RESPONSE TO EMAIL 'IAWG UPDATES', 2025-08-01 22:53UTC

Dear Kay,

There is so much about this communication (*in toto* – AH's in-line text but driven by the content of the attachments which you authored) that is deeply concerning that I hardly know where to start. And whilst the publication of SP 800-63 rev.4 is to be welcomed, the way it has been presented in this communication is, to a fair degree, a red herring.

Therefore, as a concerned member of Kantara, and with the continued good standing and openness of Kantara Initiative in mind, I offer the following observations.

I'll kick-off with the existential problem:

Management of current SACs – CO_SAC, OP_SAC, 63x_SACs:

Whilst many of us have identified and pushed for rational amendments (and some straight corrections) to existing SACs, and for the correction to and publication of related notices, these efforts have been stymied within the IAWG by arguments such as being unable to proceed because of the 'transition' (i.e. the accomplishment of gaining Accredited status under IS17065 – see below) and claims of continuing to work on establishing an action tracking process which frankly needs no more than an hour's effort) tactics in the IAWG's operation (e.g. claims that nothing can be done until the 'transition', cancelling meetings on a regular basis with unconvincing justifications. In addition, things actually agreed by the IAWG have been passed to staff yet no action has been taken to publish agreed amendments. In some cases this situation has prevailed since at least Q3 of 2024. The existing criteria will continue to be relevant for all currently-Approved and Applicant services for up to a further 15 months, possibly longer (i.e. until 'rev.4' criteria exist and CSPs have had time to absorb changes to requirements and modify their services' functions accordingly). Surely Kantara has an ongoing need and a duty to its members to apply effective management over these criteria? By closing the IAWG with no clear alternative offered other than references to a 'US Assurance Program' (a term which I for one do not recognize and for which I see no immediate description) I predict continued stagnation of the current criteria, to the detriment of the quality of Kantara's standing. How can this be justified?

Related to this is the question as to how the 'US Assurance Program' will cope with existing Approval renewals and receive new Applications, all of which at present would have to be assessed against the existing rev.3 63x_SAC.

I argue for the continued operation of the IAWG per its Charter, under Kantara's existing and essentially workable procedures (essentially the SAH and AQR), at least until such time as the current criteria are reviewed (as has been discussed within the IAWG) and consolidated at the time that rev.4 criteria are developed. Then let's see where we are. Furthermore, and perhaps against my own better judgement, I offer myself as Chairman of the IAWG, subject to: i) affirmed and timely support from 'staff' to effect changes; and ii) the ability to select and gain the agreement of a Co-Chair (or Co-Chairs) with whom I would be comfortable working.

Establishment of an Accredited Certification Body (CB):

I commence by emphasizing my support for Kantara attaining the status of operating an Accredited CB. At the same time I am very disappointed that the Kantara community at large, and I would say the IAWG in particular, has to date seen nothing tangible since this activity commenced in the latter months of last year. The presentation given in January was an overview of IS17065 and offered little in the way of how it might be applied in the particular context of Kantara Initiative.

This communication suggests to me that a number of thoughts / interpretations, perhaps even defined process, being proposed (or possibly implemented) are, in my professional opinion[1], unfounded and not in Kantara's best interests. Terms such as "concrete instructions" and "very specific instructions", taken in the context of the reference to "UKAS requirements for ISO 17065-accredited programs" cause me concern. The Accreditation requirements to be applied (and subject to applicable requirements of other normatively-referenced standards taken into consideration, most of which in fact do not apply since Kantara does not create 'products') are those published in IS17065[2] and no others. Accreditation Bodies (such as the cited UK Accreditation Service - UKAS) are not entitled to determine their own 'requirements' or preferred means of fulfillment of IS17065's requirements and cannot impose these upon their clients. If it doesn't say it in IS17065, an accreditation subject does not have to do it (no more than a Kantara Assessor can self-determine and impose upon a CSP requirements which are not with the published SACs). The terms 'assurance program' and 'stakeholder oversight group' do not appear in IS17065, so it is hard to understand how an AB can impose any such requirements. IS17065 is only about accrediting a CB.

Though admittedly I am inferring from what has been said in this communication (in the absence of any substantive information) and from past discussions, I sense that:

1) The proposed Certification Body will own 'the scheme' (to use IS17065's parlance);
2) Thus, control of all criteria will be tightly controlled from within the CB;
3) Assessors will be 'owned' by the CB which will contract directly with applicant CSPs;

In 2020/2021 I was given an assignment by Kantara to initiate a path to Accreditation, in the course of which I produced a qualitative draft Policy and Procedures document, which in the interests of openness I attach. A few simple premises were accommodated which basically took the existing (until last Thursday) IAF's structures and transformed them in as light a manner as possible into an accreditable CB. Firstly, the CB did not own the scheme, the scheme operated independently and was adopted by the CB. That this is a perfectly legitimate manner in which a CB can operate is manifestly evident in the fact that around the World there are hundreds if not a small number of thousands of CBs (that is, Accredited CBs under the auspices of the International Accreditation Forum – ironically another 'IAF') which offer certification against such standards as ISO 9001, 14000, 27001, 31000, etc., standards/schemes which clearly are owned by ISO, the publisher and copyright holder of those standards. Any AB which suggests that ownership of the scheme and its normative requirements must rest with the CB is failing. This therefore also deals with point 2) above.

The third point is also not a requirement of IS17065 and retaining the existing relationship between Assessors (Auditors) and Auditees is consistent with IS17065 requirements. I have previously taken the trouble to verify these points with ANAB (the American National Accreditation Board) and communicate them to you, and for the record that exchange follows:

Email 2025-04-16: Applying 17065
Kay, Carol,

[snip]

I took it upon myself to put a few questions to a colleague at ANAB, without revealing anything about the organization at the focus of my questions.
I spoke to Keith Mowry, ANAB's Senior Manager, Business Development, who is one of the 17065 authors/editors. I offer below his comments to the points I raised (his responses, not verbatim, are in red) and hope these may be helpful.

One area of concern is the relationship between KI and its auditors, in particular whether auditors would negotiate with CSPs for the audit fee, while KI charged a Certification processing fee, or whether KI would seek to be the sole contractual /fee interface and would pay-on to the auditors. I have concerns about auditors not being able to negotiate directly with CSPs [snip].

I specifically asked KM whether there was any requirement, expressed or implied, in 17065 regarding the contractual relationships between CB, auditors and clients. Though I didn't think there were, his response surprised me:
KM: nothing directs either way but 17065 §6.2 was written as it is with the direct intention that auditors could contract directly with the auditee.
This affirmed my understanding of 17065 that the CB has to have defined practices for the establishment of a relationship with the auditee client and with the auditor, through contracts, but that the commercial arrangements are completely independent.

In a recent email to a select group, Kay, you stated "The transition to ISO 17065 accreditation requires aligning criteria with international accreditation standards, and those changes are not optional" (my underline). I was baffled by that statement. I have never found anything in my ISO experience which governs how auditing criteria should be prepared, presented, worded or anything suchlike (unless one digs into the ISO Directives which govern how to write international standards, which is not what KI does). I attach a schematic which identifies what I understand to be the applicable standards (red = normative/requirements, blue = informative/guidance (*i.e. cannot be enforced*), shaded = not applicable (imv)) in regard to achieving accreditation as a CB for the purposes of auditing and certifying services. If you are able to identify the specific standards and clauses which impose such requirements I would be very interested to learn about them.
KM: it is not the accreditor's job to say whether a scheme is good or bad. 17065 expressly does not address the characteristics of the scheme – refer to its **Introduction**, paragraph 6: "*This International Standard does not set requirements for schemes and how they are developed and is not intended to restrict the role or choice of scheme owners, however scheme requirements should not contradict or exclude any of the requirements of this International Standard*".

Thus, it is clear that no requirements within 17065, nor 17021, address this topic. Whilst there are certainly ways in which the existing SACs could be improved, I fail to see why they could not be the basis of a Certification Scheme essentially 'as is'. We have all the procedures and controls around their maintenance and publication, which can be absorbed into the CB's operations. We have defined processes for performing assessments.

I also sought KM's view as to whether 17021 was the optimal choice from those standards cited in 17065. My rationale is that 17021 is the better choice since in the CO_SAC we have requirements which address the nature of establishment, ownership and infosec management within the service provider. When I drafted these I very deliberately aligned many of the criteria to clauses and principles within IS27001 (Infosec Management System – Requirements). Again, KM's response was illuminating:

KM: Although reference to 17021 makes perfect sense because of the management system perspective, there is no need to be bound by all of its requirements, since the CB's envisaged scope is not explicitly for the auditing of management systems. Therefore, a degree of selection as to which clauses of 17021 conformity is claimed is perfectly permissible, since IS17065 refers to 'applicable requirements' of those standards. There is no explicit requirement to actually cite any of 17020, '021, '025 if the nature of the CB's scheme is not a direct match to one of those standards and if appropriate requirements can be otherwise drawn up.
I'm not suggesting that that last sentence be used as a reason not to use IS17021, but it is an interesting observation which supports the careful selection (and perhaps defense?) of 'applicable requirements'.

I specifically asked KM whether an Accredn. Body had any authority or entitlement to impose requirements which were not in the standard(s) being used to determine whether an applicant organization fulfilled the requirements to become a CB. He stated that there were not. I have found some Certification auditors applying requirements which are not in the reference standards and it is simply bad practice, and potentially in contravention of the standards under which they themselves are accredited to operate.

Keith Mowry was very open to being contacted directly by yourselves if you wish (+1 414 501 5466). Possibly speaking to a US-based AB for the US-based (but International in scope, excluding GB) operations would prove fruitful. Keith did make the point that the cost of Accreditation is likely an order of magnitude lower than the cost of operation, and having a lean Certification process was a goal worthwhile.

I hope this is helpful. Perhaps greater exposure of the proposed Kantara CB will lay fears to rest, so I (and I would anticipate others) would certainly be appreciative of greater exposure of the work in hand, hopefully with some high-level insights rather than a fully-specified '*fait accomplit*'.

Thanks for your time,

Highlighting in the above-cited email is specific to this inclusion. It is my concern that these points are being overlooked or are not fully comprehended, or that UKAS is imposing unfounded requirements that complicates the situation, but I reiterate the point made in that email, that a lighter approach with minimal change is (surely ?) a more attractive path.

Moreover, whilst I was undertaking that previous assignment Kantara was in discussion with International Accreditation Services (located in La Brea, California) who saw no problem with the proposed principles of establishing conformity against IS17065. Perhaps that relationship is worthy of being rekindled, to have a more friendly and less imposing AB?

Accreditation against IS17065 can be accomplished independently of any revision to a publication to which Kantara's criteria (the 'scheme') are aligned. Therefore, publication of rev.4 has no conditional implications upon accreditation. My third consideration is sufficiently addressed above.

I therefore argue for an open discussion on the principles of Kantara's CB supported by whatever tangible product has thus far been prepared, irrespective of its state of review.

SP 800-63 rev.4 implications:

For over a year we have discussed in the IAWG enhancements and optimisations within Kantara's criteria and deferred these until rev.4 was released: we now have that as an impetus to achieve those objectives. However that is a significant undertaking and is a parallel task to accreditation. It seems to me that these criteria would be best addressed by those fully familiar with the operation of the existing processes and by utilizing the resources of a functional IAWG. As I hope you will recall Kay, you have an offer on the table for this work to be conducted, including revisions to better accommodate the CO_SAC, and that could perhaps be refreshed.

Accordingly, I argue for an open process for criteria drafting which actively involves all stakeholders, volunteers, or whatever.(which, by the way, is precisely how ISO works, so – once again – there is no requirement in IS17065 directing how a scheme should be operated).

Kantara's standing and modus operandum

Yes, I readily admit to a paternal instinct towards Kantara, given my long historical association with it, including foundational work even prior to its inception. I want it to work and to be open in all aspects. Kantara in all its progressions, sometimes under other names, has hitherto always been an open project, industry-based with inputs from all stakeholders at all stages. Scores of individuals have contributed thousands of hours of their *pro bono* time and professional expertise. In recent months an opaque veil has descended. I don't believe this is helpful, and my reading of this communication seems to, at the least, push away this kind of interaction and constructive development. If you have substantive material to hand, why not give it exposure to peer review as early as possible, and incrementally? And if you haven't, there is probably still a willingness to help Kantara evolve.

If I am totally, or even substantially, wrong in my observations then I apologise, but I do so with the defence that, in the absence of the provision of substantive material and in the face of evasive memos and notifications this is my best interpretation of events. And that cannot be healthy for Kantara. I will, however, be happy to be enlightened, as I suspect will be others, for I know these concerns are not mine alone.

Thank you for your time in considering these observations.

Richard G. Wilsher
CEO, Zygma Inc.

[1] – this is based on many years experience within the US' delegation to ISO JTC/1 SC/27, including acting as the nation's technical lead, and an editor/reviewer, on IS2700x standards, including accreditation and certification standards.

[2] – and by inclusion, other referenced normative standards, subject to the same caveat regarding published requirements.