Our Business is Keeping You in Business
ContinuitySA

SANS / ISO22301
International BCM Standard

By Eugene Taylor
Agenda

- **Standards: The World and the South African position**
  - Overview of the mechanisms behind standards development and adoption

- **SANS / ISO 22301**
  - The rationale and what it is

- **A Business Continuity Management System (BCMS) framework**
  - What’s needed to align to, or be certified to the standard

- **Assessments and Audits**
  - The good stuff and the bits to watch for

- **The Benefits**
  - Alignment and Certification
Other standards (local and international)
  • Those disciplines that are commonly used and develop resilience

What’s on the horizon with standards
  • Keep an eye out for these - they are strongly related to the resilience suite

Questions and Answers
  • Ask anything
Standards

The World

- ISO, CEN, CENELEC, IEC, ASIS, BSI, SABS, BCI, ECB, BoE
- CASCO, CIE, COPOLCO, IIW, IULTCS, REMCO, TMB, VAMAS
- A note about technical committees - specifically TC223

The South African position

- SABS, SANAS, King Code
Standards and Accreditation bodies

**Standards bodies**

- SABS: South African Bureau of Standards
- BSI: British Standards Institute
- ISO: International Standards Organisation
- CEN: European Committee for Standardisation
- CENELEC: European Committee for Electro Technical Standardisation
- ASIS International: “American Society for Industrial Security” – Society for Professionals
- IEC: International Electro technical Commission
- Others: CASCO, CIE, COPOLCO, IIW, IULTCS, REMCO, TMB, VAMAS

**Accreditation bodies (ISO 17021)**

- SANAS: South African National Accreditation System
- UKAS: United Kingdom Accreditation Service
- SADCA: Southern African Development Community Cooperation in Accreditation (Southern Africa)
- JAS-ANZ: Joint Accreditation System of Australia and New Zealand
- USA: ASIS, ANAB, A2LA
- IAF: International Accreditation Forum (MLA)
Technical Committees

There are many …

ISO related:

TC 1 to TC 275 (last count) - over 400 committees

Not all have produced standards

TC 223 = Societal Security (Crisis Management and Business Continuity)

Participating countries 47, Observing countries 19

7 Published Standards

The South African involvement …

SABS a full member of ISO

SA participating in 112 committees, for example …

JTC 1 (Information technology) 2590

TC 157 (Non-systemic contraceptives & STI barrier prophylactics) 13

TC 176 (Quality Management) 22

TC 223 (Societal Security) 7

TC 223 member constituents:

This is not clear and possibly not fully representative of RSA industry sectors. Anthony Kesten from SABS is chair of TC 223
Technical Committees - RSA

| TC 1 - | Information technology |
| TC 2 - | Energy efficiency and renewable energy |
| TC 3 - | Screw threads |
| TC 4 - | Rolling bearings |
| TC 5 - | Paper, boards and pulps |
| TC 6 - | Steel |
| TC 7 - | Equipment for Fire Protection |
| TC 8 - | Cast irons and pig irons |
| TC 9 - | Solid mineral fuels (S) |
| TC 10 - | Small tools |
| TC 11 - | Food products |
| TC 12 - | Paints and varnishes |
| TC 13 - | Terminology, other languages and content |
| TC 14 - | Textiles |
| TC 15 - | Pulleys and belts |
| TC 16 - | Acoustic |
| TC 17 - | Welding and allied processes |
| TC 18 - | Rubber and rubber products |
| TC 19 - | Information and documentation |
| TC 20 - | Gas Cylinders |
| TC 21 - | Building and Civil Engineering works |
| TC 22 - | Plastics |
| TC 23 - | Financial services |
| TC 24 - | Concrete, reinforced concrete and pre-stressed |
| TC 25 - | Cement and Lime |
| TC 26 - | Products in fibre reinforced cement |
| TC 27 - | Mining |
| TC 28 - | Devices for administration of medicinal products |
| TC 29 - | Wood based panels |
| TC 30 - | Fire safety |
| TC 31 - | Personal safety |
| TC 32 - | Cranes |
| TC 33 - | Bases for design of structures |
| TC 34 - | Chains and chain sprockets |
| TC 35 - | Continuous mechanical handling equipment |
| TC 36 - | Iron ore and direct reduced iron |
| TC 37 - | Freight containers |
| TC 101 - | Steel wire ropes |
| TC 102 - | Metallic and other inorganic coatings |
| TC 103 - | Mechanical vibration |
| TC 104 - | Industrial trucks |
| TC 105 - | Round steel link chains, chain slings, components |
| TC 106 - | Leather |
| TC 107 - | Packaging |
| TC 108 - | Plain bearings |
| TC 109 - | Ferralloys |
| TC 110 - | Clothing sizing systems - size designation, etc. (S) |
| TC 111 - | Non-destructive testing |
| TC 112 - | Furniture |
| TC 113 - | Footwear sizing designations and marking (S) |
| TC 114 - | Plastics pipes, fittings and valves for fluids |
| TC 115 - | Water quality |
| TC 116 - | Valves |
| TC 117 - | Corrosion of metals and alloys |
| TC 118 - | Non-systemic contraceptives and STI |
| TC 119 - | Ergonomics |
| TC 120 - | Thermal performance and energy use |
| TC 121 - | Mechanical testing of metals |
| TC 122 - | Timber structures |
| TC 123 - | Steel and aluminium structures |
| TC 124 - | Document management applications |
| TC 125 - | Assistive products for persons with disability |
| TC 126 - | Jewellery |
| TC 127 - | Quality management and quality assurance |
| TC 128 - | Lifts, escalators and moving walks |
| TC 129 - | Stand by - Masonry |
| TC 130 - | Solar energy |
| TC 131 - | Geotechnics |
| TC 132 - | Small craft |
| TC 133 - | Ceramic tile |
| TC 134 - | Sterilization of health care products |
| TC 135 - | Microbeam analysis |
| TC 136 - | Intelligent transport systems |
| TC 137 - | Environmental management |
| TC 138 - | Quality management - for medical devices |
| TC 139 - | Geographic information / geomatics |
| TC 140 - | Clinical laboratory testing and in vitro diagnostic |
| TC 141 - | Elevating work platforms |
| TC 142 - | Footwear |
| TC 143 - | Cosmetics |
| TC 144 - | Floor coverings |
| TC 145 - | Geosynthetics |
| TC 146 - | Stand by - Personal financial planning |
| TC 147 - | Societal security |
| TC 148 - | Service activities relating to drinking water |
| TC 149 - | Market, opinion and social research |
| TC 150 - | Tourism and related services |
| TC 151 - | Nanotechnologies |
| TC 152 - | Fisheries and aquaculture |
| TC 153 - | Project Committee: Project Management |
| TC 154 - | Solid biofuels |
| TC 155 - | Project Committee: Product recall |
| TC 156 - | Road traffic safety management systems |
| TC 157 - | Energy Management |
| TC 158 - | Cross-border trade |
| TC 159 - | Fraud countermeasures and controls |
| TC 160 - | Project committee: Sustainability criteria |
| TC 161 - | Traditional chinese medicine |
| TC 162 - | Project committee: Asset management |
| TC 163 - | Natural gas fuelling stations |
| TC 164 - | Project committee: Treated wastewater re-use |
| TC 165 - | Safety of amusement rides and devices |
| TC 166 - | Biogas (O-Member) |
| TC 167 - | Rules for determination of energy savings |
| TC 168 - | Project, programme and portfolio management |
| TC 169 - | Coalbed methane (CBM) |
| TC 170 - | Fireworks |
| TC 171 - | Carbon dioxide capture, transportation |
| TC 172 - | Sustainable development in communities |
| TC 173 - | Railway applications |
| TC 174 - | Customer contact centres (S) |
### Technical Committees - RSA

#### Which committees against which standards …

<table>
<thead>
<tr>
<th>Standard</th>
<th>Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 9001 Quality MS:</td>
<td>TC 176/SC 2</td>
</tr>
<tr>
<td>ISO 9004 QMS – Sustained success:</td>
<td>TC 176/SC 2</td>
</tr>
<tr>
<td>ISO 10005 QMS – Quality Plans:</td>
<td>TC 176/SC 2</td>
</tr>
<tr>
<td>ISO 14001 Environmental MS:</td>
<td>TC 207/SC 1</td>
</tr>
<tr>
<td>ISO 16xxx* Fraud countermeasures:</td>
<td>TC 247</td>
</tr>
<tr>
<td>ISO 19011 Auditing MS:</td>
<td>TC 176/SC 3</td>
</tr>
<tr>
<td>ISO 20000 IT Service Management:</td>
<td>JTC 1/SC 7</td>
</tr>
<tr>
<td>ISO 22000 Food Safety MS:</td>
<td>TC 34/SC 17</td>
</tr>
<tr>
<td>ISO 22301 Business Continuity MS:</td>
<td>TC 223</td>
</tr>
<tr>
<td>ISO 22313 BCMS Guidance</td>
<td>TC 223</td>
</tr>
<tr>
<td>ISO 22398* Exercising and Testing:</td>
<td>TC 223</td>
</tr>
<tr>
<td>ISO 24762 IT ICT Technology DR Services:</td>
<td>JTC 1/SC 27</td>
</tr>
<tr>
<td>ISO 27001 IT Information Security MS:</td>
<td>JTC 1/SC 27</td>
</tr>
<tr>
<td>ISO 27031 ICT Readiness for BC:</td>
<td>JTC 1/SC 1</td>
</tr>
<tr>
<td>ISO 27035 IT IS Incident Management:</td>
<td>JTC 1/SC 27</td>
</tr>
<tr>
<td>ISO 28001 Supply Chain Security MS:</td>
<td>TC 8/SC 11</td>
</tr>
<tr>
<td>ISO 31000 RM Principles and Guidelines:</td>
<td>TC 262 (RSA off the radar)</td>
</tr>
<tr>
<td>BS 31100 RM Code of Practice:</td>
<td>BSI Group</td>
</tr>
<tr>
<td>ISO 5500x* Asset Management:</td>
<td>TC 251</td>
</tr>
<tr>
<td>OHSAS 18001 Occupational H&amp;S:</td>
<td>BSI Group</td>
</tr>
<tr>
<td>ISO 17021 Conformity assessment</td>
<td>CASCO</td>
</tr>
</tbody>
</table>

### An observation …

TC 262 Risk Management:  
SA not involved  
ISO guide 73 and ISO 31000

### Adoption of 22301…

Argentina, Bulgaria, Colombia, Egypt, Israel, Kenya, Morocco, Netherlands, Norway, Singapore, **South Africa**, Sri Lanka, Sweden, Switzerland, Thailand, UK  
**Not:** Malaysia, Russian Federation
SANS / ISO 22301

The South African position
  • So - where are we with SANS / ISO 22301?

Professional support
  • There is plenty - but go with the reputable ones

Considerations for implementation
  • The position of BCM and people with defined BC responsibilities

How it is structured
  • Ways to approach implementing or improving your BCMS
The South African position

SABS - adoption of ISO 22301 and others …

Adopted by SABS (July 2012) SANS / ISO 22301

SABS also adopted ISO 14001, ISO 9001, OHSAS 18001, ISO 20000, ISO 22000, ISO 27001

SANAS - ISO 22301 accreditation position

SANAS is contemplating the viability of accrediting local companies to provide certification (ref: Dec 2012)

How our globe fits in ….

International Accreditation Forum (IAF) - SANAS has signed the Multilateral Recognition Agreement (MLA)

But not all those that are party to the MLA will provide accreditation outside their countries (note on ISO 17021)

A note about the King Code of Corporate Governance

1994, 2002, 2009 (King 1, 2 and 3)

Non legislative (unlike Sarbanes-Oxley) - apply or explain approach

King 3 incorporated Business Rescue and Risk Based internal audit

Many of the principles put forward in King 2 now embodied in the Companies Act of South Africa 2008
Professional support

Trusted global and local organisations

Continuity SA
- Your local centre of knowledge and subject experts
- Supports the BCI and professional leadership / excellence

TaGza (RSA)
- Affiliated to Continuity SA

BCI - Business Continuity Institute (Business Continuity)
- The Good Practice Guide (GPG)
- Local geographical forums

Worthwhile references

Business Continuity Management Systems
- Implementation and Certification to ISO 22301
  - Hilary Estall, ISBN 9 7817 8017 1463

BC for Dummies – instigated by UK Cabinet Office
Considerations B4 implementation

**B1 - Business Case**

You need a really enthusiastic sponsor - and one from “top management”

The person(s) who will manage implementation, maintenance and improvement needs to be qualified!

The Business Case must exemplify the benefits and approach

**B2 - Buy in of your Executives and Directors**

You’re on a non-starter if your executives are not keen - you need to do some serious sloooshing

You need to clearly identify the costs and BENEFITS over the life cycle of the BCMS

**B3 - Budget**

Don’t just look at resources to implement - look ahead at tools and complexity in delivering components

Get the budget secured - and own it

**B4 - Build relationships**

You MUST get buy in and support from across your organisation before you implement

You MUST engage your senior management on how you wish to approach the delivery programme

You MUST NOT get disheartened
ISO 22301 structure

Section 4: Context of the Organisation

Section 5: Leadership

Section 6: Planning

Section 7: Support

Section 8: Operation

Section 9: Performance evaluation

Section 10: Improvement
Section 1, 2 and 3

• Section 1: Scope of the standard
• Section 2: Normative references (there aren’t any)
• Section 3: Definitions

Do read the introduction
This part of the standard is about knowing what the business wants / needs

The standard wants ...
The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its BCMS.
The organization shall identify and document the following:

- the organization’s activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident;
- links between the business continuity policy and the organization’s objectives and other policies, including its overall risk management strategy; and
- the organization’s risk appetite.

In English ... 
The context will more than likely mature following the Business Impact Analysis (BIA) but you need to engage the business executives in the first instance to understand drivers, stakeholders and key mission statements around objectives, products and branding.

Most importantly there are some high level policies that need to be looked at - and possibly reviewed – such as the Enterprise Risk Management (ERM) policy and associated risk appetites.
Section 5: Leadership
This part of the standard is about leadership COMMITMENT

The standard wants ...
Top management shall demonstrate leadership and commitment with respect to the BCMS by
• ensuring that policies and objectives are established for the business continuity management system and are compatible with the strategic direction of the organization
• ensuring the integration of the business continuity management system requirements into the organization’s business processes
• ensuring that the resources needed for the business continuity management system are available
• communicating the importance of effective business continuity management and conforming to the BCMS requirements
• ensuring that the BCMS achieves its intended outcome(s)
• directing and supporting persons to contribute to the effectiveness of the BCMS
• promoting continual improvement, and
• supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.

In English …
This leadership and commitment can be shown by motivating and empowering persons to contribute to the effectiveness of the BCMS.

Commitment by leadership (top management) cannot be at arms length - they need to be actively involved.

Get your BCMS Policy in the right place, ensure roles, responsibilities and authority are communicated
Section 6: Planning

This part of the standard is about preparing your BCMS program

The standard wants ...
When planning for the BCMS, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to
• ensure the management system can achieve its intended outcome(s),
  • prevent, or reduce, undesired effects,
  • achieve continual improvement.

The organization shall plan
• actions to address these risks and opportunities,
  • how to integrate and implement the actions into its BCMS processes (see 8.1),
  • How to evaluate the effectiveness of these actions (see 9.1).

In English ...
This is all about setting up your program of projects to deliver all the elements of your BCMS. You do need to read a little ahead if you are implementing for the first time.
Section 7: Support

This part of the standard is about resources and documentation to support your BCMS

The standard wants ...
The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the BCMS.
- Competence, awareness, communications

The organization’s BCMS shall include documented information required by this International Standard, and documented information determined by the organization as being necessary for the effectiveness of the BCMS.
- Creating and updating, control,

In English …
Make sure people involved in the BCMS receive the right training and that their competencies are measured. The also need to keep up to date so regular training and awareness is essential.

Many companies do not have a Document Management System (DMS) - you will need to create one if this is the case. Documentary evidence is vital and it all needs to be neat and tidy.

DO NOT WRITE BOOKS
Section 8: Operation

This part of the standard is about the detail and making it work

The standard wants ...
The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by
• establishing criteria for the processes
• implementing control of the processes in accordance with the criteria, and
• keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

And then it continues with the serious stuff
• BIA and risk assessment
• BC Strategy (Determination and selection, resource requirements, protection and mitigation)
• BC Procedures (Incident response, Warning and communications, BC plans, Recovery), and
• Exercising and testing

In English ...
This is where a LOT of the work is done. The BIA is fundamental to the components that follow. Do your BIA properly and the rest will follow.
Section 9: Performance evaluation

This part of the standard is about monitoring, measuring, analysing and evaluating your BCMS.

The standard wants ...
The organization shall determine
• what needs to be monitored and measured
• the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results
• when the monitoring and measuring shall be performed, and
• when the results from monitoring and measurement shall be analysed and evaluated.

Key requirements;
• Internal audit
• Management Review

In English ...
If you keep a handle on all your activities and you record issues that could impact the business you will know where your BCMS weaknesses lie and you can do something about that - even if that means recording a non-conformity without a mitigation option. Just make sure you have a “plan” on how you will measure and evaluate your BCMS performance.

Your management review and some mechanism of audit is vital in this process.

DO NOT ENTERAIN ANALYSIS PARALYSIS
Section 10: Improvement

This part of the standard is about ongoing resilience development

The standard wants ...
When nonconformity occurs, the organization shall
• identify the nonconformity,
• react to the nonconformity
• evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by
• implement any action needed,
• review the effectiveness of any corrective action taken,
• make changes to the business continuity management system, if necessary.

The organization shall continually improve the suitability, adequacy or effectiveness of the BCMS.

In English ...
Things change, priorities change. Stay on top of your BCMS program and make changes in good time – don’t leave it until you are approached. Stay connected with the business.

There will always be some form of risk but its what you do to minimise impacts that count- and therefore why you need to constantly look for improvements to your BCMS.
A BCMS framework

The Core components of a framework
• Commitment, Governance, Ownership, Process

What the framework does
• A framework is not the finished product

Getting it all to work
• Embedding, Cultural change, Improvement, Maintenance
A BCMS Framework

Core components of the framework

A Policy signed by the CEO that prescribes;

- Terms of reference for the BCMS “Top Management” review board / forum / committee
- Terms of reference for your response structure
- A BCP - framework of requirements that satisfy the requirements of your organisation - and the standard

What the framework does
Clearly identifies those with BC Responsibilities and their authority

Sets a clear perspective of what will be delivered and who needs to be involved

Sets the foundation for continual review and improvement

Empowers people to think for themselves at the same time knowing they are loved

Getting it all to work
Someone must own the product

Someone must own the delivery

Someone must check its all working

People need to commit to the requirements of the BCMS - cultural embedding is core
Assessments and audits

The Formal (and informal) process
• Pre assessment, stages, ongoing surveillance, internal audit

Preparation
• Making sure your people have the BC culture

Your rights
• The good, the bad and the not so pretty
Audit and Assessment

The formal approach
Get a pre-assessment some time before certification
Engage an established supplier - watch the corporate politics
Make sure the supplier is properly prepared - AND competent
Set a schedule of interviews with the certification body
Structure and prepare for the audit visit
Do NOT go ahead if you are winging it
Bear in mind continued surveillance visits

The informal approach
Use an external consultant to give you a health check
Ask your internal audit team to focus on weak spots
Use an external body or peer industry to certify alignment
Do this every year and get the audit programme approved
Preparation

Internal gap analysis
Break the standard up - and identify common threads
Create an evidence matrix
Regularly measure compliance
Engage the top management review team - regularly
Identify non-conformities and risk to alignment / certification
Be very good at vulnerability and risk reporting
Be sympathetic about people’s day jobs - but do keep training them

Internal audit
There MUST be a schedule for internal audit
Your internal audit team are there to help the business - not punish it!
Let you audit team decide scope - but help them
During your internal audit be brave about the things you feel are weak
Do NOT be disheartened by audit reports - they will help your case
Internal audit reports must be seen by the CEO
Your rights

The good stuff - you gotta love it
You interpret the standard YOUR way
You use terminology that YOUR organisation is used to
You provide evidence YOUR way
You apply best practice to suit YOUR organisation
You improve the BCMS YOUR organisation's way
You train and make YOUR people competent YOUR way
It is YOUR BCMS and YOUR organisation - sell your BCMS like that!

The “bad” and not-so-pretty
Some auditors are punitive - watch the commercials ($$$)
Chasing evidence could remove the focus of the greater good
There are subtle “bullying” tactics that need to be avoided
Often - the spirit of all your good work is sunk by ignorance
Opinions can be reported out of context - can auditors have opinions?
The auditor report is final - or is it?
Many auditors are incompetent when relating to a BCMS
Benefits of a BCMS

Organisation benefits
- I want to keep my job - so PLEASE keep your business healthy

Certification benefits
- Why would you want certification - duh?

Benefits symbiotic with other disciplines
- Remain connected - remain resilient
Benefits

**Organisation benefits**
Improved resilience

Unprecedented improvement in behaviours

Transparent value-add vulnerability and risk methodologies

Supports corporate social responsibility - the way societal security was intended

**Certification / alignment benefits**
Reduce costs - repeatable visible processes:

Increase effectiveness - helps to demonstrate to customers and stakeholders that the business is run effectively; known goals and objectives; well understood standards and frameworks; Plan-Do-Check-Act cycle of activities; continuous improvement;

Reduce risk - remove uncertainty; perceived competence, dependability and openness; acknowledgement of following ‘best practice’;

Improve commitment - regular assessment will improve responsibility, commitment and motivation of personnel.

Reduces vulnerabilities and risk

Keeps existing business

Gains new business

**Symbiotic benefits**
Cross discipline consistency

A unified business - serious about keeping itself resilient
Symbiotic standards and disciplines

Pap en Wors
- Add some onions, tomatoes, garlic, chili and some Aromat
- It all comes together but it does take time - and experience

Core disciplines
- I love this chart - and it’s only a snippet of the main picture
Core disciplines

Compliance

Quality

Business Continuity

Information and Physical Security

Service Delivery

H&S / Environmental

Risk

Financial Control

Liquidity

Products & Services

Resources

Production

Stakeholders

ISO 9001 (Quality MS), ISO 9004 (QMS - Sustained Success), ISO 10005 (QMS - Quality Plans), ISO 19011 (QMS - Auditing)

SANS/ISO 22301 (Business Continuity MS), ISO 27031 (IT-ICT-Readiness for BC), *ISO 22398 (Exercising and Testing), PAS 200 (Crisis Management), *BS 11200 (Crisis Management), PD 25111 (Human Aspects), PD 25222 (Supply Chain), PD 25666 (Exercising), PD 25888 (Recovery)

ISO 27001 (IT-Information Security MS), ISO 27031 (IT-ICT-Readiness for BC), *PAS 555 (Cyber), ISO 27035 (IT-IS-incident Management), ISO 24762 (IT-ICT-Technology DR Services), ISO 28001 (Supply Chain Security MS), ANSI PSC0x (Private Security), BS8484 (Lone Worker Devices), *ISO 16xxx (Fraud), *ISO 5500x (Asset Management), EN 14383 (Prevention of Crime - Planning)

ISO 20000 (IT-Service Management), ISAE 3402 (Assurance), ITIL (IT Service Management), PRINCE II (Project Management), Agile (Project Management), SDLC (Service Delivery Life Cycle)

ISO 22000 (Food Safety MS), OHSAS 18001 (Occuptional Health and Safety MS), ISO 14001 (Environmental MS)


King Code of Governance, Sarbanes Oxley Act (SOX), PCI DSS (Payment Card Industry - Data Security), European Central Bank, Bank of England
Standards: Coming soon

Stuff being developed or considered
• It’s not over yet - and it may never be

Stuff that’s been/being binned
• Whoopee! But look out for future initiatives.
• Some people just won’t give up!

Get involved if you have an interest
• We all need to make sure that we are NOT overwhelming or complicating demands
Standards – and beyond

Stuff being developed or considered
BS 25999 has a lot to answer for - in a nice way
ISO 28000 - Supply chain - erm, or is it? (Marine and Shipping)
BS 45000 - Organisation Resilience - Guidelines
BS 11200 - Crisis Management - Guidelines (To replace PAS 200)
ISO 22398 - Exercising and Testing
ISO 16xxx - Fraud Countermeasures
ISO 55xxx - Asset management

Stuff that’s been binned
ISO 22323 - Organisational resilience: Gone back to the drawing board

How do YOU get involved
Find out who represents your constituency
Find out which committee represents your subject(s)
Join forums
Volunteer as a constituent representative - get your management approval first - lots of work
Publish your thoughts, views, objections
The 223nn suite from TC223 - SSM/1

The “Business Continuity” suite …

ISO 22300 Societal security - Terminology
ISO 22301 Societal security - Business continuity management systems - Requirements
ISO 22311 Societal security - Video surveillance - format for interoperability
ISO 22312 (TR) Societal security - Technological capabilities
ISO 22313 Societal security - Business continuity management systems - Guidance
ISO 22315 Societal security - Mass evacuation (WD)
ISO 22316 Societal security - Organisational resilience - Principles and guidance (WD)
ISO 22320 Societal security - Emergency management - Requirements on incident response
ISO 22322 Societal security - Emergency management - Public warning systems (DIS)
ISO 22324 Societal security - Emergency management - Colour coded alert (CD)
ISO 22325 Societal security - Emergency management - Capability assessment (WD)
ISO 22351 Societal security - Emergency management - Shared situation awareness (WD)
ISO 22397 Societal security - Guidelines on setting up partnerships agreements (CD)
ISO 22398 Societal security - Guidelines for exercises (DIS)
ISO 22399 (PAS) Societal security - Guideline on IPOCM

Beware of focusing on these standards in isolation.
For more information contact:
ContinuitySA
+27115548000
marketing@continuitysa.co.za

Our Speaker for the day:
Eugene Taylor  MBCI MIoD
Managing Director
TaGza (RSA and UK)
Eugene-Taylor@TaGza-RSA.co.za
Building structures vary and therefore so will their maintenance requirements

Let’s first look at the structure of the two documents and then examine a few examples of fundamental differences.

25999:
- Section 3: Establishing and managing the BCMS (Scope, Objectives, Policy, Resources, Competencies, Embedding, Documentation)
- Section 4: Understanding the Org (BIA, Risk assessment, Strategy, Developing a Response, Exercising, Maintaining, Reviewing)
- Section 5: Internal audit, Management review
- Section 6: Preventive and Corrective actions, Continual improvement

22301:
- Section 3: Context of the Organisation, Needs of interested parties, Determining Scope,
- Section 5: Leadership
- Section 6: Planning
- Section 7: Support (Resources, Competence, Awareness, Communication, Documented Information)
- Section 8: Operation, BIA, Risk Assessment, Strategy, Procedures
- Section 9: Performance evaluation
- Section 10: Improvement

So – not only are the structures different but there are additional language and considerably varying format requirements which may well attract different approaches during compliance assessments.

Those aligned or certified to BS25999 who might assume they could just copy and paste to comply with ISO22301 would be adopting a very dangerous approach.

So, more trees will need to be cut down ...

Documentation! Documentation! Documentation!

The fundamental difference is that compliance to 22301 requires a load more documentary evidence.

Have a look at section 8 of 22301 and you will notice there are now more onerous requirements on documented processes – quite a few of which were not requirements in 25999. Be especially wary of section 7 which has a lot to say about documented information.

In fact, 22301 mentions “documented” evidence requirements all over the place – some 27 clauses in contrast to 24 clauses in 25999. Don’t be fooled by this hint implying only a “little more” as the clauses requiring “documented” anything in 22301 are much more detailed and prescriptive.
For example:

**25999:**

4.1.1.1 Understanding the Organisation: BIA: There shall be a defined, **documented and appropriate method** for determining the impact of any disruption of the activities that support the organisation’s key products and services (see 3.2.1).

**22301:**

8.1c Operation: The organization shall determine, plan, implement and control those processes needed to address the risks and opportunities determined in 6.1 and to meet requirements, by keeping **documented information** to demonstrate that the processes have been carried out as planned.

8.2.1a The organization shall establish, implement and maintain a formal and **documented process** for business impact analysis and risk assessment that establishes the context of the assessment, defines criteria and evaluates the potential impact of a disruptive incident.

These quirky little twists in the language make the demand on compliance evidence much more voluminous, 25999 merely requiring a **method** while 22301 requiring **information** and **process** – both of which could become subjective issues.

**Just a little warning!** There are some clauses that require evidence but don’t specify “documented evidence” however when reading the clauses there appears no other way to provide “evidence” - other than by documented means.

---

**To the board we go ...**

This bit I really like! Section 5 of 22301 clearly requires “board level” leadership commitment and this means BCM cannot be shoved in some cupboard and brought out conveniently each year to be dusted off.

At this point it might be worth mentioning the “notes” within 22301. Whilst many of the clauses are clearly prefixed with references there are also a number of “notes” within 22301 and my guess is that auditors will use those for compliance requirements. So, while some clauses in 22301 may not reference requirements previously evident in 25999, the “notes” capture similar “indicative requirements”. Watch them!

---

**No more holidays for BC Practioners!**

For those looking to apply a BCMS for the first time and take the 22301 route life should be pretty peachy as 22301 has a very nice structure which could well define the implementation approach.

For those who have been aligned or been certified to 25999 there will be a significant rise in workload to meet the requirements. Removing the reference to “25999” in governance policies, associated BCMS documentation, awareness and training material will be a task on its own.

But – this is a good time to take advantage of 22301 to improve a BCMS which is currently structured under 25999. For instance the Policy and Governance structures now have a clear focus on leadership commitment and that may well improve the recognition and programme delivery of BC within organisations.

This will also be a good time to look at the organisation’s BC community resourcing to ensure capability able to fit the requirements of 22301.
Don’t ignore changes in language.

There is no mention of “embedding” in 22301 – promise! So does that mean that lovely outer ring in the diagram we have been proudly showing off over the past few years is now gone? Well – actually the whole diagram has gone! (Ref: BS25999-2:2007 figure 2 page 3). No! Embedding has not gone.

Quite simply the language in 22301 has changed (really to synchronise with other standards) and because ISO have a way of doing things that compel consistency across the various disciplines which have applicable standards. Quickly skim through the ISO/IEC Directive, Part 1 Consolidated Supplement if you really want to know a bit more.

25999 has a specific clause requirement for “embedding” (25999: 3.3a) while 22301 qualifies “embedding” under various clauses but ultimately expects top management to do this by ensuring the BCMS requirements are integrated into the business processes (22301: 5.2).

Yes – that reminds me. 22301 requires certain processes and that these are documented (more trees to cut down). More importantly (and subtle in many clauses) 22301 also requires information which supports processes and structures to be documented.

Are we better off?

Clearly 22301 is better structured and more specific on what is required than 25999 as it flows in a way one might typically implement a BCMS. While it may require more from practitioners initially, much of it ought to structure a simpler methodology for addressing routine maintenance of 22301.

The key improvements of 22301 which will encourage better methods of addressing resilience building and enhanced capability is the clear requirement of leadership involvement and commitment.

Because section 4 is a lot more specific about interested parties, products and services, there will be greater clarity on scope and understanding of what constitutes a component of the BCMS. That in itself will be an enabler for the leadership teams to be more focussed on strategy.

Ah, the strategy word! Interestingly enough strategy is emphasised in 25999 under “management review” (5.2.3c), whereas in 22301 this now has its own section (8.3.1) and follows the BIA section within the structure of 22301. This I agree makes sense!

In parting……

Read 22301 very carefully – it tends to say the same thing in a number of places which doesn’t mean you have to have a correlating number of documents or processes as you will just create duplication.

For example:

4.1b, 5.2, 5.3b, 6.2, 8.2.2, 8.2.3d, 8.4.1, 8.5, 9.1.2c and 9.3 all have some reference to Business Continuity Objectives.

22301 is a good standard, but by no means complete on its own if you want to develop your organisation’s resilience. Nonetheless 22301 is a valued component to support your business “firewall”.

Good luck!

Did you know...?

You can now follow us on Facebook
...stay in touch