standard:

ISO 9001:2008

Scope of Registration

The Design and Manufacture of Universal Joints and Complete Shaft Assemblies for various industries including Industrial and Specialty Vehicles, Aerospace, Military, Packaging/Converting & Conveying, Food Processing, Steel Processing and Leveling, Industrial Machinery, and Woodworking Equipment.

Chief Technical Officer

This is a legitimate ISO 9001 certificate. It features the logo of the registrar, as well as that of the accreditation body. You can thus check with either organization to verify the truth of the certificate.

Know the Auditor's Playbook

Registrars are accredited to ISO 17021. It's a good idea to buy the standard and read up on it so you know when the CB violates the rules… which, unfortunately, will be a lot. This isn't necessarily because the auditors are cheating, but rather that the individual auditor was never trained on this properly. In other cases, their desire to "make friends" with you (and keep your business) overrides their objectivity, and gets them into consulting, which is disallowed.

If you know ISO 17021 ahead of time, be sure to tell your selected registrar that you expect the home office and the assigned auditors to stick to those rules, and that you will send (polite) complaints when they don't.

You can buy a copy of ISO 17021 here.

Hiring Local Is Bad Advice

Unfortunately, most companies attempt to hire "a local guy" to conduct audits, under the thinking that this saves money. It's not always the case, since often a local auditor may be flying in from another client across the planet, and you have to pay their airfare anyway. But most of all, the focus on hiring a local auditor denies you the ability to hire the best auditor. If you get a bad auditor who routinely saddles you with bogus audit findings, it can cost you far more than the travel expenses ever would.

Understand the Pricing

auditdaysThe going rate for ISO 9001 audits is $1200 a day, and for AS9100 or other specialty certifications, as high as $1350. The number of audit days is generally based on your employee count, illustrated by the table at right (for ISO 9001 only — additional days are required on top of the ISO 9001 days, for standards such as AS9100 or ISO 13485.)

You will sign a 3-year contract with a registrar, but don't panic. You can cancel at any time, and you only pay for what you used. The three-year contract is just so you have a firm end period, and a chance to reconsider your relationship with the CB at the end of that three year period.

A three year contract will consist of:

- Application fee (normally waived if you ask) – normally about $500
- OASIS fee (for AS91xx only, cannot be waived) – $500- 600
- First year's initial audit days (see table)
- Second and third years' surveillance audit days; surveillance audits are shorter than the initial audit (see table)
- Expenses: travel, hotel, rental car, etc.

If you sign a follow-on contract after three years, you don't start over, but instead undergo a "Recertification Audit" which is about 2/3 the number of days of your first year's initial registration audit. This is normally true even if you switch registrars, but not if you are doing so to "get out of" any existing nonconformities with your previous one; the new guys will check, so don't try it.

The first year will be the highest of the contract, because the initial audit is the longest. using the table at right, calculate the number of days and multiply by $1300 (a good average), then factor in expenses. When you receive a quote from a registrar, and you see the numbers are wildly different, you must be on guard. Occasionally an registrar may "low ball" the audit days, which is not allowed and could get both you and the registrar in hot water with the accreditation body. Or the CB may sense a "dupe" and jack up the price unrealistically.

A few caveats: the number of audit days may deviate from the table above depending on a few other factors. The following may result in less days required:

- If you take any clause exclusions (such as design responsibility)
- If you have a large number of people doing one task
- On the other hand, these factors may result in a higher number of audit days:
- You have multiple sites, geographically spread out
- You have a complex management system, perhaps integrated with other standards
- You are in a highly regulated industry, such as medicine or food, which requires additional time to consider regulations

Check the Fine Print

As we said, most accredited registrars will have similar prices. This means that most auditor quotes will be similar, so you will need to check more than just the day rate, since some CB's will want to sneak a few extra dollars in through a side window.

Look for bogus "application fees" (you can usually get those waived just by asking) or per diem expenses. You should pay hotel, rental car and travel… and that's it. If the CB is going to charge you for every trip to the minibar, find another registrar.

Consultant Recommended a Registrar? Be Careful!

Often your consultant will recommend a third party registrar. At times this can be helpful, since some consultants have a great deal of experience with the various certification bodies. But at times this could be the sign that the consultant has a secret "handshake deal" with the registrar, where they swap favorable audit results for leads. This doesn't help anyone, and just promotes corruption in the ISO certification scheme, and must be avoided at all costs.

If your consultant is being particularly heavy-handed about recommending a single registrar (or individual auditor), take care. A good consultant may provide you some recommendations, but should offer at least three, and allow you to contact their clients to discuss the suggested registrars' performance. A really good consultant won't recommend any registrars at all, and only advise you on how to ensure you have an accredited certification body.

Quid Pro Quo: Registrar Recommending Consultants?

The opposite is also true: more and more, registrars are recommending consultants. This is usually a red flag that indicates the CB has an improper relationship with some consultants, usually those that in turn bring their consulting clients to the registrar. While there's no cash exchanging hands, there is a financial quid pro quo in effect.

For now, the Accreditation Bodies are not cracking down on this behavior, since it's being done by some of the biggest CBs in the world. But you will want to be wary no matter what. If a registrar has a "preferred consultant" or "consulting business partner" program, you may want to tread carefully with that registrar, even if they are accredited.

The best registrars maintain a strict firewall between themselves and consultants.

The Registrar Is Not Your Friend

Forget any notion that you will build a “relationship” with your CB. Their sales people will tell you this, but it’s code for, “I want a lifetime contract.” Ultimately whatever the sales person says is pointless, because the final measure of a registrar is your interaction with the assigned auditor. And their job is to assess you, not make friends. The auditors, too, may try to befriend you, but don’t let them, as it just leads to problems later. Remember you are hiring someone to assess you, which may mean giving you bad news. Approach the selection of a registrar objectively, and don’t let feel-good marketing spin knock you off of critical judgment.

Ensure A Fair Registration Audit with These Contractual Obligations for Your ISO 9001 Registrar

YOU ARE THE BOSS. *NOT YOUR REGISTRAR.*

ISO 9001 certification bodies (CBs, or "registrars") are subject to the rules of ISO 17021, the standard that defines what CBs must do to become accredited. CBs are audited annually by their Accreditation Body (AB) who is tasked with ensuring they comply with ISO 17021. Unfortunately, ABs are paid by their CBs, so overlook most violations, since enforcing the rules would impact on their revenue. Furthermore, most ISO 9001 end users do not even know of the accreditation rules, even though their intent is to protect the auditee and ensure an objective, fact-based audit.

In a survey[1] of over sixty US ISO 9001 registered companies, six of the top ten most common concerns with registrars were related to various failures by the CBs to abide by the requirements of either ISO 17021. Specific violations included failures of the CBs to abide by audit schedules, failures to record evidence on nonconformance reports, making auditees uncomfortable and prescriptive auditing styles by auditors. In a single 2013 incident, a poor audit by an accredited CB had been witnessed by the company's customers, and resulted in the company having its risk rating increased, causing it to lose out on a billion – ***with a "b"*** --- dollar contract. Layoffs resulted, and real people lost their jobs, not because of inadequacies of the client's QMS, but because the inadequate CB auditing led the customers to question the validity of the certification.

It becomes valuable, therefore, to ensure that an organization's registrar is abiding by ISO 17021. That means you should not only purchase a copy of ISO 17021 (from ISO or your country's ISO member body) but also understand it.

But if registrars are already required to abide by ISO 17021 and, as the survey suggests, simply not doing so, what can be done? Another requirement of ISO 17021 is that registrars maintain a robust complaints handling process; this becomes a critical tool for reporting ISO 17021 disconnects with the registrar. Unfortunately, ISO 9001 end user organizations are often too timid about filing complaints with registrars. Evidence bears this out: of some 50,000 registered companies in the US, the ANSI/ASQ National Accreditation Board (ANAB) only receives a dozen or so complaints per year, according to data posted on www.ANAB.org. That's not even possibly accurate.

Clearly, waiting for the registrar to break the rules, and then reporting it, is not palatable to most companies. It is not particularly fair to the registration companies, either. Instead, it is important to invoke key points within ISO 17021 beforehand, to ensure that the registrar intends to stick to the rules, and to provide a pre-established baseline for resolving issues that may arise later. Remember, ISO 9001 requires companies to fully define their requirements to vendors, and registration companies are vendors. ***You have the right to assess your CB as any other supplier, and then hold them accountable when they fail to uphold their requirements.***

ISO 17021: YOUR NEW BEST FRIEND

[1] Conducted by OQRI in 2006. A similar study was conducted of 50 companies in 2013 and found identical results.

ISO 17021 assumes a model that is antithetical to how most people view the ISO 9001 registration audit process. The 17021 standard puts the end user of the audit – the auditee – in control of the entire audit, not the auditor. CBs will say that this is the way it *should* be done, but day-to-day practice and real world experience tell us a different story. Instead, clients sign up with a registrar and then let that CB drive the audit process. The client accepts the auditor's schedule without question, sits back during the opening meeting, and passively participates in the audit by fetching information and individuals to suit the auditor. They even run around and get coffee.

Tip: show the auditor where the coffee machine is. If an auditor can't get his own coffee, the rest of the audit is only going to go downhill.

It is necessary for the organization to establish control at the very beginning, before a contract with a CB is even signed. When deciding on which registrar to use, organizations are encouraged to make their intent to enforce ISO 17021 known, and to clearly spell out their expectations for audits. It should – theoretically – be impossible to find an accredited registrar who ***refuses*** to follow ISO 17021, but in the event that one encounters such a company, it is best to let them know they can get their business elsewhere. Enforcing ISO 17021 ***enhances*** objectivity and fact-based auditing, and reduces opportunities for miscommunication, complaints or arguments; registrars should respect this reality, especially since it is part of their accreditation requirements.

EASY RIDERS

When a company signs on with a registrar, the CB will require the company to sign a contract. The registrar's typical contract will include a lot of language on what your company must do, but rarely do these terms and conditions include language on what rules or requirements the registration body itself must abide by. Therefore, the contract becomes the easiest means by which to transmit your company's wishes. By developing a contractual rider – one that becomes part of the purchase order agreement with the registrar, and takes precedence over any "stock" language in a CB's existing contracts – you ensure you have properly transmitted your requirements to the CB. And – the best part – ***it is legally enforceable.***

Citing specific ISO 17021 requirements is critical. The contractual language should include the following general requirements:

- □ The CB agrees to adhere to the requirements of ISO 17021 during all audits and activities conducted with our organization.
- □ The CB acknowledges that the audit scope, objectives and processes are to be defined by our organization's selected representative.
- □ The CB agrees to notify our organization in writing if and when these requirements conflict with established rules under ISO 17021, to the extent that such requirements would invalidate or threaten the validity of the audit or resulting certification.

The last sentence gives some power back to the registrar, because it is conceivable that a company could begin issuing so many requirements on the CB that the audit itself no longer meets the necessary

criteria for a legitimate audit. In such cases, the rider language puts the onus on the CB to define and defend such cases.

In additional to general language, some specific citations of ISO 17021 are in order. These seek to address many reported disconnects between auditor behavior, CB management or other issues that could hinder an effective audit. The first thing is to establish a scope of the audit, and define it clearly in the contract:

- □ The CB agrees to limit its activities to the following scope of the audit:

Your audit scope is not the same as your scope of business (or scope of certification) but is the overall set of parameters of the audit itself. It should include the following information:

- □ Sites included (if not all)
- □ Departments included (if not all)
- □ QMS Processes included
- □ Standards to be used
- □ Clauses to be excluded (per the permissible allowances defined in the standard)
- □ Languages to be used (in reports and in verbal communication)

Regarding the processes, it is a recurring complaint that CB auditors do not abide by the processes as defined by their customer, but instead use process breakdowns they have developed ahead of time, usually in worksheets they have made that divide the ISO 9001 clauses into logical chunks, making their jobs easier. When these don't align with the actual processes of the client, the auditor will usually just defer to his/her own list. This is not allowed. The CB auditor must audit to your processes, not his/her own. To ensure they comply with this, therefore, you must provide your process breakdown to the auditor ahead of time. That's only fair. If the auditor nevertheless ignores your process structure, and audits against his/her own idea of what a process is, now you have legal grounds to enforce your rights.

Your contract should also include a statement on the scope, or activities that are ***not*** to be included in the audit:

- □ The CB agrees to not engage in auditing of any of the following activities which are deemed out of the scope of the audit:
    - Safety issues unrelated to the safety of the auditors themselves [2]

[2] Safety is a particularly common, and problematic, issue that comes up during audits, typically defended by the auditor as being an extension of "statutory or regulatory requirements." We often see CB auditors write up safety issues if the quality system documentation makes the most passing reference to OSHA, for example; however, such citations are clearly out of the scope of the audit and could lead the CB into litigation. For example, we have seen cases where QMS auditors write up findings on the control of SDS records; however, the Federal labor laws governing the content and use of SDSs are complex, and there are certain elements of the ISO 9001 document/record control requirements which could actually put a company ***in noncompliance*** with the law, or (worse) risk a catastrophic incident affecting worker health. Clients hire the CB for its expertise on quality systems, and do not typically vet the auditor for their expertise in occupational health, industrial safety, or the laws behind either. Furthermore, we know of no accredited

- Accounts payable
- Employee personal protected information or data
- Union rules
- Activities or processes not included in the scope of the quality system

KNOW YOUR AUDIT OBJECTIVES

Once the audit scope is determined, the audit objectives must be determined and defined. This is a concept that is routinely ignored by CBs who typically establish the objectives for the auditee by assuming what they want. This is backwards, of course. The organization must tell the registrar what it wants; no company, CB or otherwise, should ever assume customer requirements.

Objectives should include a plainly-stated goal for the audit, and detailed definitions of the types of acceptable outputs for the audit. Here are some examples:

□ The CB agrees that the objectives for the audit are limited to the following:

- Audit of our organization's quality management system against the standards listed in the Scope (above) for the purposes of obtaining/maintaining registration to those standards.
- Auditing in accordance with the other conditions defined in Scope (above)
- Written reporting of nonconformities between the QMS and the requirements listed in Scope (above)
- Written submission of a completed audit report in accordance with the CBs normal format, to be submitted to our organization within *(x)* number of weeks.
- Written reporting of opportunities for improvement, where such opportunities are discovered by the auditor so long as such opportunities are constrained to the Scope (above).
- Documented statement of recommendation or denial of recommendation for registration to the standards listed in Scope (above) to be provided upon the close of the audit.
- Approximate date(s) for any surveillance or follow-up audit activities.

MISCELLANY IS GOOD FOR THE SOUL

The end user organization should also provide the CB with a detailed listing of other expectations and requirements, all of which are enforceable as part of the purchase agreement.

registrar that provides training of their QMS auditors on safety… nor are they required to. Finally, auditing of safety issues takes valuable time away from auditing things that are in scope. CB auditors should be strongly discouraged from writing safety issues up during a quality management system audit, unless this is agreed to in advance of the audit, or unless some compelling evidence can be provided by the CB that proves otherwise.

- □ The CB shall use as its point of contact the following authorized representative of the organization: [name and contact information of representative].
- □ In the event that the authorized representative is not available, the following secondary representative is to be used: [name and contact information of secondary representative].
- □ The CB acknowledges that its audit activities are to be conducted in accordance with ISO 17021.
- □ The CB agrees to the definitions of terms as listed in ISO 17021 and ISO 9000.
- □ The CB agrees to the principles of auditing as listed in ISO 17021.
- □ The CB shall provide to our organization a written proposed audit schedule, defining which clauses and processes are to be audited on which dates. This schedule must be received at least two weeks before the first audit day.
- □ Our organization reserves the right to review and revise the proposed audit schedule so that it better aligns with our organization's specific processes and process approach, provided that such revision does not invalidate the scope or objectives of the audit.
- □ The CB agrees that exchange of documentation for the purposes of documentation review may be done electronically.
- □ The CB agrees to populate its audit team with auditors knowledgeable in our industry, SIC codes and the standards listed in the Scope; where such auditors are not available, the CB shall request a waiver for this requirement in advance.
- □ The CB shall provide our organization with the credentials, certifications and/or resumes of its proposed audit team members within sufficient time so that our organization may request alternate auditors if we deem a selected auditor is not adequate.
- □ The CB shall not send auditors, trainees or observers who have not been pre-approved by our organization, with the exception of witness auditors from the CB's accreditation body.
- □ CB auditors agree to act in accordance with the requirements of ISO 17021, and refrain from actions which may be seen as combative, argumentative, intimidating or in any other way counterproductive to the audit process.
- □ CB auditors agree not to be prescriptive in their auditing technique; i.e., to infer or require the implementation of specific methods for compliance.
- □ CB auditors agree not to make conclusions or assumptions about our organization's quality management system on the basis of previous experience.
- □ CB auditors agree not to provide consulting during audits in any form, whether by providing specific solutions, or by providing examples of concepts the auditor has seen at other companies.
- □ CB auditors agree not to disclose to any other client or third party any intellectual property, whether viewed visually or through documentation or other means, without explicit written

permission from our organization, regardless of whether the CB auditor does so without naming our organization specifically. Transmission of our intellectual property and confidential information is protected by law, and will be vigorously enforced.

- □ The CB agrees to acknowledge the full responsibilities and authorities of company representatives selected by our organization as escorts, points of contact, authorities and representatives during the on-site audit activities, including any contract personnel so assigned by our organization. The activities of these individuals shall be in accordance with the requirements of ISO 17021.
- □ The CB agrees to provide a written report of the Stage 1 portion of the audit *(x)* weeks/days prior to the first day of Stage 2 activities. This report must list specific nonconformities or concerns found during the Stage 1 event, in accordance with the nonconformity reporting requirements below. Failure to provide this report within the allotted time may result in our organization rescheduling the Stage 2 activities at the full expense of the CB.
- □ If the audit activities result in a recommendation for (or maintenance of) certification to the standards referenced, the CB agrees to provide this certificate within *(x)* weeks of the last day of the on-site audit activities.

THE RIGHT WAY TO WRITE WRONGS

The writing of findings, especially nonconformities, continues to be a problem reported by ISO 9001 end users. Many times, CB auditors write nonconformances that "make sense at the time" but which cannot be comprehended later, after the auditor has left. This is because some auditors have gotten into the habit of writing the finding one way, and then verbally explaining it and adding context during the closing meeting. This practice, however innocent-looking, is a severe violation of ISO 17021 which requires that auditing be an "evidence-based" activity and that findings be verifiable.

Another bad practice is illustrated when auditors write a finding beginning with the phrase "there is no objective evidence that…." Auditors routinely write findings with this preface when they do not – or cannot – find evidence to prove compliance to a requirement. However, it must not be overlooked by the auditee that this means the auditor cannot find evidence to *disprove* it either. Imagine the district attorney who prosecuted criminals on the merits of having ***no*** evidence.

There is no allowance for writing up the ***absence*** of evidence as a finding. If the auditor has not found evidence, this does not mean there is a nonconformity; it means, rather, that the auditor stopped following the audit trail prematurely. In the end, any finding written up with the words "there is no objective evidence" is an admission by the auditor that he/she did not do their job. Such audit findings should be rejected by the auditee wholesale.

The industry expert coalition ISO 9001 Auditing Practices Group, founded by ISO and IAF, agrees. In a recently released guidance document on the writing of nonconformities, APG wrote, "If there is no audit evidence, there is no non-conformance."[3]

[3] http://www.irca.org/inform/issue7/APGnon-conformity_reports.htm

Instead, auditors must corroborate ***each*** finding with evidence. In order to ensure this, the following language should be included in the contract with the CB:

- When writing findings, the CB must adhere to the following convention:
    - Clearly record the nonconformity
    - Indicate the clause under which the nonconformity falls
    - Clearly state the objective evidence that supports the nonconformity
    - Indicate whether the nonconformity is a major or minor, using definitions of those terms as defined by the CBs procedures
    - Review the nonconformity, and revise as necessary, to ensure that it is written in a way that is verifiable at a later date without any further request for information.
- Findings that do not follow all the requirements of this convention will be considered to be nonconforming against ISO 17021 and rejected by our organization until corrected
- If a finding cannot be corrected by the auditor upon such a rejection, the nonconformity will be voided.
- The rejection of findings under these conditions shall in no way delay or hinder the receipt of all other objectives, including certification to the applicable standards, if applicable.
- Signing of nonconformities during the CB audit shall constitute acknowledgment of the receipt of nonconformity, and shall not be construed as acceptance of the nonconformity, nor shall it negate our right to appeal the nonconformity. This rule shall trump any language present on the CB's nonconformity form where such language contradicts this clause.

Once again, this may look ominous to a registrar (or their legal department!) but should pose no obstruction to their ability to provide your company service, since this convention follows the requirements of ISO 17021.

COTO Interruptus: The Missing ISO 9001 Clause on Strategic Direction

*[The following is a full chapter excerpted from the book **Surviving ISO 9001:2015** by Christopher Paris. The book is available for purchase at* www.survivingiso9001.com*.]*

If you recall, I mentioned that the entirety of the COTO Exercise was building up to the development of a "strategic direction" for the company. No, there really isn't a clause 4.5 in the standard, and technically, ISO 9001:2015 makes no firm requirement for a strategic direction at all, but instead keeps talking about it as if it were part of a movie prequel you had already seen. Specifically, ISO 9001 name-drops this concept in five places:

0.3.1 The Process Approach: "*The process* [should] *achieve the intended results in accordance with the quality policy and strategic direction…."*

4.1 Understanding the Organization and its Context: "*The organization shall determine external and internal issues that are relevant to its purpose and its strategic direction…."*

5.1.1 Leadership & Commitment: Leadership and commitment shall ensure *"that the quality policy and quality objectives are … compatible with the context and strategic direction …."*

5.2.1 Developing the Quality Policy: The quality policy must be *"appropriate to the purpose and context of the organization and supports its strategic direction."*

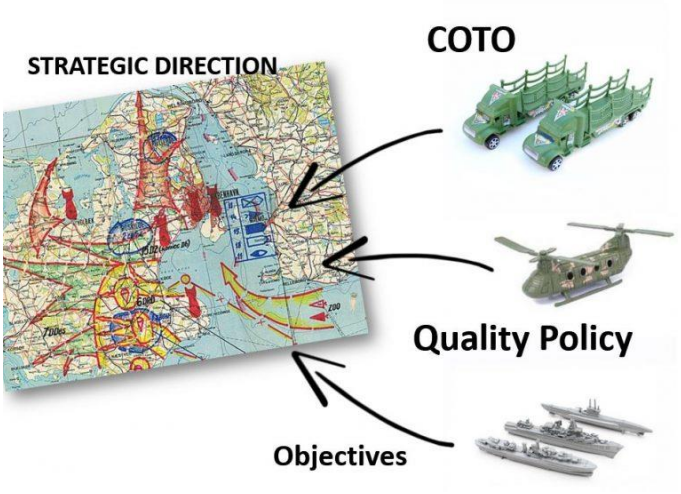
9.3.1 Management Review: "*Top management shall review the organization's quality management system … to ensure its … alignment with the strategic direction…."*

Summarizing, ISO 9001 thus invokes this idea of a "strategic direction" by suggesting the strategic direction be considered five times:

1. … when identifying processes
2. … when identifying the issues of concern (during COTO Exercise)
3. … when developing the quality policy
4. … when developing the quality objectives
5. … as a metric to measure the overall QMS against during management review

So, if you need to have a thing in order to conduct five required steps, it helps, therefore, to ensure the thing ***actually exists***. Having said that, since it's not a mandatory requirement, this means it can "exist" any way you'd like, even as a set of cohesive thoughts held by the top management and communicated verbally.

SpaceX had the most elegant strategic direction; when moving from an R&D house to a full production company, Elon Musk's edict was summed up in two words: "forty cores annually." This meant everything was adjusted to target a production goal of forty rocket cores per year: production capacity, engineering throughput, plant layout, staffing, budgeting… every single thing the company did was redesigned to "hit" the forty core mark. When asked, anyone in the company could recite a single goal – "*forty cores*" – and then go on to elaborate on how it affected them, in their particular department or function. Simple, elegant, and it worked.



But, as usual, SpaceX may be an outlier. Reducing your strategic direction to two words wouldn't work in most companies. So, most organizations have far more complicated strategies: perhaps to expand in one market while getting out of another, or to grow the business by 50% in a five-year period. If that sounds a lot like a quality or process objective, that's not by accident: the strategic direction should ***inform*** the development of the quality objectives, after all.

The strategic direction isn't binding; it's going to change over time. For SpaceX, once they've mastered "forty cores" it's likely Elon will issue a new strategic direction statement, and it will probably be "get my ass to Mars." So these things do change, and it's not written in stone. I do recommend writing it down, though, and my best recommendation is to put it in the records of Management Review, which we will discuss in section 9.3.

I've found, however, that some executives don't want their plans written down for general consumption by the company employees; one of my clients was pursuing ISO 9001 as a means of making the company more attractive to potential buyers, so his strategic direction was "to sell the company." He didn't want employees to get terrified and quit *en masse*, so he kept this very close to the vest. In such cases, it's fine if the executive writes it down and keeps it private; there's no requirement the direction be publicized or even communicated. In such cases, it's the top management's job to ensure the direction is being met, even if the employees don't know what it is. It's a good idea to have it written down, though, if only to show an auditor, in private.

So while it's not a firm requirement, developing the strategic direction – and ensuring those five points above align with it – is a critical step in developing an ISO 9001:2015 quality system.

Great Third-Party Sources of Info to Support the Trickier AS9100 Clauses

AS9100 Revision D adds a few new requirements that are confusing to some users. Here are some invaluable third-party sources of information and support which can help you address the more complicated and unusual AS9100 clauses.

Counterfeit Part Control

The Rev D standard introduces its most major change by adding requirements to prevent the use of counterfeit parts. The standard doesn't explicitly specify what it's talking about, but industry experts know that it means two things: counterfeit electronic components (resistors, ICs, capacitors, etc.) and counterfeit materiel (not a typo, "materiel" is a military term referring in broad terms to metals, plastics, raw material and hardware.) The following sources can help:

- **Two Critical Standards:** I recommend you purchase and download either (or both) of the following standards, depending on the scope of the materials you use and your industry:
    - AS5553 "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition"
    - AS6174 "Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel"
- ERAI: this is the world's number one source for news, information and updates on counterfeit parts, including reports on counterfeit parts found in the wild; it's focus is electronic components. As a result, it's a critical source of information for those monitoring their supply chain and internal inventory. ERAI now offers some fantastic, role-focused training on counterfeit part control through its new Intercept program; each course of which is short, web-based, and targeted at specific employee positions, helping them learn how to identify counterfeit parts in real life.
- Henry Livingston's Blog: Henry regularly provides news on updates to FAR/DFARS and counterfeit product updates.

Organizational Knowledge

ISO 9001:2015 added a new clause on "organizational knowledge," so users of both "vanilla" ISO 9001 and its aerospace neighbor AS9100 will get use out of these next suggestions. The clause is a diluted, reductive nod to "knowledge management" (or "KM") which itself is a rich field of study on its own, and worth looking at in greater details. To learn more about KM and to get more value out of this otherwise confusing clause on organizational knowledge, try:

- RealKM – fantastic source for free articles and in-depth studies on the KM field and approaches you can use right now.
- KM Institute – they sell certifications, which is usually a red flag (do we really have to become certified in *everything*?), but do have some training programs and other materials you may find useful.

Configuration Management

"CM" is a complex discipline affecting product design, identification and technical documentation, and one which is often overlooked by anyone other than large aerospace companies with mature in-house engineering staff. But the AS9100 standard imposes it on everyone, including those tiny machine shops that may have a toe in the water of design. As a result, some third party training may be needed. Be careful, because the software engineering and CMMI worlds offer a lot of material on CM, but this isn't always the same as what you would need for AS9100 compliance, especially if you're a hardware manufacturer.

- CMStat offers some training courses that will get you up to speed on this concept, without offering 1,000 dubious "personal certifications" that so many other training providers throw at you. They also offer related CM consulting.

FOD – Foreign Object Debris/Detection/Damage Control

Blink and you'll miss it, but clauses 8.1, 8.5.1 and 8.5.5 mention the need to control foreign objects. It doesn't call out a need for a formal "FOD Program," but nevertheless that's essentially what AS9100 expects. The good news is that FOD programs can be scaled up or down, based on the complexity — or simplicity — of your QMS processes, so it's not something to panic about.

- FOD News – this is the number one source for FOD news (if you're into that sort of thing) but more importantly, they publish the absolutely fantastic "Ultimate FOD Prevention Program Manual." I have a dogeared copy on my desk for 15 years or more, now, and it's never let me down. They also offer training videos and the usual FOD posters.

ITAR / EAR / Export Controls

While ITAR is not named at all in the standard, AS9100 does require you to adhere to customer's requirements and related statutory and regulatory requirements. As I've written, ITAR and EAR are being flowed down to the entire supply chain these days, and this can be a daunting and intimidating task. We've got you covered, however.

- Aerospace Exports Inc. – the export experts at AEI can help implement an ITAR/EAR and overall compliance control program in only a few days, if you're willing to do the necessary study of the regs afterwards. They will help put the documentation and methods in place, and then offer support afterwards. Since failure to do so can be a felony, you'll want to make sure your ITAR program is legit, and fully implemented. Best of all, AEI's services are ***not*** expensive, and nearly any company will find room for this in its budget.

Everything We Thought We Knew About ITAR Is Wrong

I'm going to admit this. A few weeks ago, I was ambivalent about ITAR, the International Traffic in Arms regulations, and often literally dismissed it by telling clients "you can download a free manual off the internet and call it a day." A few days later, I basically shit myself after finding out how horribly, horribly wrong I was.

Ignorance is not bliss, not when it comes to ITAR. Ignorance is, instead, the cold steel of handcuffs on your wrists as guys in windbreakers with big yellow letters on the back drag you kicking and screaming into some godforsaken pit for the rest of your life. Simply put: the fact that you don't know about ITAR means you are probably, right now, a felon.

What's worse, is nearly everyone reading this thinks they understand ITAR, and they are sniffing indignantly at any suggestion to the contrary. They also think "it's not that big a thing," after they downloaded a generic ITAR manual off the internet, and put in a "visitor sign-in log" on the receptionist's desk. They don't know what they don't know, and it's terrifying.

Oxebridge fans know I am not given to fear tactics or hyperbole, unless telling you how wonderful I am; then there isn't hyperbole enough. But when I sell ISO 9001 I tell the truth: it's not easy, but it's also not the scary and expensive journey that some consultants would have you believe. The truth is somewhere in the boring, non-hyperbolic middle. I recoil at consultants who sell ISO 9001 on the basis of scaring the death out of people: "if you don't get ISO 9001, your customers will take their business elsewhere!" or "if you don't hire a consultant, your quality system will stink of fish and kill all the children in your towns and villages!"

But ITAR. Good lord, ITAR.

I'm a Felon, You're a Felon, We're All Felons!

During my last AS9100 Braindump in Cocoa Beach, you may know I shared the stage with representatives of ERAI — who spoke on counterfeit part controls, something I will address in an upcoming article — and Aerospace Exports Inc. Mark Stevens of AEI went over the application of ITAR, as well as EAR, FARs and DFARS, in an AS9100 setting. The Stevens bit came after I had already spent about 10 hours of the 2-day event making an idiot of myself by joking about AS9100, Godzilla movies, Eddie Izzard transvestite comedy routines and making exactly 300 inane pop culture references that nearly no one understood. In between, we learned a little about AS9100 (one hopes.)

Then Stevens got up, and scared the living shit out of everyone. We know this because the shits he scared out of us were literally alive: they got up, left the room, and immediately stormed into the local DMV to get drivers licenses so they had legal documentation to vote during the next election. Now it wasn't Mark's presentation style that frightened us; not at all. He was friendly and lively and engaging. But he also told everyone the truth, and we walked out like vampire victims, all gone sheet-white, the blood drained from us. Let's just look at a few truths about ITAR, but be prepared to watch your shits march to the DMV and later vote for the exact party you hate the most.

No, You're Not Certified. You're *Targeted*.

First of all, and perhaps most importantly, get it out of your head that the Department of State — or anyone — issues an ITAR certificate for your company. There is no such thing as being "ITAR certified," and the minute you put that bogus logo on your website, you are telegraphing to everyone — including the guys with windbreakers and handcuffs — that you're probably violating ITAR, not complying with it. It's the arms trafficking equivalent of a pothead rolling past the cops with smoke coming out his windows and a 3-foot wide pot leaf decal on the back of his '72 Camaro while he plays reggae and asks directions to the closest place to buy a new bong.

You see, you actually get registered with the Department of State, who then puts you in their system. You're now being watched. It doesn't mean the DoS has certified you, nor verified compliance in any shape or form. It means you have identified yourself to the US government as a potential handler of material or information subject to ITAR export controls, and which must then be controlled to prevent misuse by a bad actor. Not doing so may temporarily keep you off of DoS' line of sight, but then if you're caught dealing with ITAR products things are much, much worse because you've been operating illegally. Registering your company keeps you legal, but also alerts DoS that you exist, and thus they start watching. Choose your hell wisely.

Next, it's likely you will be faced with this reality very, very soon. Recent expansion of related regulations has forced OEM's and other defense contractors to flow ITAR down not just to their 1st or 2nd tier suppliers, but everyone at every tier. And the deadline for this has already passed. So already, Oxebridge clients are finding themselves receiving a rash of ITAR flowdowns they had never expected, and suddenly have to comply with. It's a perfect storm.

But Wait, There's More!

I'd love to promise some good news in this mess, but alas, there's none to be found, other than reading this article may save you from being hauled away in iron and fed to crocodiles at Gitmo. Because things get much, much worse.

If you thought you complied with ITAR, I can say with near 100% certainty, you are absolutely wrong. See that visitor sign-in sheet on the receptionist's desk? The one that invites guests to indicate "Y" or "N" to the question "US citizen?" ITAR assessors call these "death logs," because as soon as they see one, they know you're dead. Metaphorically, that is. This is because the organization must have a "record of screening" when they check "N." As recently as two weeks ago (as of this writing) I saw a client's ITAR log with numerous "No's" filled in, and nearly 100% of the visitors checked "Yes" when asked if they had recording equipment on them (cell phone cameras.) The client had no controls in place for these situations. Dead.

Here's an easy one: have you maintained a record that your ISO 9001 registrar auditor is a US person? There are few people who have the level of unprecedented access to ITAR controlled documents than your registrar, and yet most companies allow the slovenly auditor to roam around the plant without so much as a sign-in. Ironically, the very same auditor who is tasked with ensuring you are complying with related requirements is likely violating them, and you're complicit. It's not like your CB is going to invest in even 30 seconds of ITAR training for their auditor pool.

So you let the UPS or FedEx guy roam freely and use the company bathroom? Congrats, you're going to jail, you filthy felon. If you didn't carefully watch what the driver was doing, you can't know for sure he didn't engage in some ITAR-prohibited action while you weren't looking, like picking up a blueprint, or snapping a few shots of something with his cell phone. And if you can't know for sure, you can't really claim to be ITAR aware. You're playing Russian roulette with five bullets loaded, using a gun that only has four chambers. (It's a Russian gun, I guess. I dunno.)

Now say your sales guy flies out of the country for an international sales trip, and has customer emails on his laptop that have ITAR controlled drawings in them. If he simply loses control of the laptop for a moment — say, by leaving it in his hotel room while he's at the bar, and that maid with the weird accent cleaned the room while he was out — you violated ITAR. Go, again, to jail.

You printed those technical files from the hotel printer right before the big meeting? Well, guess what: those printers are not secure, their memories can totally capture whatever is printed (and do so by default), and just yanking the USB drive out doesn't do squat. Go to jail.

What's that? You've joined they "Yay, Cloud" movement, and have all your important files backed up on Google Drive, MS OneDrive, or even Carbonite? If you can't be sure how that backup traffic works — meaning knowing what countries it travels through in order to get between you and the storage dump — you're screwed. Worse is if your company server physically resides outside the US, which is more common than you'd think. Jail.

(Some services, such as Iron Mountain, offer ITAR compliant backups, meaning their services are located within the US and have DoS compliant security controls. To be sure, ask your cloud backup provider, and if they don't offer an ITAR compliant service, get your data off immediately.)

If you think we've hit the Ninth Circle of Hell, Dante Alighieri has much more to show you in the ITAR Divine Comedy. Inspectors tasked with assuring ITAR compliance among registered companies have lots of tricks they use. For one, if they know a company is ISO 9001 or AS9100 certified, they likewise know the company staff is used to being audited. DoS will send in a contract assessor who goes in through a back door, dressed in a nice suit and carrying a clipboard, and who then walks up to the first machine operator they see. "I'm doing an audit, can you show me that print there?" they ask. If the operator doesn't question their authenticity — and what machine operator would? — well, you've got yourself a violation. If you think I'm kidding, I'm not. (In fact, test this. Have a friend dress in a suit one day and walk around the plant, to see if anyone questions them. Watch how blabbermouthed your employees get, thinking they are being helpful during an audit.)

How about this: your facility's in-house cameras are operated and monitored by some third party security firm, and the cameras are dutifully hovering over the machining area, or engineering cubicles. Congrats, you've got people of unknown origin, working for the security firm, able to capture and record design data for your ITAR sensitive parts, just by using the zoom lens.

Then there are the boneyards, those hastily constructed areas outside your plant where you dump all your scrap or random parts you made from 10 years ago but still haven't discarded. You put a chain link fence around it, and maybe even some barbwire. Who cares? With nothing more than a thick blanket I can get over that barb wire without a scratch, and rifle through all your allegedly "secured" ITAR parts.

And ITAR is just the tip of the iceberg. EAR (Export Administration Regulations) invokes a whole bigger set of requirements, having to do with a broader range of products other than the "weapons-focus" of ITAR. Federal Acquisition Regulations (FAR) clauses, and their DFARS defense industry cousins, invoke even more such requirements. Right now the US government is flowing down new cybersecurity requirements to the entire supply chain, forcing companies to update their IT activities to ensure ITAR and such records can't be hacked or leaked.

The shift in environment comes (again) from the fact that the US government is now aggressively flowing these various requirements down to everyone, regardless of size. Previously, a ten-man machine shop didn't have to worry much about this stuff; now they do, and the Dept. of State won't weigh their response to violations on the basis of the size of the company.

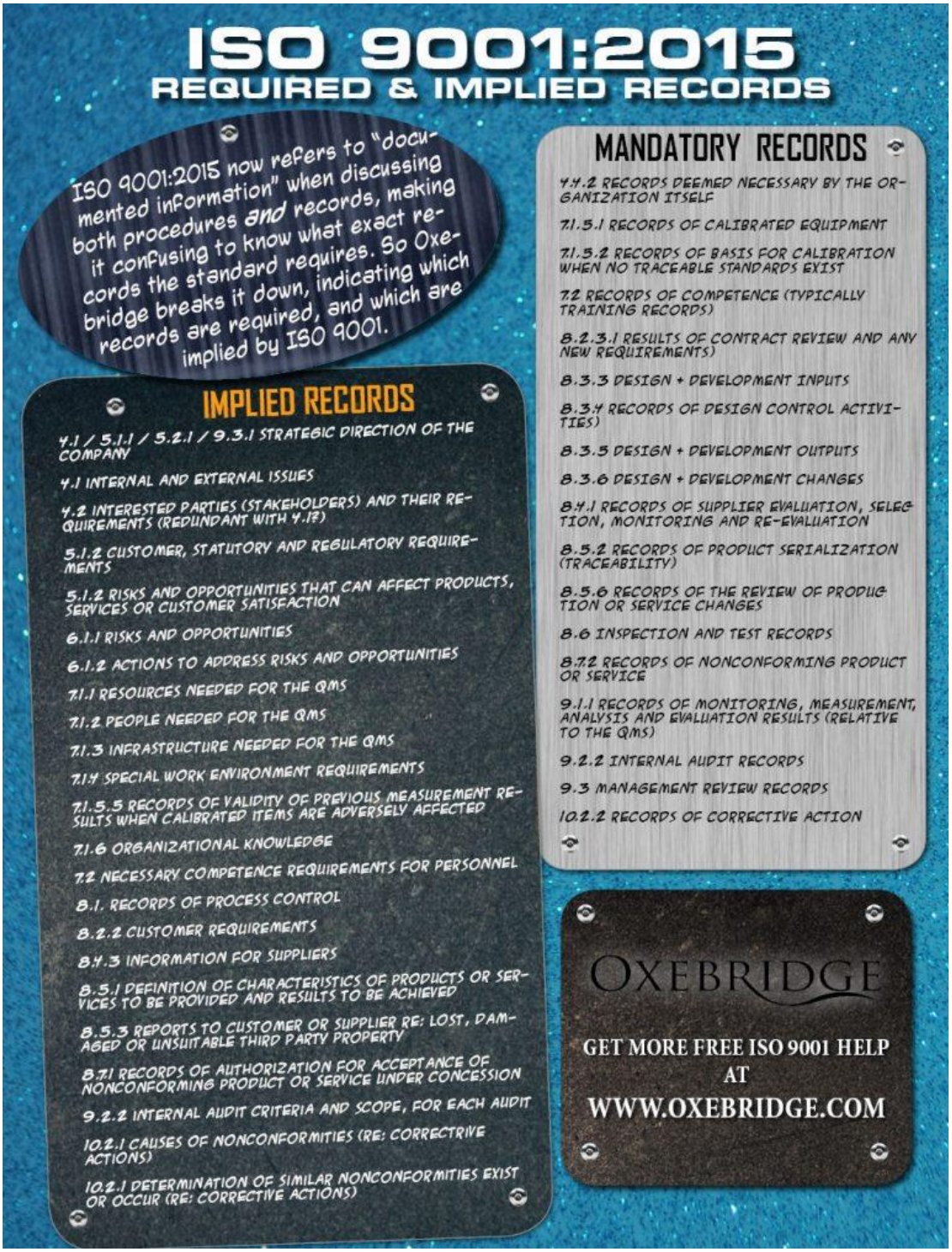
It's likely you've been ignoring, dismissing or underestimating just how serious ITAR is. It's likely that you, like me, were just blowing it off, thinking it was something only other people had to deal with. Those days are over. They rules apply to you, whether you know it or not. Often, whether the customer tells you or not. It's critical you get informed as soon as possible on ITAR, EAR and the related FAR/DFARS clauses.

Oxebridge doesn't offer training in this area. We're still learning ourselves. Instead, I urge you — nay, beg you — contact Mark Stevens at AEI and find out what you don't know. Read his blog. Reach out to him for a quick phone call. Spend the money to have him come in and train you (it doesn't take long, and doesn't cost much). The ramifications of failing to do so are too severe.

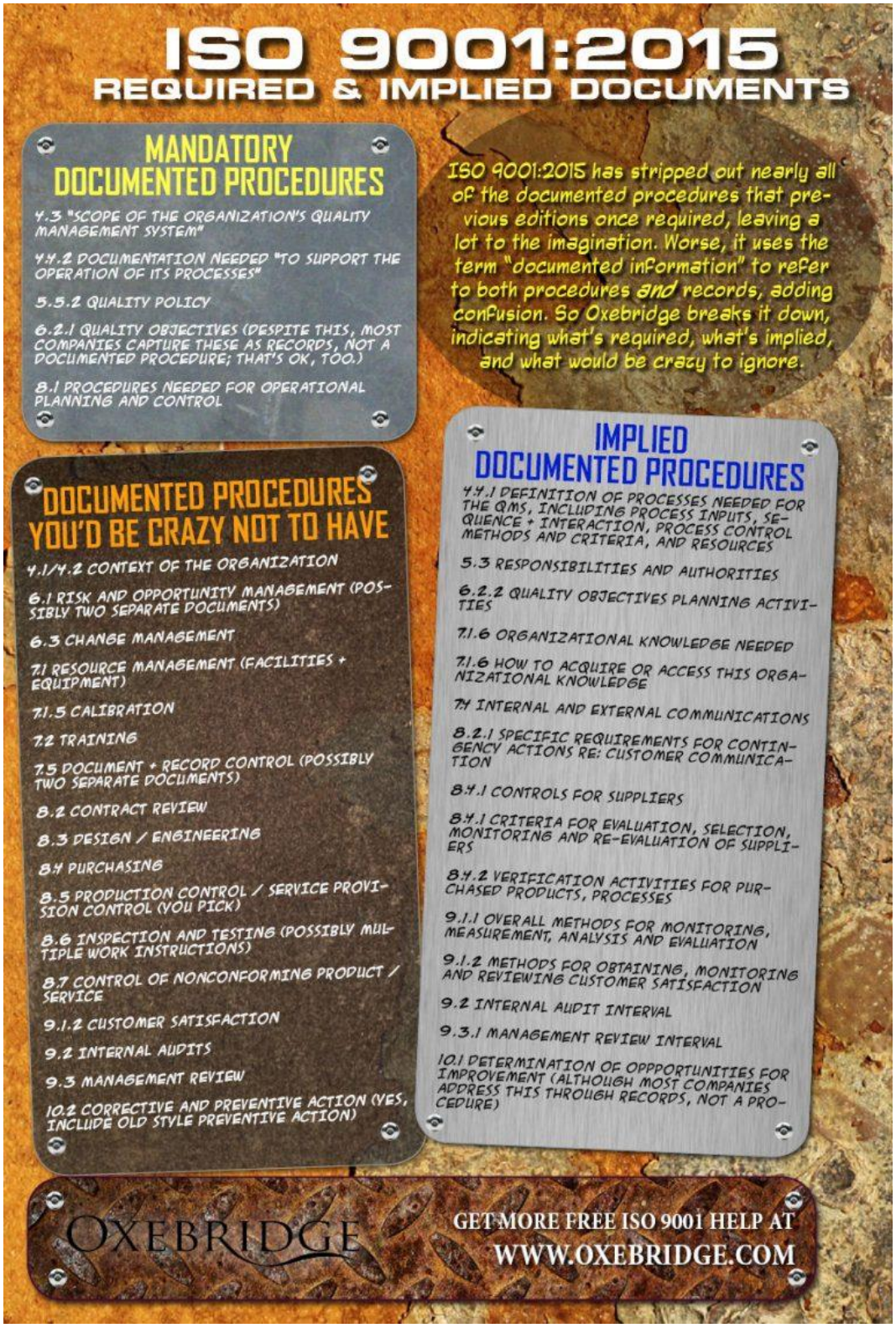
One final point: it doesn't matter if you're running a vanilla ISO 9001 system or an aerospace AS9100 system; it's likely ITAR and/or EAR apply to you. Both standards require you to comply with relative statutory and regulatory requirements; both require you to adhere to customer contractual requirements.

Good luck!

Infographic: Required and Implied Records in ISO 9001:2015



Infographic: Required, Implied and Recommended Documented Procedures for ISO 9001:2015



Five Official TC 176 Rulings on ISO 9001 You Probably Didn't Know Existed

ISO 9001 isn't always well understood, as you can imagine. To help ensure some consistency, Technical Committee 176 — the authors of ISO 9001 — issue "Official Interpretations" when a question is posed to them. The process is laborious and slow, and each request must be framed to allow for either a "yes" or "no" answer, but eventually TC 176 issues a ruling. These are supposed to be upheld by third party certification body auditors, but unfortunately the CB auditors rarely consult the resulting file, and many don't even know it exists. A few outright scoff at TC 176 and say they will do what they like anyway.

But arming yourself with the official TC 176 Interpretations is useful, since you can reference these when responding to a bogus audit finding, and thus win your appeal. You can find the complete set here. But here are a selection of five of the most eye-opening interpretations issued by TC 176 to date.

1.) You can contract out the role of ISO management representative. (TC 176 RFI # 109)

Ruling: TC 176 settled this a long time ago, but auditors and others still insist that the "management representative" cannot be a consultant or contractor. TC 176 ruled that management may assign this to a person who "*works for the company in a managerial capacity, is not a permanent member of staff, but works full-time on a contract basis*."

ISO 9001:2015 applicability: this ruling ***would*** stand, as new standard removes the requirement for a management representative entirely, so if a company wants to continue to use a contractor or consultant in such a role, they may.

2.) Maintenance records are not required. (TC 176 RFI # 111)

Ruling: CB auditors have routinely demanded to see records of preventive maintenance of equipment and/or facilities, despite there never having been a requirement in the standard for this. Eventually TC 176 ruled that no, ISO 9001 does not "require records of the maintenance of infrastructures." This would include preventive maintenance or any other kind of maintenance records. Having them may be a good idea, but it's not a requirement.

ISO 9001:2015 applicability: the ruling ***would*** stand under the new standard as well, since the 2015 version, under clause 7.1.3, does not require such records either.

3.) You do not have to notify the customer if you discover you sent them nonconforming product. (TC 176 RFI # 117)

Ruling: This one may shock you, but there's no hard requirement for you to notify the customer if you later find out you sent them nonconforming product, even if the nonconformance is related to their specific requirements. The ruling probably came about with some hesitation, but in the end TC 176 had to yield to the fact that the requirement simply was never put into the standard.

ISO 9001:2015 applicability: the ruling ***would probably*** stand under the new version as well, but only because of poor wording in the new standard. It appears the authors intended to fix their mistake in ISO 9001:2008, but screwed it up again by poor wording, as clause 8.7.1 now requires the company to "*deal with nonconforming outputs in one or more of the following ways*" and then presents a list of four choices which includes "*notify the customer*." However, since the literal language says "***one or more***

ways," a company may select *other* options from the four choices, and thus ignore "*notify the customer*," and still be in literal compliance with the requirement.

Note: We should probably file a new RFI and get an updating ruling on this one, so proceed with caution. But technically, if TC 176 were to rule that customer notification was required, they should be forced to update the standard, because they'd be contradicting what they wrote. Since they don't like doing that, they'd be forced to rule that no, you still are not obligated to notify the customer.

4.) New documents do <u>not</u> require review. (TC 176 RFI # 106)

Ruling: Wait… *what*? Yes, TC 176 ruled that new documents only require "approval" and no actual review. In their minds, they feel *"some degree of checking, examination or assessment by the person or persons approving is inherent in* [the requirement for] *'approval for adequacy'."* Whenever a standard relies on something being "inherent" then you know you're in trouble.

ISO 9001:2015 applicability: the requirement ***would not*** stand under ISO 9001:2015, which now requires ***both*** "*review <u>and</u> approval for suitability and adequacy*."

5.) You do <u>not</u> have to retain records of inspection of purchased product. (TC 176 RFI # 115)

Ruling: Maybe it was an oversight, but under ISO 9001:2008 clause 7.4.3, TC 176 only required companies to "*establish and implement the inspection or other activities necessary for ensuring that purchased product meets specified purchase requirements*" and never actually required any records of it. Most companies keep "receiving inspection" records anyway, but it is entirely optional.

ISO 9001:2015 applicability: it's ***not clear*** how this ruling would apply under the new standard, since the clause 8.4 "Control of Externally Provided Processes, Products and Services" is badly written, the result of trying to do too many things in one clause. Technically clause 8.4.1 "General" says that company must "*determine the controls to be applied to externally provided processes, products and services*" and then "*retain documented information of these activities and any necessary actions arising from the evaluations*"; but this language appears to be a re-phrasing of ISO 9001:2008 language related to the controls over the supplier, which would mean it deals with supplier audits, surveys, flowdown of requirements, etc. – and thus ***not*** inspection of incoming purchased materials. This is reinforced by the fact that the next clause, 8.4.2 "Type and Extent of Control," goes on to discuss "*verification, or other activities, necessary to ensure that the externally provided processes, products and services meet requirements*," which clearly addresses incoming product inspection. That clause, however, does ***not*** require any records.

Note: We will need a new RFI ruling on this one, as clauses 8.4.1 and 8.4.2 seem to contradict each other, or at least do not compliment each other.

Want to request an official TC 176 interpretation of ISO 9001:2015? Grab the proper request form here, and send it to your nation's official TC 176 member body. The list of member bodies can be found here. Then sit back and wait, because it can take up to a year or more for TC 176 to process and vote on it. Yes, I know they haven't updated the RFI form to reflect ISO 9001:2015, but fill it out anyway. I've alerted Charles Corrie at TC 176 to update the form, but I am sure that will take at least a decade to actually happen.

VIDEO: Context of the Organization & Risk-Based Thinking

by OQRI | Oct 12, 2016 | Guidance Document, News |

A video of the presentation given to ASQ Huntsville is now available for public viewing. The subject is Context of the Organization & Risk-Based Thinking: Implementation of the New Requirements of ISO 9001:2015.

The 1-hour presentation presents the origin of COTO and RBT, and then discusses how to implement the requirements in a practical manner. The October 11th event was extremely well-attended, with ASQ Section leadership indicating they had never had a turnout for any such event in the Section's history. Oxebridge has a fond relationship with the Huntsville area and ASQ Section1503 because of the wide diversity of industries represented, including aerospace and medical devices.

You may view the video on YouTube by clicking the image below:

Exploding the Myths of ISO 9001:2015

Yes, I'm squatting on the name of Andy Nichols' next book, but it was either that or "Cracking the Case of ISO 9001:2015" and ticking off Jack West. In retrospect, I probably should have come up with my own participle phrase concoction, like "Shoving Your Face into ISO 9001" or "Drowning in the Detritus of ISO 9001" but I'm too lazy to go back and edit it now.

The FDIS of ISO 9001:2015 is fast upon us, but already some myths and memes are forming, much to the frustration of anyone who's actually read the damn thing. Even if the eventual published standard fixes some of these, they are already so burned into the common chatter — led mostly by ISO 9001 registrars — it's unlikely they are going to change any time soon.

So let's fire up the debunkerizer, and see if we can cut through this mess.

Risk-Based Thinking = Risk Management

It really doesn't matter how many times ISO and TC 176 tell people that its scented-candle aromatherapy approach called "Risk Based Thinking" ***isn't*** full blown risk management, they are going to continue to say so anyway. Nearly every CB, and every CB auditor, is trotting out FMEA and "risk registers" as the way to address the "risk management requirements of the new ISO 9001 standard."

As reported to me directly by the people who invented it, RBT isn't risk management, it's just a way to nudge companies into considering risks when dealing with pretty much anything in their QMS. The idea was to ***avoid*** calling it risk management since, based on the scope and size of a company, full-blown risk management may not be useful in many companies. A small 3-man machine shop doesn't need risk registers the scale of what Honeywell uses, for example. TC 176, for all its faults, at least understood that.

But in the vacuum of comprehension left by TC 176's inability to properly explain RBT, ISO 9001 experts are filling in the gaps with what they do know, and that means FMEA, risk registers, and insisting that RBT=RM. It's utterly untrue, and must be challenged every time we hear it.

You Don't Have to Document Anything Now

The TC 176 authors have always confused being generic with being vague, and fell deeper into this trap with the 2015 version by gutting all specific callouts for documentation. They claim this allows companies the freedom to document what they want, but already it's being misinterpreted as "we don't have to document anything!"

Not quite. In fact, the standard calls for "defining" quite a few things, and often "defining" means "documenting." And you will still need to determine which aspects are best communicated through documentation. The good news is that you have more freedom to decide how to do this, but companies that delete all their documents and move to using only verbal communication are likely to struggle.

ISO 9001:2015 is a Major Change

The bulk of the changes made from 9001:2008 to the 2015 edition was paragraph shuffling; by our estimate, as much as 74% of the changes were just renumbering old requirements. Of the material that was added, "risk based thinking" pops out as the biggest ideological shift, but since (as we said) there are no requirements tied to RBT, so it doesn't actually count as a significant change. It's a *theme*, not a rule.

In fact, the most significant change to the standard is the clause on "Context of the Organization" which is a one-time mental exercise that most companies should muddle through with few problems. While this fact should be a welcome relief to users, it will frustrate trainers, consultants and registrars trying to sell $1,000 a seat "transition" courses.

The Standard Was Developed by Consensus

Many of the changes that *were* made were driven by the imposition of something called "Annex SL." As we've discussed at length elsewhere, Annex SL was dreamed up not by TC 176, but by the ISO Technical Management Board, which doesn't follow the same rules of consensus as the TC's. In short, they forced TC 176 to adopt Annex SL, and prohibited TC 176 members from refusing any of its requirements.

That's not consensus, that's a dictate. Big difference.

BTW, when challenged on this point, not a single TMB member would agree to comment. That tells you something, if even *they* can't defend their position.

The High Level Structure Matters

The biggest talking point coming out of the various experts is that the new standard adopts a "High Level Structure" (HLS) required by Annex SL. The HLS does nothing more than shuffle the paragraphs into a common sequence that can later be shared by all management system standards, such as 14001. It's part of a marketing push by ISO to sell the world on "integrated management systems," enabling it to sell two, three or four standards at once, rather than just one.

Let me be real clear: ***how paragraphs are numbered is utterly irrelevant to users.*** If anything, this finally gives companies the chance to break free from slavish alignment with ISO clause numbers, and just use their own structure. The HLS impacts on other standards developers the most, and nearly not at all for ISO 9001 end users. Only those obsessed with keeping their documents numbered in accordance with the standard will be stressed by this.

The New Standard Addresses Worker Ergonomics

OK, so I might be partially responsible for this because of some stuff I wrote earlier on how "human factors" got slipped into the 9001:2015 draft. Had I not said anything, this might have slipped under the radar, but it became a thing once people noticed.

Under 6.4, the new standard reads *"the work environment shall give consideration to human factors and human performance, and ensure that the effectiveness of personnel is not unduly impaired."*

Because few in the quality profession understand "human factors," they jump to what they do know, and think it's all about ensuring operators have the right chairs, keyboards, and spongy mats to stand on. People who actually study HF know that's not true, and "ergonomics" is a complex brew of a thousand other concepts, but it certainly sounds good when you are trying to appear like an expert.

Hopefully this gets pulled from the final 9001 release, so we can avoid this mess entirely. But, no, you won't have to buy new ergonomic keyboard drawers to comply with ISO 9001 now.

You Don't Need a Management Representative Anymore

While technically true — the new revision does away with the requirement for a single management representative — the risk here is that users will miss the more obvious truth, that the new standard just pushes all that responsibility onto top management. The benefit here is that now it allows management to delegate roles to multiple people, rather than one, but demands that top management retain overall responsibility, rather than assigning it to some unlucky lackey.

In short, top management is its own representative now, and that's better.

Documents and Records Are the Same Thing Now

Because the scented candles they used when dreaming up "risk based thinking" were apparently spiked with something stronger than just incense, the TC 176 gang decided to combine the concepts of "documents" and "records" into a single thing, called "documented information." To anyone with a functioning cerebral cortex, this makes no sense.

Documents and records are separate things, requiring separate controls. The previous language wasn't broke, but TC 176 decided to fix it anyway. Idiots.

Now companies will forever be confused if they have to advance the revision level of a log sheet every time they make an entry. If you don't think that will happen, you aren't paying attention, because I get that question all the time. At least before I could point to the standard and explain it; now I can't, because even the standard doesn't understand the difference.

No, documents and records aren't the same thing, and never will be. Users will have to trudge over the bad wording of the standard, and continue to maintain separate control mechanisms.

Top Ten Dumb Things ISO Consultants Say

ISO consultants love to parrot each other. One dummy will say something that sounds reasonably smart, and get picked up by everyone else until it becomes an assumed truth. This is how the meme "say what you do, and do what you say" got started. They tend to cause a lot of problems, too.

These repetitive memes are surefire ways to identify a consultant who has never really worked under ISO 9001, and only has the most bare-bones practical experience, even while they claim to have decades of it.

In no particular order:

1. "Don't Use ISO 9001 Language in Your QMS"

This old saw sounds great if you shut off any frontal cortex activity. *"Your QMS should be written based on your own practices and procedures, and not with ISO 9001 language. In fact, you should avoid ISO language entirely!"*

The thinking is that you can lose people's focus and comprehension if you obsess too much with the ISO 9001 language; that's because ISO 9001 is written by a committee of people who all speak different languages, so the end result looks like it was written by drunk lawyers on a wobbly boat during a typhoon. It's a fair criticism, but consultants then try to go all folksy and populist by inferring that your internal processes and procedures should rule the system, without any consideration — or even training! — on ISO 9001 itself.

That's great if you *don't* want your system to comply with ISO 9001. If so, then go for it. But at some point you will have to prove to your internal auditors, customers and possibly external auditors that you comply with ISO 9001, and the only way to do that is to know what exactly you are complying with.

While it's not a good idea to train everyone in the company on every detail of ISO 9001, it's important for them to understand the basics, and to have at least a few hands on deck that are very (very) conversant in translating the ISO 9001 requirements into the company's jargon, and back again.

2. "Woe is Me! Lack of Management Commitment!"

The argument here is that any failing of a QMS can be blamed on a "lack of management commitment." This is not only nutty, it's self-destructive. Consultants who make this claim — and ***it's nearly every single one of them*** (here, here, here, here, here, here, here, here, here… just for starters!) — must be dead set on not getting any business, because it's the top management who will decide what consultant to hire. Who is going to hire a guy that disses them before even meeting them?

It's also nonsense. The argument imagines that all consultants and QMS activities are funded by the QA Manager, who somehow holds the purse strings, and then has to convince his stupid bosses on how to do the right thing. Here's a tip: if the boss signs the checks to pay for a QMS, that's a pretty good indicator of some level of commitment. It doesn't mean he's obligated to buy the QA Manager (or the consultant) a monogrammed swimming pool.

This argument comes from the fact that consultants flee the need for an "escape clause" in the event things go awry during their contract. By arguing "you didn't take my advice, so I'm not responsible" they

think they've inoculated themselves from failure, but it's indicative of the consultant's inability to (a) properly communicate, and (b) convince management of his approach. A good consultant needs to motivate clients, win them over on things they may find unlikable, and get people on the same page.

Reality check: any failure to obtain management commitment ***is the fault of the consultant.***

3. "QMS Templates Are Great, Really!"

ISO 9001 template documents suck. Just stop it already.

4. "You Only Need a Four Page Quality Manual"

Heck, just hire a guy to write your Quality Manual on a grain of rice!

I've built an entire career around simplifying ISO 9001 for clients as much as I can. But I won't go so far as to make stupid statements that defy reality, even if they sound awesome.

Yes, technically everything that ISO 9001 literally requires *could* fit in a four page quality manual. That's because all it requires is a scope statement with exclusions, overall process flow diagram and references to other procedures. Heck, use a small font and you can get it on *two* pages, like this guy.

But here's the question to ask yourself: who is the intended *audience* of the quality manual? Normally it is not just for internal consumption. Anyone bidding on contracts may find themselves having to submit a quality manual as part of the bid, or to submit a copy for review by a customer in order to get on their approved supplier list. Will the customer share your obsession with miniaturization? Probably not. In fact, the money you save on pages will likely be lost ten-thousand fold if you lose that contract. Then let's hope your resume isn't as abbreviated as that quality manual was, 'cuz you're going to need it.

Next, what *about* internal consumption? Who — within the organization — will benefit from a quality manual? In that case, what would they want to see? A tiny manual is likely to gather as much dust as a huge one with too much detail.

The other downside to the micro-manual is appearances. A company that produces only the absolute bare minimum required gives the impression of a company that is also likewise to avoid taking any extra steps for anything. It projects an image of a company that is lazy, crafty, and isn't about to expend energy on making things useful.

A customized walkthrough of the companies' QMS requirements, including a matrix of ISO 9001 clauses (for auditors and those darn customers) is a good middle ground. I say "customized" so you don't get into the template trap I mentioned above.

5. "All You Need is Six Procedures"

Like the mini-manual, this one is technically true if you apply only a quantum of concern over meeting the spirit of ISO 9001, and want to alienate pretty much everyone by your adherence only to the letter of it. Good luck with that.

I'm no fan of documentation at all, especially ISO 9001's notion of it, but there are some activities that you will have a hard time controlling without some form of documentation. For example: inspection practices, calibration methods, and any complex activity where variation between operators could be fatal to the product or service quality.

Remember, one of the documentation requirements is *"documents determined by the organization to be necessary to ensure the effective planning, operation and control of its processes."* By writing only the "required six," you are telegraphing to your employees, customers, auditors and everyone else that you don't need anything else to plan, operate and control your processes.

If your consultant uses "only six procedures" as a selling point, ***run***. A good consultant will assess the company's needs before making any bold proclamations about an appropriate documentation set.

6. "You Cannot Outsource The Management Representative Role"

I've written so much on this subject, it's practically tattooed on the inside of my eyelids. Consultants (and registrars) insist you cannot outsource the management representative role, and point to the requirement that the MR be "a member of management." They stop there, never bothering to ask what "member of management" actually means.

A member of management must be an employee; this much we know. What ISO 9001 does not say — nor could it ever — is what constitutes an "employee." In today's environment, employees can be full time, part time, temporary, temp-to-perm, contract, subcontract, piece-work, commission based, apprenticed, union, non-union, probationary or even "at large." ISO 9001 cannot tell a company who to hire, nor how to hire, lest it run afoul of a million labor laws. What if the only valid candidate is a retired, minority woman who requires a wheelchair, but can only work part time? How is that going to look if some consultant or ISO auditor tells them to fire her? Will they pay for the avalanche of discrimination lawsuits?

Today in many companies, nearly the entire workforce may not even be "employed" by the company itself, but instead by a payroll processing company such as ADP or Paychex. Employees may be hired by an outside headhunting firm, and remain employees for that firm for the first year before "transitioning" into employment by the actual company. Does this mean the all the workers are ineligible for their roles too?

One of my clients was being managed by a CFO who was on temporary contract, because the previous CFO had passed away. The contract was only for six months, while the company recruited a new CFO. The auditor did not blink when auditing this "part timer" despite the fact that it was clearly a subcontracted role. Why does the ISO MR position get higher scrutiny than the senior-most executive?

Truth: a company can hire a "member of management" ***in any capacity it wants,*** so long as that person is granted the responsibilities outlined by the standard. End of story.

7. "ISO 9001 Has Always Been About Risk."

No. No it hasn't. Shut up already.

This new meme is prompted by the upcoming inclusion of "risk based thinking" in ISO 9001:2015, trotted out by ISO consultants who never studied actual risk management in the fields where it is most mature (finance, insurance, pharma, etc) and thus don't actually know what risk management is. So they repackage preventive action as "risk" and throw in a Failure Mode Effects Analysis spreadsheet to show how smart they are. Risk management is a complex discipline that one can get a university degree in. It's not CAPA 2.0, and anyone saying so is a complete newbie on risk.

If a consultant says this, ask them to show you ***their*** risk assessments on vetting new customers, or for the design of their implementation programs. Expect a whole handful of nothing.

8. "You Need a Gap Analysis Before Starting"

The "gap analysis" is one of the biggest consulting scams running. If you are new to ISO 9001, then here's your gap analysis:

You don't comply with ISO 9001. There. Done. And entirely for free.

Consultants may charge as much as a week's work to conduct a "preassessment" audit, the results of which everyone already knows. It's like a patient going into the dentist and the dentist conducting a series of tests just to decide if the patient has teeth.

The resulting report — which the consultant will charge for, too — is equally useless. It will list all the areas you do not comply, which is only useful to the consultant and of no use to the client. The client wants to know what to do moving forward, not where they have failed for the past few decades.

Instead, it's better for a consultant to spend time learning the company's activities, and assessing them silently in his or her head for compliance. Then the consultant can prepare an implementation plan based on the level of compliance, and just get on with the business of consulting and implementing. Extending this activity into a formal audit, with a formal report, wastes the client's time and money.

9. "You Have to Calibrate All Measurement Equipment"

This one costs clients a lot of money. ISO 9001 is explicit on where calibration of equipment is required: for devices used *"to provide evidence of conformity* ***of product*** *to determined requirements."* (Emphasis added.) This means anything used to "buy off" product as part of an inspection or test.

Process equipment does not require calibration unless it is used to also measure the product and determine whether the product passes inspection. This means that temperature gauges, pressure gauges, flow monitors, etc. do not ordinarily require calibration. Furthermore, if you have a series of similar devices that inspect the product in serial, only the final one needs calibration, because it's the one determining final buy-off.

Now this is not to say that calibrating process equipment is a bad idea. On the contrary, it's a great idea. ***But it's not a requirement.*** And that means you get to decide what to calibrate, not the consultant.

With calibration, you want to do what's smart. Just be sure to identify any equipment you do not calibrate with a proper identifier ("no calibration required") — not because it's a requirement, but merely to fend off any questions.

10. "There's a Difference Between 'Continuous' and 'Continual' Improvement"

When your consultant starts to spout this one, understand it probably plays well at all his high society balls and drawing room parties. Or not. Either way, it's pretentious and nonsensical.

They're freakin' synonyms:

And just because I like to give away stuff, here's a free ***eleventh*** dumb thing consultants say:

11. "I'm an Expert, Because I Wrote A Book"

In the age of the internet, everyone's an expert. After all, if I say so on the internet, then it must be true, right? We all know nothing gets published on the internet that isn't true.

In the age of the internet, however, self-publishing is more prevalent than ever. While this is often awesome — it gets previously unheard-of writers in the hands of eager readers, a reality which would never happen in the previous age of the transom — it comes with a downside. Anyone with the patience to write a book (meaning they have nothing better to do, because they are under-employed) can be an overnight expert by having Amazon or some other online self-publishing outlet sell a book for them. These books aren't edited, often not even proofread, and are not published by reputable publishing houses.

Heck, I wrote a book. So there.

Why Auditing "Active Orders" is Terrible Practice

As recently discussed, self-proclaimed ISO 9001 expert David Seear revealed his idea of a "process audit" is to merely select a handful of active orders, chosen during a pre-audit shop floor tour, and then audit those. Unfortunately this practice isn't something reserved to wannabe Demings who never studied statistics, it is pretty much practiced by every auditor out there. We've all seen it. But it is not only NOT a process audit, it's also a pretty horrible way to gather evidence. Here's why.

Sampling By Divining Rod

Mr. Seear alleges his approach is a "sampling method." Of course, it's not, because it doesn't look anything like this. ISO 19011 requires the sampling plan be documented, approved, and communicated to the client; "active order" auditors never do this. They think it's so obvious, that it doesn't even need to be defined. Since accreditation bodies never cite CBs for failing to comply with sampling rules, and apparenty they do the same thing when auditing CBs, this whole mess gets a green light, leading auditors like Seear to believe it's just fine.

But let's be very clear. Simply choosing a "handful" of active orders — and therefore relinquishing all non-active orders from any scrutiny — is not sampling. It is not an organized selection of candidates from a set pool for the purposes of determining compliance of the whole. It is sticking one's finger in the air and hoping the plant air conditioner is on.

Luck Be A Lady During This Audit

This method also requires something that should never enter an auditor's sampling plan: luck. By merely hand-picking orders that happen to be running that day, the auditor could accidentally skew the results in one direction or another. If, by luck of the draw, that day's orders happen to be for products that are well-established, with few problems ever arising, the resulting decision on conformity of the entire QMS may be a false positive. Likewise, if — by bad luck — the process is running a difficult product that day, the resulting decision may be a damnation of the QMS without a sense of context.

If a process happens to be shut down that day — say, for maintenance or office Christmas party — then the auditor is left with nothing at all to audit, and may just skip it.

Home Off the Range

If a given manufacturing process could run different products, at different process settings or conditions, then merely auditing "active orders" fails to assess the process across its potential range.

For example, if the product is a powder, it may enter a given process as a slurry mixture, and undergo a series of drying steps, coatings, baking, sifting, and finally dumping into tote-bins. For one particular product, the settings for temperature, air flow, conveyor rate, agitation and pH may be different than for another product. Assessing only what happens to be running that will only assess if the process is effective at the particular settings for that day. It will not assess products run at higher (or lower) temperatures, speeds, etc. If the equipment or process struggles at the high end of the range, the auditor might never know.

Service Sector, Shmervice Shmector

The method entirely ignores the service sector, and assumes every process is a manufacturing process run by machines with setpoints and using "job orders" to define work. Try applying this to a hotel, or software development company, or a municipal services provider. In these industries, sampling multiple process outputs under varying conditions is critical, because those conditions may change dramatically from one to another, even day to day.

Ghillie Suits and Ninja Moves

Finally, this method allows the client to intentionally skew the results of an audit by populating processes with "easy" jobs, thereby ensuring a positive result. While this is difficult, it's not impossible, and I have seen it done more times than I would like. The clueless auditor, full of self-importance and armed with his "solid sampling method" has no idea the entire thing is a joke, played off his ignorance. Everyone loses.

The Un-Seear Method

Audits must consider *both active orders, and inactive ones*. Active orders allow for easy-to-see objective evidence, and can highlight process deficiencies easily. But a review of the records of inactive orders is critical to ensure the process is assessed across its full range, and to ensure that no funny business has been engaged to skew the audit. Sampling should be based on a defined method. Inactive orders should be examined as far back as the previous audit, not merely recent jobs and not very, very old ones.

This requires reviewing records, conducting more interviews, and trying to piece together what happened without the benefit of seeing things underway at the time. But it's easy, once you get the hang of it.

For clients, if they see an auditor conducting "sampling" in the David Seear method, they should stop the audit and have a quick counseling session with the auditor. If the auditor pushes back, show them the door. You won't get a good assessment of your processes, and may even get some false nonconformities.

Six Sense Auditing: How Your Eyeballs Fail You During Audits

Vision is great. It helps us to drive our cars, choose our mates, and accurately spear a woolly mammoth for dinner; often in that order, if your date goes well. But when it comes to conducting audits, our eyeballs let us down. They lead us down the wrong path, and make us confident over the wrong things.

Multiple surveys over the past few decades have repeatedly reported that the top ISO 9001 nonconformities are related to:

1. Document control errors
2. Product identification
3. Calibration
4. Product preservation (especially expired shelf life materials)

What the data suggests is that client organizations are incompetent when it comes to revision control of documents, or keeping the labels on calibrated tools from falling off. Employing Occam's Razor, the reality is even more simple, and totally contradicts that assumption: it is not that companies are statistically failing in these areas, but rather that *these are the findings that auditors routinely discover* due to poor auditing techniques.

Do Your Neck Exercises

Question: what do those top nonconformity types have in common? Answer: ***eyeballs***.

Each of those findings requires merely that an auditor place their eyeballs in a straight-to-slightly-lowered position. From that perspective, things like revision letters are noticed on documents, dates on calibration stickers or chemical labels are spotted, and product lacking ID markings is discovered. An auditor can be brand new, just out of the gate, with 0 days experience, and still find nonconformities related to these clauses. Why? Because they are discovered with no physical or intellectual effort. They're easy pickins.

This is also why so few findings are issued against the more complex requirements requiring the use of more than just eyeballs, like 4.1's process approach requirements, or 7.3 design and development. These require using the grey stuff behind the eyeballs, and auditors get nearly no training on this. Sight is our primary sense, so it's a given; auditors don't need much training on how to use their vision.

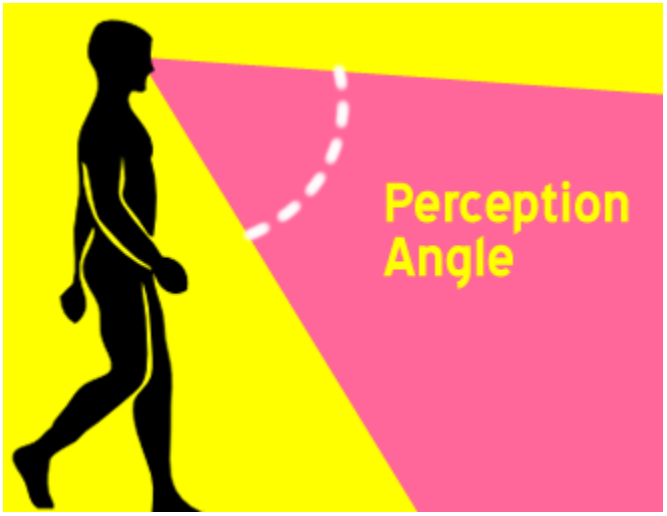
But this sight-centered auditing habit leads to misleading nonconformities and improper audit findings. Noticing a document has the wrong revision on it results in a finding against 4.2.3 Document Control, when in fact the problem may well be something more risk-inducing: perhaps the company laid off its only subject matter expert and that's why the document wasn't revised, and a finding against 6.1 would be more appropriate.

Auditing While Blindfolded

Meanwhile the other senses — like touch and hearing — are ignored or intentionally turned off. Yet these senses add valuable sources of additional evidence that can enhance, or even correct, evidence gathered merely by the eyes. We may see something, but when applying additional senses, we find out

that our assumptions based on sight were incomplete, and the result is very, very different. Use of the other senses can also open us up to finding evidence that we might not, when relying on sight alone.

Reliance on vision pushes us to lazily accept the habits of our body. The human head and neck are "programmed" to rest at a position slightly below the horizon, and so our vision falls in that angle of perception. We have to exert effort — however minute — to raise the head towards the horizon, and much more effort to lift it (and the eyes) to any position *above* the horizon. Consider that many of us spend all day looking down at our keyboards without much discomfort, but if we spend two hours in a front-row seat at a movie theater, looking up, we come out with neck strain.



For auditors this means they have a pre-programmed limited field of perception, and anything outside of that field may well be missed. And — get ready, CB guys — ***clients know this.*** As a result, the top shelves are the best places to hide unidentified scrap or other dirty secrets because everyone knows the auditor will never look there. Why? Because it's above the normal field of perception. A quick survey by Oxebridge found that auditors are 75% more likely to investigate downward — even going so far as to bend over — than they are to investigate upwards.

That's the simplest example. There are lots, lots more.

Auditors must learn to use all their senses when auditing, in order to accurately gather objective evidence. The result, when combined with an all-important *sixth* sense, is a better audit report, with true "value-added" findings that can help clients generate real improvement. Plus, it results in findings supported by so much evidence, they can't be challenged by anyone.

What's the sixth sense?

Sorry, you'll have to book a training event to find out.

Top Ten Mistakes ISO 9001 Consultants Make

Here I present some common mistakes that ISO 9001 (or other management system) consultants make which both hinder their own success, as well as the success of their clients. In no particular order:

1.) Expect to get rich. ISO 9001 is not, by any measure, a rich man's game. Dwindling interest, increased resistance, and poor oversight by its authorities have cut deeply into the market. Would-be consultants have an unfounded fantasy that if they hang their shingle, clients will come running. That's not true, and market forces have driven pricing down so that when a client does appear, they will not be handing you an open checkbook. Padding contracts with long term conditions, unending expenses, and "up-selling" additional services are the mark of a truly bad consultant who has little understanding of his or her client's true needs. Fixed price contracts are the best approach. A good consultant works fast, provides accurate and excellence service, and focuses on earning a living by acquiring multiple clients, not by trying to earn an entire year's salary on one or two. Even then, you will not pull bank like a Hollywood plastic surgeon. You must enter this business because you want to help companies, people and industry, not because you want to buy a new boat to put inside your other boat.

2.) Doomsaying. Consultants have an unusual tendency to present current-state reality as a Zombie Apocalypse. They also always seem shocked that a client who has just hired them doesn't have anything already in place (hint: that's why they hired a consultant.) A typically over-gloomy remark might sound like. "You haven't done anything! This is going to take so much work. You really are far off from where you need to be!"

This doesn't do anyone any good, even when it's 100% true. Consultants need to learn some bedside manner, and present bad news with tact, calm and even a bit of spin. Consider instead: "We've got some challenges, but nothing I haven't seen before. We can work this out, we'll just have to stay focused." See how I incorporated myself into the discussion by saying "we"? It's a team effort, and the client wants to know they hired you to help them, not merely shout the panicked orders of a captain on a sinking ship.

Clients want to see calm, experienced confidence. Panicking them only makes you look like a newbie.

3.) Overemphasize "management commitment." This common claim has its origins in a well-intentioned ISO 9001 requirement (clause 5.1), but has become the crutch for lazy consultants who want to start their work with an easy escape clause: if things go wrong, they can blame management.

Other than the obvious, this is also bad for two other reasons: first, it sends a message to the client that the consultant lacks the ability to rally the team, including management, and is offloading that responsibility back to the people who hired him. Second, it is often interpreted as a subtle jab at the guys paying you; it implies the company hasn't had any management commitment to date. Even if that's true — especially if it's true — the client doesn't want to hear it.

Finally, it also happens to be nonsense. Management commitment helps, but in many cultures – especially the US – management has to be won over after the fact. A good consultant can lead the ISO 9001 effort even in a environment hostile to ISO 9001, and then win them over later by showing them the results of the program. (Right now a lot of not-so-good consultants are shaking their heads on that point. Managers, meanwhile, are nodding in agreement.) By showing management end results such as

reduced scrap, increased productivity, profits, you will get far more "management commitment" than any speech at an opening meeting. These are the things that win over managers, and often times you have to do the work first and get the "commitment" later.

Is that ideal, or even easy? No, but it's what you are being paid for.

4.) Reliance on friendly auditors. Here I am not talking about outright collusion, where a consultant and auditor have a side deal that provides financial benefit to them both, outside of the view of the client. Instead, some consultants find an auditor they like, and promote that auditor from client to client. Perhaps the auditor is friendly, perhaps he or she "goes easy" on the consultant's clients, perhaps it's an old friend, or previous trainer. None of this serves the client well, and it weakens the consultant's abilities over time. When a different auditor enters the mix, all hell breaks loose.

A good consultant should be able to handle any auditor a registrar throws at them, being skilled enough to implement systems that meet the majority of auditors' expectations, and being willing to (gently!) challenge a bad auditor, when they encounter one. (More on that point later.)

5.) Data dump. Few consultants actually have any training on how to be a consultant. As a result, they do now know the best methods for knowledge transfer. They perform a "raw data dump" and regurgitate all their knowledge onto the client, in no particular sequence or, worse yet, following the numbering of the ISO 9001 standard. The client is left struggling to interpret the mess long after the consultant has left. This is why ISO 9001 implementation training courses are so notoriously bad … they rely on this method of knowledge transfer, rather than tailoring it to the particular client.

All information must be transferred in an ordered fashion, optimized to help the client understand why certain things are required, letting them pause to work with it for a while before moving onto the next subject. Despite appearances, this will result in a faster implementation program, because the information is pushed more quickly and absorbed more readily. Less re-training is required later.

To do this, the consultant must develop a true implementation "program" – a blueprint for how the consulting activities will normally progress, through milestones and other activities. This can be a template, but then must be modified for the particular client. It should be updated as the contract progresses, and changed accordingly.

6.) Training the client to be a consultant. Consultants often don't realize that by teaching clients everything they know (see #5 "Data Dump"), they are not training clients on ISO 9001, but instead training them to become their competition.

Typical scenario: a procedure is required, so the consultant trains the client on how to write a procedure. Perhaps a week later, the consultant returns to review the client's procedure, only to point out the weaknesses, order some edits, and come back later to check again. It's agonizingly slow, and would be better served if the consultant just wrote the procedure based on information gleaned from interviews.

This approach teaches the client how to create an ISO 9001 QMS, rather than use one, which is only good if the client wants to become an ISO 9001 consultant. It sounds like a subtle distinction, but there is actually a vast difference. Clients are not tech writers, they are not skilled at writing procedures that

address all the requirements, and they don't need to be. Once again, that's what they have hired you for.

You are paid to develop and deliver the QMS. The client wants to get busy with using the system, not crafting it. Their input is essential, of course, but the nuts and bolts of building the system are the work of the consultant. Then the client can focus on implementing those procedures and moving forward to improve them.

Consider this: your doctor doesn't teach you how to do surgery on yourself, but he will help you improve once the surgery is complete.

7.) Reliance on boilerplates and previous client documents. Boilerplate documents provide a limited use, mostly for saving time when writing procedures that are unlikely to differ between clients, such as management review (because the standard is so descriptive in what is required, leaving little room for creativity.) But the bulk of procedures are likely to be very, very different from one client to the next, and the use of boilerplates will either require the consultant to fit the company around the procedure (never good), or to re-write the procedure from scratch anyway.

Consultants will also often use documents they've written for other clients, and the risk here is that (again) the previous client's approach doesn't work for the new client, or (most embarrassingly) the previous client's name will pop up in the document's text or metadata, revealing the game. Instead it's best to only use boilerplate text as a last resort, to obtain data from the client through interviews, and then write procedures based on that, only adding or changing things when a specific requirement is not met.

8.) Staying within the box. ISO 9001 has devolved into a set of memes, cultivated by lazy registrar auditors and somnambulist consultants. These include such non-requirements as the "training matrix," "master document list," "job descriptions," "process maps" and "document numbers." None of these are specific requirements, but you'd be hard pressed to find an auditor or consultant who didn't think at least one of those really was mandated by ISO 9001. As a result, consultants tend to impose these methods on clients, rather than find an alternative "out of the box" approach that might better suit the client.

Consultants must tailor their solutions to the client, and sometimes that means "going nuts" with new ideas. For example, I once wrote a quality manual that utilized single-panel cartoons to present most of the information. Don't worry about getting registrar buy-in; that can be dealt with later, by communicating clearly with the registrar. During the implementation, focus on what works for the client, and constantly bounce it against the actual language of the standard, not your memory of it. If it meets the intent, the auditor will have to agree to it later.

9.) Representing the registrar over the client. Too many consultants conduct their own work with both eyes on what they think the registrar will accept. This has the effect of the consultant working more for the registrar than for their own client. As I've said, registrars must — by accreditation rules — attempt to understand how each client has interpreted and implemented the various requirements. The client will have plenty of opportunity to explain the approach or method to the auditor. An auditor who refuses to accept a given approach without citing specific evidence on how it fails to comply can be challenged. The client must come first.

10.) Needlessly combating the registrar. The industry may suffer from poorly trained auditors, deceptive CB sales reps, unmotivated Accreditation Bodies and inept ISO management, it's still no excuse to go off half-cocked on an auditor. Auditors will make mistakes — lots of them, if history is any indicator — and these must be addressed in a calm, procedural manner. Accreditation rules require registrars to process appeals and complaints according to set requirements, and consultants should learn these (ISO 17021) and know how to run such concerns through the documented systems. You'll have a harder time convincing an auditor, or the appeals committee, of the validity of your challenge if you don't ground it in evidence and facts, and instead rely on full-on freakouts to make your case.

"Passive" Customer Satisfaction Measurement for ISO 9001

Since ISO 9001:2000 was released, there was a requirement to gather data on customer satisfaction. This resulted in a flood of "Satisfaction Surveys" being released by ISO 9001 certified organizations to their customers. This had the unexpected result of causing such customers to ignore the surveys entirely, as they were receiving more and more of them. So no one was getting feedback.

Marketers say you are lucky to get a 10% return on any survey. I'd bet in the ISO 9001 world, the return rate is even lower.

So, how do you meet the requirements of 8.2.1? Try what I call "Passive Customer Satisfaction Measurement" — the word "passive" being used because you can collect a bit of satisfaction data without active engagement by the customer. No calls, no surveys, no contact at all.

1.) Baseline your current level of business with each customer. That can be by measuring dollars per year, # of PO's they place with you, orders, # line items, etc. Whatever works. Then, continue to take that snapshot ever month. What you are looking for is a sudden drop off in sales or orders. Frequently customers switch vendors without any notice: it may be that they are frustrated with your quality but never filed a complaint, or it could be a change in their buyers, who bring their preferred suppliers with them. When a drop is noticed, research it: did the customer go out of business? Did they move? Were their quality problems with product you delivered to them? As a last resort, call them to find out. But even failing that, you can set goals for customer retention.

2.) Measure returns. Even if customers don't file complaints, they may just return product. That counts as a metric of customer dissatisfaction, and should be measured. You're probably already doing this, but simply apply it to the metrics used for 8.2.1.

3.) Monitor external sources of perception. By this I mean forum boards, social networking sites, etc. See if people are posting bad things — or good things — about your company online. Even if the information is posted anonymously, possibly by competitors or disgruntled ex employees, it's valuable information about the public's perception of your company, and thus your customers. Act on such information as best you can, resisting the urge to post in your defense or slam the folks (trolls) discrediting you. Take away their ability to gripe by becoming excellent.

4.) Consider the Anti-Survey. This is a postage-paid card inserted into every shipment that invites the customer to send it only IF THEY HAVE A PROBLEM. (Be sure to word it in a friendly and upbeat manner, so you don't make it look like you are EXPECTING problems with your products.) Count the number of anti-surveys you send, and then calculate those returned. Each one returned is a hit of dissatisfaction, and you can make a semi-reasonable argument that everyone else is semi-satisfied.

These methods are not as concrete as "active" methods (such as surveys), but they are a great way to obtain data when you can't get it directly from your customers, or as a compliment to a struggling survey system.

Need more help? Join the O-Forum!

Oxebridge has launched **The O-Forum**, a rollicking place to learn, ask questions, gripe or just hang out while discussing ISO standards, certifications, and all that jazz. Other forums are dominated by registrar reps who censor anyone challenging the standard view, but you won't find that to be the case at the O-Forum!

OXEBRIDGE
QUALITY RESOURCES INTERNATIONAL LLC

North America (USA): 863-651-3750
South America (PERU): 011-511-936-102-315

www.oxebridge.com