Improving the usability of ISO standards by M&SME

Why don’t Micro and SME love ISO?

Kenneth Tombs – Independent
ISO November 2022 SME Workshop

©2022 Business Compass
Harsh realities

- Risk, trust, vulnerability
- Extremist leaders
- Regulatory overload
- ESG/EESG/E2SG
- Political instability
- 3rd party assurance
- Performance metrics
- Consequential damages

“Manslaughter by gross negligence occurs when the offender is in breach of a duty of care towards the victim, the breach causes the death of the victim and, having regard to the risk involved, the offender’s conduct was so bad as to amount to a criminal act or omission.”

UK Sentencing Council, 2018
In essence

“Smart business people who aren't paperwork hobbyists need a quality point of assistance they can afford for all aspects of compliance – the quick fix!

They need quality as being smaller lessens little the need for quality and consistency in compliance.

They need trusted allies to help them, yet there is no such capability unless they work with a myriad of specialists on a topic-by-topic basis.”

Source: BusinessComply Limited, 2019
Why not?

• The essence is MSME want it simple, quick, and cheap – £1000 to £7000.

• Current ISO management systems for MSME are ‘brain-space’ prohibitive.

• ISO consultancies can’t deliver this in the current Internal Audit regime.

• The ISO Practical advice for Small Businesses (27001) Compact Disk is ‘too difficult’.

• Multiplicity of silo standards only confuse.

• Supply chains/regulators want comparability across all sizes M, SME and Corporate.

Source: BusinessComply Limited, 2019
## Leader behaviours

<table>
<thead>
<tr>
<th>Micro organisations</th>
<th>SME into Majors</th>
<th>Corporate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Its about taking away their specific problem immediately</td>
<td>Its about joining up choices and legacies</td>
<td>Joining up disconnected silo</td>
</tr>
<tr>
<td>“Feel they are not taken seriously by suppliers”</td>
<td>Its often internally political</td>
<td>Managed operating cost</td>
</tr>
<tr>
<td>“Feel not significant to suppliers”</td>
<td>Responding to change fast</td>
<td>Fastest time to detect threats</td>
</tr>
<tr>
<td>‘One stop’ solution avoids hunting for services</td>
<td>Integration with existing practices</td>
<td>Fastest time to remediate</td>
</tr>
<tr>
<td>‘Immediate on’ gives a quicker fix</td>
<td>Integration with existing systems and suppliers</td>
<td>A wide range of support functions</td>
</tr>
<tr>
<td>Trivial operating cost</td>
<td>Predominantly ISO 27001</td>
<td>Timeline preparations for compliance and regulation</td>
</tr>
<tr>
<td>Little consideration of the details</td>
<td>Maximum trust of the chosen supplier</td>
<td>Fastest time to report and regulate</td>
</tr>
<tr>
<td>Prefers to use a trusted person</td>
<td></td>
<td>Manage the details, no gaps</td>
</tr>
<tr>
<td><strong>About income</strong></td>
<td><strong>About recognising a future</strong></td>
<td><strong>About anticipating and protecting</strong></td>
</tr>
</tbody>
</table>

Source: BusinessComply Limited, 2019
Deconstruct ISO – Corporate ISMS

• Commitment
• Adoption
• Boundary
• Formulation
• Decision
• Enactment
• Usage
• Evidence
• Interaction
• Audit
• Assurance
Deconstruct ISO - MSME

- Commitment
- Adoption
- Boundary
- Formulation
- Decision
- Enactment
- Usage
- Evidence
- Interaction
- Audit
- Assurance

For MSME we cannot imagine the ultra-simplicity leaders want!
Improve usability

- Assume MSME conformity will mostly off-set to MSME suppliers.
- Reshape IUMSS to be the ‘Coat Hangar’, as an auditable standard.
- Recognise IUMSS has the central role in open management systems.
- Merge, simplify, reorganise ‘how’ - not the intent.
- Automate Internal and External Audit.
How?

• We need ‘an acceptable to the ISO family’ alternative way-of-working for MSME.
• Digital automation could deliver, if the ISO family accepts it.
• COVID confirmed that remote working and online disclosure are viable.
• Reshape IUMSS to become the ‘first choice’ ‘onboarding’ standard.
• Do not re-wite the standards just for SME – re think them.
• Need for universal management systems to replace silo based GRC - ‘Open GRC’.
• Anticipate greater roles for certifying bodies, ‘Light Touch’ ‘Performance Related’ ‘OpenGRC’.
Why?

ISO must unambiguously offer all sizes of enterprise a management system, that supports political initiatives to simplify regulation

or

Lose hard-won leadership as a myriad of ad-hoc competitors undermine ISO’ cohesion.
About

The presenter

Kenneth has over 40 years experience starting as an engineering apprentice; journeying through sales, marketing, training, and then technology exploitation. He worked for Honeywell-Bull, Hanover Education and PwC, before becoming a Strategic consultant to HMG and others, then Board roles for Chandler Macleod, Fluid Oil, and Fusion Experience. The last four years have been focussed on GRC and Compliance, particularly towards Micro and SME organisations.
Trust secures our futures

- Customers need trust in their suppliers’.
- Executives need to trust in their business.
- Employees need to trust in their executives.
- Regulators need to trust in the data.
- Investors need to trust goals and objectives.
- Auditors need to be trusted.
“The Plan for Digital Regulation emphasised the crucial role that join up between regulators will play in enhancing the overall effectiveness of regulatory interventions. As innovations in technology continue to defy traditional definitions, and blur regulatory boundaries, closer coordination will be needed across the regulatory landscape - for example, to enable effective data sharing across sectors by intermediaries or to deal with the cross-cutting challenges of digitised sectors such as online advertising or gambling. Going forward, sharing expertise, developing common capabilities, maximising efficiencies in the way regulators operate, and minimising unnecessary burdens on business will be paramount.”
The Proposition – transparent GRC

1. Government mandates every organisation, business, charity, or enterprise, must have and maintain an electronic GRC.
2. That GRC must follow a recognised standard, ideally ISO.
3. Government issues/revises/withdraws specific sectorial ‘Controls’ for every each GRC.
4. GRC status is reported to a national body as a public register.
5. In exchange Governments stop publishing complex legislation that requires interpretation and is always confrontational.
6. Controls being specific and simpler, could be more aligned internationally and more swiftly.
About

The presenter

Kenneth has over 40 years experience starting as an engineering apprentice; journeying through sales, marketing, training, and then technology exploitation. He worked for Honeywell-Bull, Hanover Education and PwC, before becoming a Strategic consultant to HMG and others, then Board roles for Chandler Macleod, Fluid Oil, and Fusion Experience. The last four years have been focussed on GRC and Compliance, particularly towards Micro and SME organisations.

Contributions:

• Barry Welsford-Lippiatt – Independent
• Prof. R ‘Bob’ Garratt – Author and Director of Good Governance Limited
• Christopher Gleadle – Paddy Ashdown Centre
• Daren Martin – GRC One
• Jeff Ashbolt – BusinessOptix
• Karly Olsen-Haveland – Independent
• Prof. Michael Mainelli – Z/Yen Group
• Simon Mills – Z/Yen Group Stephan Hamm – ESG
• Prof. Vicki Lemieux – Vancouver Business School