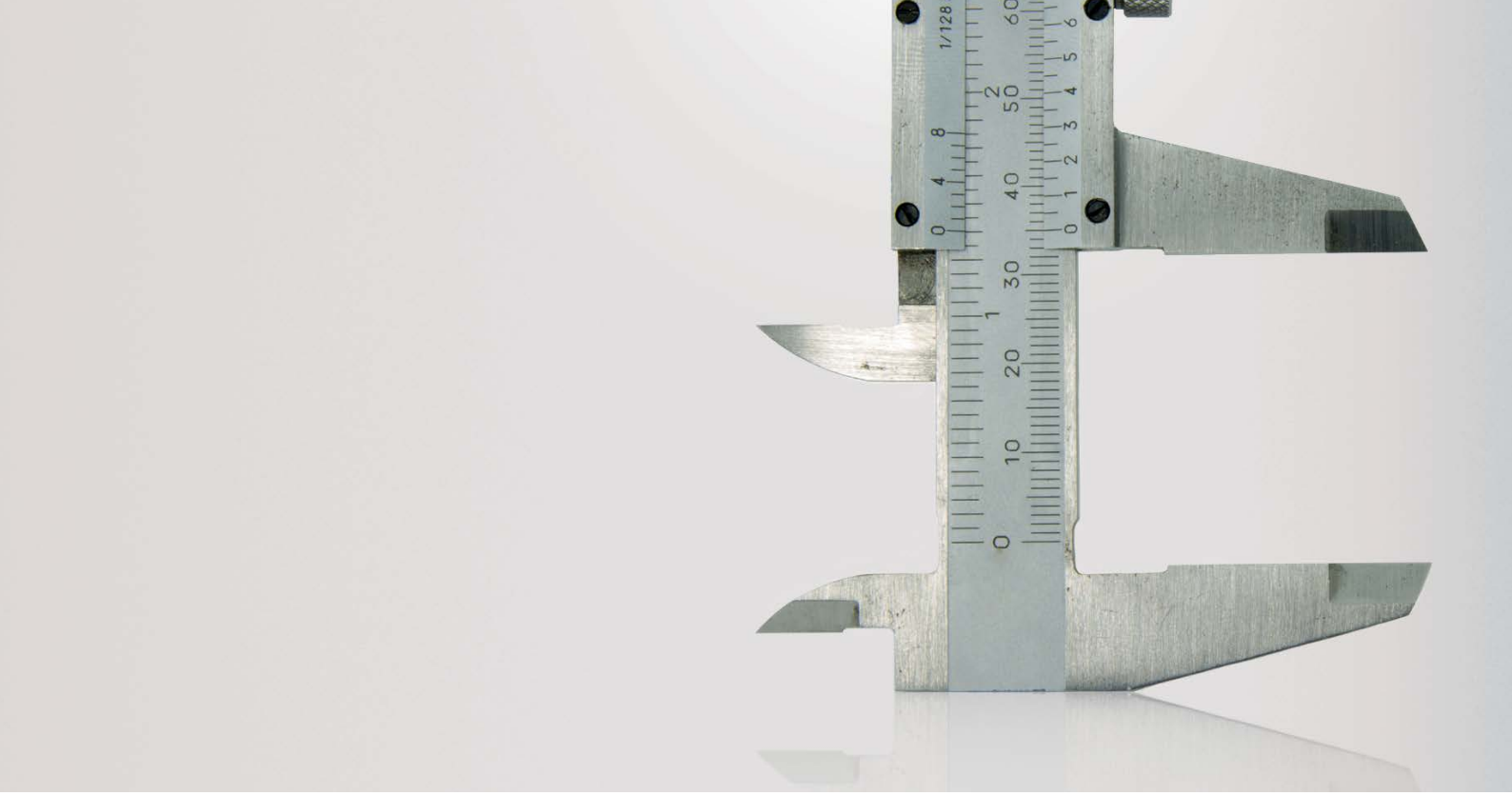

Measurement matters

The role of metrics in ISO 22301

A BSI whitepaper for business

bsi.

...making excellence a habit.™

Executive summary

- The business continuity standard ISO 22301 recognizes the importance of having accurate performance information
- The standard lays down requirements for "monitoring, measurement, analysis and evaluation"
- The emphasis on monitoring performance, measurement and metrics in ISO 22301 has caused confusion in some organizations
- This BSI whitepaper clarifies the requirements around measurement in ISO 22301
- Three BSI clients describe how they have approached these requirements

Measure for measure

"You can't manage what you can't measure" has become a cliché in business. Many managers will have this well-worn phrase pasted to a noticeboard or taped to their PC. But, in common with many clichés, the saying is fundamentally true – and valuable.

Nowhere is measurement more important than in the discipline of Business Continuity Management (BCM). Without measurement – or, more specifically, without the key performance data that monitoring and measurement provide – businesses cannot hope to evaluate their Business Continuity Management system (BCMS) effectively. Having the right information is vital, as without it informed judgements cannot be made when managing or improving an organization's BCMS. Above all, the overall value of the business continuity programme to the organization cannot be assessed.

The international BCMS standard ISO 22301 recognizes the critical importance of having accurate performance information and, unlike its predecessor BS 25999, this relatively new standard lays down requirements for "monitoring, measurement, analysis and evaluation."

Clarifying confusion

The greater emphasis on monitoring performance, measurement and metrics in ISO 22301 has been accompanied by a flurry of confusion in some organizations, as they ask:

- How do we assess whether our BCMS is performing as we want it to?
- What sort of metrics should we adopt and why?
- How are other organizations approaching the issues of monitoring, measurement, analysis and evaluation?
- What challenges have other organizations encountered when implementing the new requirements in ISO 22301 and how have these been overcome?

Lorna Anderson, Global Business Continuity Technical Manager at BSI, says, "In general, measurement within BCM systems is not done well." She suggests the problem stems from two main factors. First, business continuity professionals brought up on BS 25999 have not been schooled in the discipline. "It wasn't a requirement, so people simply didn't do it," says Anderson. Second, and more fundamentally, "They don't know what to do. They see the word 'metrics' and shout 'help!' We see organizations struggle, especially if they aren't heavily into standards – it comes more easily where the standards' mentality of plan-do-check-act is more ingrained."

ISO 22301 tasks Business Continuity (BC) professionals to:

- Monitor the extent to which their business continuity policy, objectives and targets are met
- Measure the performance of processes, procedures and functions that protect its prioritized activities
- Monitor compliance with the ISO 22301 standard and the business continuity objectives
- Review historical evidence of deficient BCMS performance
- Conduct internal audits at planned intervals
- Evaluate all this in the management review at planned intervals

Anderson puts it simply: "You need to determine what needs to be monitored and measured, what metrics you'll use to do it, when to do it, and what you'll do with the information."

When the results are analysed, she says, the key is for organizations to evaluate the performance and effectiveness of their BCMS, take action to address adverse trends before nonconformities occur, and ensure they retain relevant documentation of results.

Setting goals

Julian Thrussell, Senior Consultant at Ultima Risk Management (URM), a consultancy specializing in business resilience standards, agrees that organizations do not do metrics well – and adds a third reason for it. "They don't really know what their end goal is and therefore what they should be measuring. I often see metrics that are not as meaningful as they could be, such as how often the BC plan was updated, or how often it was reviewed. Whilst it's important to update BC plans, this is not their raison d'etre."

He continues, "Before organizations measure anything they need to work out what success looks like, so they have a benchmark and an objective to aim for. Before they can score anything as say, 5 out of 10, they first need to define the characteristics of 10 out of 10."

Experts agree that many organizations need to take a big step forward to a situation where they can benefit from using the most suitable metrics, to measure the most important variables, at the most appropriate times – providing them with valuable data that they can analyse and gain useful insights. They are then in a position to take action and improve the effectiveness of their BCMS and ultimately enhance organizational performance.

"Conducting a business impact analysis will provide a clear assessment of the organization's most important activities and will provide the basis of the BC plan. Just as a BC plan is unique to every organization, the things they are looking to protect and the importance of these activities are going to be unique too," says Thrussell.

"Too often though, there is just one overall objective in BC plans, so when organizations conduct an exercise they simply ask 'did the plan work as expected? Did it pass or fail?' What organizations should be doing is breaking down the plan into its key component parts, so during the exercise they record metrics around how the key component parts have worked, " suggests Thrussell.

He cites the example of how well a company performs, after an incident or a business continuity exercise, in contacting interested parties, such as customers, key suppliers, staff and investors. "Simply having a statistic saying the organization successfully contacted, say, 90% of their interested parties is not sufficient. What if a key customer was amongst the missing 10%? What would be the impact if this key customer then received information about the incident from social media, rumours and the press?" Thrussell suggests that the organization needs to break the metric figure down into different types of interested parties and ensure all interested parties are identified. Each of these categories will require input and information from different people within the business to ensure the accuracy of records. Furthermore, if these records are not accurate there needs to be a corrective action process in place. If for example, a customer contact detail has not been updated and this has resulted in a 'non-contact', it will require a corrective action from the sales director to 1) correct it and 2) ensure it does not recur. Likewise, if there is an error in the shareholder register, the company secretary will need to address it. "Passing or failing the plan as a whole is not terribly valuable when some aspects have worked very well and others require improvement," says Thrussell. "Success is about accuracy and attention to detail."

Unknown unknowns

"There are **known knowns**; there are things that we know that we know.

We also know there are **known unknowns**; that is to say we know there are some things we do not know.

But there are also **unknown unknowns**, the ones we don't know we don't know."

Donald Rumsfeld, US Defense Secretary, 2002

Business continuity experts agree with Donald Rumsfeld, in the sense that simply auditing your plan and putting metrics against what you already have only goes so far – because you will not find things that are entirely missing from the plan.

"To discover the unknowns, run an exercise with a business unit, stressing that it's not a pass/fail test, but an exercise that is designed to improve the organization's response to an incident and ensure nothing falls between the gaps," suggests URM's Thrussell. "An exercise will show you very quickly and publicly what works and what doesn't. That understanding is invaluable to a BC manager, who can use objective metrics that other people have fed into, for improving the plans and validating the time and money being spent on business continuity. It is better to discover a problem during an exercise than during an incident. Would you rather identify the out-of-date contact details in an exercise or when that key customer is on the phone to you demanding a response to rumours circulating on social media?"

Beyond the numbers

While the requirement for effective measurement suggests a wider range of metrics and collecting more information from more places, BSI's Anderson stresses that the quality of data is more important than the quantity. "It comes back to having objectives that are 'SMART'– Specific, Measurable, Achievable, Relevant, and Time-based. They also need to be 'DUMB' – Doable, Understandable, Manageable and Beneficial."

Anderson summarizes, "People have done 101 different things and we need to bring some sense to this area. Metrics are simply agreed objective, actionable measurements that reflect your critical success factors."

Performance evaluation

Clause 9 of ISO 22301 brings together the maintaining and reviewing of a BCMS.

Clause 9.1 Monitoring, measurement, analysis and evaluation is a set of requirements designed to ensure that appropriate metrics are in place to effectively manage the BCMS and provides the input to management reviews.

Clause 9.2 Internal audit – includes a requirement that the management responsible for the area being audited must "ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results."

Clause 9.3 Management review – includes a new requirement to provide information for the review on the trends in:

1. Nonconformities and corrective actions
2. Monitoring and measurement evaluation results
3. Auditing results

Additionally, when considering the output from the management review, changes may be required to risk reduction and security arrangements and operational conditions and processes, if appropriate. It may also be appropriate to change the measures for "how the effectiveness of controls are measured."

This clause concludes with a requirement for the organization to "communicate the results of management review to relevant interested parties, and take appropriate action relating to those results."

9.1 Clause for thought

Clause 9.1 of ISO 22301 specifically states that, "a compliant organization shall determine:

a. What needs to be monitored and measured
b. The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results
c. When the monitoring and measuring shall be performed, and
d. When the results from monitoring and measurement shall be analysed and evaluated.

The organization shall retain appropriate documented information as evidence of the results.

The organization shall evaluate the BCMS performance and the effectiveness of the BCMS.

Additionally, the organization shall:

- Take action when necessary to address adverse trends or results before a nonconformity occurs, and
- Retain relevant documented information as evidence of the results.

The procedures for monitoring performance shall provide for:

- The setting of performance metrics appropriate to the needs of the organization
- Monitoring the extent to which the organization's business continuity policy, objectives and targets are met
- Performance of the processes, procedures and functions that protect its prioritized activities
- Monitoring compliance with this International Standard and the business continuity objectives
- Monitoring historical evidence of deficient BCMS' performance*
- Recording data and results of monitoring and measurement to facilitate subsequent corrective actions.

(* Deficient performance could include nonconformity, near misses, false alarms, and actual incidents).

Case study 1: Allen & Overy

Not just numbers

UK law firm Allen & Overy LLP employs over 5,000 staff, including more than 500 partners. Founded over 80 years ago, it has built a global network spanning 45 offices in 31 countries and is the only firm to have been ranked in the top three of the FT Law 50 since it began in 2006.

As a leading legal player, Allen & Overy's ability to serve its clients at all times is paramount. It maintains certification to ISO 22301 for its London and Belfast offices, audited by BSI, to ensure its business continuity management system is always robust.

Clive Restall, Senior Manager Global Resilience, says, "When I started out with ISO 22301 and its requirement for metrics, I struggled with it. Metrics is a word that needs careful interpretation and application. We could measure many numbers and values – for example, how many people can log on remotely to our systems at any one time; or how many seats we have at our remote recovery site – but I wouldn't necessarily relate these statistics to how well our BCMS is performing. They don't tell me whether our plan is good, bad or indifferent."

Business continuity planning is not a function that produces tangible outputs such as motor cars or widgets, and Allen & Overy is a service business with no physical products either. "The issue of metrics posed a difficult question for us as to what to count or measure," says Restall. "I also wanted to keep the chosen measures straightforward so they would be understandable to all my stakeholders."

Restall's starting point was to list all the things he undertook as part of maintaining an effective BCMS – "things that we could look back on at management review and say whether we'd done these things or not. Some of them had a quality element, where I don't just want a tick in the box, I want to make sure I've got something worthwhile".

Restall's high-level metrics consists of:

- Management review – twice a year
- BC plan review – set of review meetings and plan reissue process – twice a year
- Gold team exercise – once every two years
- Business recovery team exercise – every two years
- Automated cascade exercise – annually
- Recovery test at our professional work area site – annually
- Internal audit – three-yearly rolling programme
- ISO audits – three-yearly rolling audit and recertification programme
- Other documents are reviewed, as required
- Staff training and awareness – three-yearly rolling programme and annual census

The list creates a calendar of regular monitoring events, creating a picture of how the BCMS is performing and providing all the information required to exercise management control.

"At management review meetings, I expect to report that all these things I've undertaken to do are on track," says Restall. "But clearly there are going to be issues raised that will lead us to identify actions for improvement. For example, when remote working was first introduced at A&O, we assessed our ICT capacity for staff to work offsite. It was fine for our day-to-day needs, but in the event of an emergency we might have been lacking. We've now increased that capacity to a high level. If we fail to follow through on the actions, this will be picked up either at management review or by one or more of the auditors."

"We don't leave it there," says Restall. "We sometimes carry out additional activities to add confidence. For instance, we recently invited an external agency to do a review of our BC plan arrangements. It wasn't something required by the BCMS or by auditors, but we decided we wanted an independent report that went more into our BCMS's fitness for purpose."

He concludes, "You can apply some numbers to the high-level metrics I've cited, but numbers alone don't go far enough. It's all very well to say, 'yes, we've had two management review meetings' and put a tick in the box, but what was the quality of them?"

He concludes, "What we need to be asking is: what are the things we should do? Have we done them? And, what is their quality and value? The management review process exists to ensure we're satisfied with the answers."

Case study 2: ScottishPower

Metrics maturity

ScottishPower, part of global utilities group Iberdrola, supplies electricity and gas to millions of homes and businesses around the UK. Headquartered in Glasgow, its operations include electricity generation, transmission, distribution and retail.

Ben Woodall, Business Continuity & Communications Manager, describes the company's BCMS as "pretty mature in terms of knowing our business and knowing ISO 22301, and bringing the two together."

He continues, "We've always had business continuity in some form at ScottishPower, but the process was reinvigorated in 2007. We went on to become certified to BS 25999 in 2008, before transitioning to ISO 22301 in 2012."

Prior to implementing ISO 22301, Woodall and fellow Business Continuity Manager, Katherine McNamara, brought together the BCM systems in ScottishPower's Retail and Generation businesses, which were previously certified separately. With office and power station environments differing significantly, the process revealed a host of different tasks and metrics that needed to be rationalized and recorded more efficiently.

The starting point was to redefine the objectives from two management systems into a single BCMS and these have been further refined since, so there are now 10 objectives:

1. Align and certify to the most relevant or beneficial standard for business continuity
2. Deliver the Retail and Generation BCMS within the agreed and allocated budget
3. Fully understand the organization and develop a robust and enduring continuity response in critical areas and activities
4. Exercise and test continuity arrangements and plans to ensure suitability
5. Work with our internal IT providers to ensure IT disaster recovery arrangements are appropriate for the Retail and Generation businesses
6. Provide appropriate training and awareness of the BCMS to further develop the continuity culture within the Retail and Generation businesses
7. Maintain and continually improve the BCMS to ensure it remains current, appropriate, effective and aligned to industry standards and best practice
8. Develop and maintain relationships with national government, devolved government and local emergency planning groups
9. Manage existing and emerging external continuity considerations (in essence, understanding customers and suppliers)
10. Review and maintain continuity-related risks and threats to the Retail and Generation businesses

The objectives align loosely to a plan-do-check-act methodology and also to the requirements of ISO 22301.

McNamara explains, "Having set the objectives, we define the actions that will allow us to complete each one, breaking them down into a manageable annual operating plan, with monthly checks and controls – which include a number of metrics and measurements we use to ensure we're on track."

No metric is required for objective 1 and fairly obvious financial budgets are applied to objective 2, but, says McNamara, "The way staff have performed in training, for example, is a relevant metric for objective 6."

Woodall describes how objective 3 involves multiple activities and metrics. Objective 3 is delivered by four key actions: define the BCMS strategy; complete the business impact analyses (BIA); create the recovery plans; create pandemic or people-impact plans. Against each one is a metric. In the case of the BIA, for example, ScottishPower has identified 25 BIAs it plans to review in 2014. Logically, there are also 25 recovery plans. Due to the nature of pandemics, there are 16 site-related (as opposed to department-related) pandemic plans, corresponding with 16 company sites.

Woodall and McNamara explain that, for many of the other objectives, ScottishPower's BCMS draws upon numerous metrics, from the strategic to the tactical level, to inform management, drive corrective actions and maintain compliance with ISO 22301.

The standard does not dictate what metrics ScottishPower should use. It gives the flexibility for the company to select measures, scoring systems and benchmarks that are both easily accessible and useful. In reporting to management, for example, the company's BC professionals use a simple traffic light system – red, amber and green – to flag up issues relating to its 10 BCMS objectives.

Woodall concludes: "It gives the senior management team a really quick and clear understanding of where our management system is and what we're doing about it, when throwing numbers at them probably isn't going to help them."

Case study 3: Telefónica

Cutting complexity

Telefónica is one of the largest telecommunications companies in the world in terms of market capitalization and number of customers. The Spanish multinational employs around 120,000 people and has a significant presence in 24 countries, and is better known in the UK as the mobile network operator, O2.

David Clarke, O2 Business Continuity Manager for Telefónica UK Limited, says he has found ISO 22301 much more explicit in its reporting requirements than its predecessor, BS 25999. "For example, you have to report to senior management annually on how many nonconformities with the standard you've had."

He adds, "The value in frequent tracking and trending is that you identify risks and take steps to mitigate them sooner."

Clarke says the company's starting point for business continuity metrics was to "look at what we do". "We've thought through what an incident is and have gone on to categorize all the different types of incidents that might affect us from 'major' to 'minor', using a scoring system that runs P0, P1, P2, P3 etc," says Clarke. "The benefit of this is that people across the organization are familiar with these categories, so they immediately understand the level of seriousness of any incident being referred to."

He continues, "We know how many incidents we have in each category and we also know how many system failures there are, so we have metrics internally that give us a clear picture of what's happening. But the people that businesses tend to forget are partners and suppliers. So we've built it into our contractual requirement of suppliers that they have to keep track of, and tell us, how many incidents have impacted on their service to us."

This is key, according to Clarke, because internally any company maintaining certification to ISO 22301 will manage itself effectively, but often they are dependent on external third parties.

"In reality, we can't always track every small suppliers' performance against this requirement, but we can monitor key suppliers and partners, such as the outsourced provider of our sales and service operation. It provides us with external data where we would otherwise be in the dark," he adds.

An important external measure is O2's customer satisfaction index (CSI) score, which is independently validated by a third party. "We track our CSI score across every part of our business, so it highlights service interruptions, recurring incidents and business continuity problem areas," says Clarke.

"Another metric we know is the number of times a BC incident is declared, and again we require our suppliers to report to us how many times they've had an incident. With this data, we can analyse the history and see if we are hitting a particular problem at a particular time."

The company can also draw on data from its internal audit function and from an external company that provides it with quality checks.

O2 is monitoring compliance with ISO 22301 too. For every incident it has a post-incident review and uses an internal accredited body to review compliance against the standard. The company aims to correct nonconformities within six months and keep documentation up to date.

"We have to be monitoring and measuring for a six-monthly report to the board, as well as for BSI to audit us to ISO 22301," says Clarke.

"But it's so easy for people to do. You don't have to invent new measures – clause 9.3 within the standard on management review tells you everything you've got to look at."

For O2, the issue of metrics involves a host of numbers – for example, the number of incidents, the scoring of those incidents, the number of nonconformities, CSI scores and so on. But, says Clarke, "the heart of the issue goes beyond numeric values and measures".

He concludes, "The terminology in the standard uses the terms 'metrics' and 'measurement' and some firms have got really hung up about these words, creating excessively complex processes. But the standard allows companies to define what 'metrics' means to them. We've tried to stick to plain English and straightforward measures that we were already doing."

Taking action

BSI's Anderson leaves organizations with the following questions to help them start on their approach to metrics. "Organizations must remember that if you're going to invest in BCM and wish to have a clear view on the health of your BCMS, then you need to track its performance. In other words, your BCM metrics constitute your BCM scorecard, the way you figure out where you are. To use another term, they form your dashboard. So, when considering your metrics please ask yourself the basic 10 questions:"

1 Do your metrics link directly back to your BCMS and its objectives?

2 Will the metrics drive improvement and progress?

3 Do your metrics follow the SMART principle:

- **S** = Specific: clear and focused to avoid misinterpretation. Should include measurement assumptions and definitions, and be easily interpreted.
- **M** = Measurable: can be quantified and compared to other data. It should allow for meaningful statistical analysis. Avoid "yes/no" measures except in limited cases.
- **A** = Attainable: achievable, reasonable, and credible under conditions expected.
- **R** = Realistic: fits into the organization's constraints and is cost-effective.
- **T** = Timely: doable within the time frame given.

4 Does each metric include a clear statement of the expected results?

5 Does each metric focus on effectiveness and/or efficiency of the element being measured?

6 Does each metric allow for meaningful trend or statistical analysis and include milestones and/or indicators to provide qualitative feedback?

7 Are your metrics challenging, but at the same time attainable?

8 Have assumptions and definitions been specified for what constitutes satisfactory performance? Is it clear what 'good' or compliance actually looks like?

9 Have those who are responsible for measuring performance been fully involved in the development of the metrics?

10 Do your metrics allow for clear reporting to their intended audience?

bsi.

BSI New Zealand
Level 10
21 Queen Street
Auckland 1010
New Zealand

T: 0800 583 965
E: info.nz@bsigroup.com
bsigroup.com/en-nz