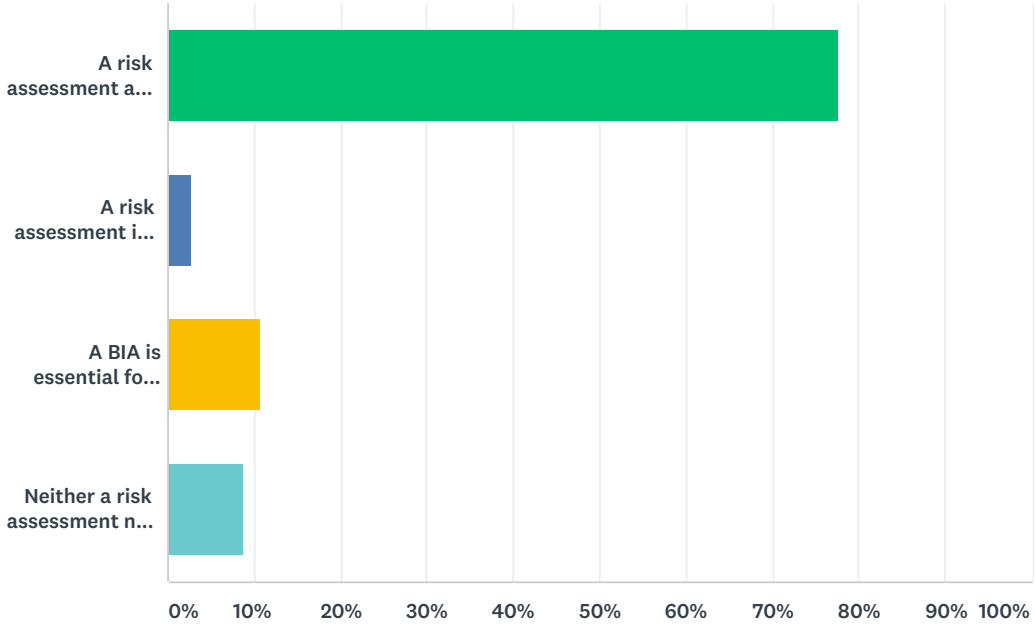
Q6 Thinking about compliance with the business continuity standard stated in Q5, which comes closest to your view:

Answered: 260 Skipped: 8



ANSWER CHOICES	RESPONSES	
A risk assessment and a BIA are both essential for compliance with this standard	77.69%	202
A risk assessment is essential for compliance with this standard but not a BIA	2.69%	7
A BIA is essential for compliance with this standard but not a risk assessment	10.77%	28
Neither a risk assessment nor a BIA are essential for compliance with this standard	8.85%	23
TOTAL		260

#	IF YOU HAVE TIME PLEASE EXPLAIN YOUR ANSWER TO THIS QUESTION:	DATE
1	The standards are what keep us relevant and they are important. However, to be certified, you need to put a LOT of work into what they ask for. It isn't worth it for every company. I just left a company of 100,000 employees and my opinion was the same for that organization. :-)	6/9/2019 6:09 PM
2	It will never be about "what standard do you use" - rather what components from all of the standards fit the culture and the risk appetite of the company. There should never be a total elimination of either Risk or BIA - but rather determining business impacts and risks based on what's important to the business culture. Needs to be scaled down versions of the original "full blown assessment" that fit the culture and the business's risk appetite, and based on those best practices that fit the business climate (which most of the time, are plucked from the various standards, not to mention there is overlap between the standards).	6/5/2019 10:00 PM
3	I think this is precisely the wrong questions to ask. I strongly believe that in order for the discipline and the profession to be relevant for modern times and for the evolving workplace of the future, we should not be emphasizing compliance with the standard but build an evolving enterprise capability which helps the organization to survive disruption shocks in realtime or near realtime. The true value is not in complying to procedural and documentation heavy standard but rather in building a fit for purpose capability response which when disaster strikes, helps preserve if not boost reputation, share value and the customer perception of the organization.	6/3/2019 6:23 PM
4	It is about a management system not about having functional solutions in place which is why the Standards have always been weak and of little use. But again great for consultants as can charge huge amounts to create all the paper work.	6/3/2019 2:13 PM

5	Certifications have become a little industry that seems to be getting larger. Customers need to understand that their supply chain is resliliant and holding these certifcations adds some credence and acceoptance that they do. We still have regular customer audit to understake even with BC and risk addressed under 27001 and whihc we are regularly audited by the BSI	6/3/2019 10:17 AM
6	Risk assessments are managed by the organisation's Audit and Risk Unit. The organisation's risk and consequence matrix is used to measure the impacts overtime and to validate BCM RTOs and MAOs. Any new risks identified during the BIA phase are forwarded for consideration and potential inclusion on the organisation's risk register	6/3/2019 1:49 AM
7	It depends on the auditor but typically BIA is requested.	6/1/2019 9:16 PM
8	If BC professionals insist on using traditional BIA and Risk Assessments, their leadership teams will continue to lose confidence in their work. BC professionals need to become more flexible and, unfortunately, the interim results of this survey show too many are stuck in the same old methods and unwilling to flex. If you're unwilling to flex, be prepared to be the first up on the chopping block when business gets tough...you'll be seen as "optional".	6/1/2019 8:01 PM
9	Remove either the BIA or RA and the process will be the poorer for it.	6/1/2019 6:43 PM
10	Going through these processes helps educate the leaders in what business continuity is.	5/31/2019 4:10 PM
11	The standard allows you to make your own choices - however it does advise that if you don't do something, write down your reasons for not doing it.	5/31/2019 2:44 PM
12	Section 8.2, paras 8.2.1, 8.2.2 and 8.2.3	5/31/2019 1:42 PM
13	Both the BIA and risk assessment are required however, each one should be done independently of each other for improved results	5/31/2019 11:18 AM
14	Section 8.2 requires this.	5/31/2019 9:26 AM
15	A BIA is essential, however on the whole it is not essential to comply with any standard whatsoever to deliver a good program.	5/31/2019 12:38 AM
16	I don’t relate the word ‘compliance’ to using Standards, but in this case these 2 processes, whether completed formally or informally, underpin continuity arrangements.	5/30/2019 11:01 PM
17	Don't know	5/30/2019 10:01 PM
18	Na	5/30/2019 9:55 PM
19	They are called for specifically.	5/30/2019 8:52 PM
20	This is the old question of compliance versus adherence. Compliance indicates you are doing it for a certification. Adherence indicates you are doing it just because it's good business.	5/30/2019 6:21 PM
21	Standards including NIST utilize familiar words and concepts. At the end of the day, if the assessment yields a prioritization and timeframe for processes what it is called is not material. That said, it is true that some audit plans still check a box looking for terminology.	5/30/2019 6:13 PM
22	Can work with an auditor to show that your methodology aligns (same or better) with compliance.	5/30/2019 6:12 PM
23	For compliance with the standard you still need a RA and BIA - however, the question is: does the standard provide value by requesting two practices that don't have a value added?	5/30/2019 4:37 PM
24	As per comments indicated	5/30/2019 4:25 PM
25	ISO 22301 is useful as a guidance, but for us the local regulatory requirements are essential.	5/30/2019 3:25 PM
26	It is imperative for this standard for our company to follow a risk based strategy to BCMS. A large part of our audit evidence to cover the standard and clauses specifically section 8 is where we use our risk assessment/reporting and BIA's.	5/30/2019 3:03 PM
27	or should be.....	5/30/2019 2:36 PM
28	Compliance and the actual identification/mitigation/monitoring of risk and potential business impacts are not totally compatible - i.e., you can be in compliance and miss critical risks, potential impacts due to the nature of operations today.	5/30/2019 2:35 PM
29	BIA is without a doubt necessary. Identifying individual processes and MTOs, technology assets, office equipment, people etc. A BCP without a BIA is in my opinion useless. The BCP SHOULD be an All-Hazards approach in theory, but in practice different organizations/business are exposed to different hazards that have significantly different impacts on the business and the BCP Strategies. Hazards aren't uniform and strategies can't necessary be universal. However, I do think that there is opportunity for the risk assessment to be outsourced to the risk management department if necessary; or for a more uniform approach.	5/30/2019 2:21 PM

30	If you can explain where your Risk Assessment is conducted (perhaps in another portion of a large corporation) then that is fine, just need to document. And the BIA is necessary, just need to capture the information but can be collected in different manners.	5/30/2019 2:12 PM
31	No internal auditor or external regulator will accept a report without both. A well crafted BIA, approved by Steering committee is priceless.	5/30/2019 2:09 PM
32	Risk assessments are not unique to the BCM process so if you are risk aware and plugged into the risk management system, and actually manage risks (in addition to writing them down) but haven't delivered a separate risk assessment, I'm not going to mark you down. If you haven't worked out what needs to be in scope of your programme and your plans, I'm going to question whether it's protecting the right things; over or under scoped. How do you know?	5/30/2019 1:39 PM
33	it is a requirement, the impact over time issue though does cause us a problem.	5/30/2019 12:56 PM
34	The BIA shows the functions of each business area; work can then be prioritized based on importance to entity survival. A Risk Assessment tells what are the most probable risks and which are the most damaging if they occur. Intersection of the two helps to provide the priority for work completion.	5/29/2019 5:37 PM
35	The RA is usually at a very high level and covers universal risks that impact all areas of the enterprise. Those risks could inform what questions are included in the BIA; for example, a regional earthquake risk would prompt BIA questions related to alternate work areas, unavailability of employees, damage to resources, etc.	5/24/2019 7:39 PM
36	The BIA and RIA are the basic to make the right decisions what to do preventive and repressive	5/24/2019 5:58 PM
37	Understanding the risks and impacts to our business from loss of services (facilities, people, etc.) is critical to building resiliency in our business. Developing sound recovery procedures is impossible without a clear knowledge of both risks and impacts.	5/21/2019 5:27 AM
38	The problem is that the people who are making the standards are not representative at all of the overall BCM practitioners population.	5/15/2019 2:01 AM
39	I recognise that both BIA and RA are required to be compliant with ISO22301/313, and I often do both. However, I have done BCM projects in the past for organisations where BIAs were conducted to inform BCPs and RAs were left out, and this worked okay given the contraints, environment and maturity level of the organisation.	5/14/2019 1:09 AM
40	Required - full stop !	5/10/2019 1:55 PM
41	This is what the lawyers might call a "leading question." As Mark Armour pointed out in his response to the first survey, yes, the standards do indeed call for a risk assessment and BIA but, no, it doesn't necessarily follow that the requirement is based on any demonstrated return of value for the effort. We need to keep in mind that the standards are developed and maintained by committees whose members are generally NOT selected because they've developed reputations for being industry "radicals" who challenge the collective sense of what constitutes "good practice." Their results will, quite predictably, reflect a strong bias towards the status quo ante.	5/9/2019 7:01 PM
42	If we didn't have a full suite of Risk assessments and BIAs we would not be certified against the ISO 22301 standard.	4/26/2019 3:23 PM
43	Strictly, the ISO does require a risk assessment. However, we aim to "align with" rather than "comply" so we can flex our risk and BC processes accordingly.	4/23/2019 3:55 PM
44	ISO 22317 outlines better than ISO 22301 why we do the BIA	4/18/2019 6:10 PM
45	A RA and BIA are required as part of the NFPA standard.	4/17/2019 5:31 PM
46	The answer applies to Adaptive - it is not necessary to do a risk nor a BIA to get the desire outcome: being better prepared	4/11/2019 9:27 PM
47	we are not certified so follow requirements loosely to fit business needs but both are felt as needed even if we dont have full engagement / understanding of the exec team	4/11/2019 7:42 AM
48	While none of my employers have been obliged to comply with any BC standard, I view them as guidance for establishing a robust framework and have introduced them into the process.	4/11/2019 2:53 AM
49	Section 8.2 of the standard advocates for both BIA and RA	4/10/2019 7:57 PM
50	The Risk Assessment and BIA are methods for gathering information. The plans are key to recovery. I would say a hybrid approach to identify the critical areas by priority of the business. Work with the business to assist with collecting and documenting key processes (including manual method), resources and dependencies to operate the critical area. It is hard to get the proper attention needed to gather the risk and BIA, then come back and figure out the recovery plans. Sometimes you get one shot because everyone is busy.....	4/10/2019 6:30 PM

51	The FFIEC guidance is specific on both the BIA and Risk Assessment	4/10/2019 6:29 PM
52	Compliance with a six year old standard may not represent an appropriate approach the current technologies employed.	4/10/2019 5:09 PM
53	A risk assessment and BIA will tell you what is likely to go wrong. Which can be reduced to a handful of options (loss of facility, loss of utilities, communications, people). Focusing on the core issues just gets straight to the point. The effort to identify that earthquakes, tornadoes, etc... will result in a power outage should be common sense. My organization works out of 139 different facilities. Running 139 different risk assessments or BIAs based on location is just not possible. It is also pointless to try to undertake a single or grouping of these facilities as each is significantly different. Covering a baseline of possible disruptions is much simpler in a large organization.	4/10/2019 4:21 PM
54	Just because it is in the standard does not mean it is actually adding the most value to the organization. Further work is needed to ensure, from a compliance perspective, businesses are able to 'demonstrate' their own effectiveness to disruption events. Currently, compliance to the standards can be as simple as showing the right bits of paper are in place. (based on my years of being on the receiving end of audits) It is far and away from a practical measurement of resilience.	4/8/2019 6:07 AM
55	The need for time consuming and expensive BIA/RIA analysis is a major reason for firms not seeking certification against this standard	4/5/2019 11:04 AM
56	They are mandatory requirements for all industry standards.	4/5/2019 1:21 AM
57	Risk has its place but must not impede true BC planning. The BIA has been taken over by over thinking and cumbersome questionnaires and software products. Let’s get back to KISS principles. Have conversations with the business and endure dependent processes are in the conversation together to endure criticality end to end is captured. I believe good BC practitioners do this already but newbies tend to over complicate and use template approaches.	4/5/2019 12:43 AM
58	The outputs from each are important but the same information can be obtained using different, less traditional approaches.	4/4/2019 5:25 PM
59	That’s why we don’t follow the standard. BIA and RA don’t make sense.	4/4/2019 4:02 PM
60	I have a very poor opinion of this Survey and hope that you realize that giving space and voice to inexperienced people like those in ABC is NOT a good idea. It does not help making the world more resilient, it just helps mediocrity insinuating in a serious, professional environment.	4/4/2019 3:57 PM
61	That's what the ISO says in clause 8.2.1: 'The organization shall establish, implement and maintain a formal and documented process for business impact analysis and risk assessment.'	4/4/2019 1:53 PM
62	Standards are guidelines. There are ways to be more effective in the business continuity space while still satisfying the spirit in which the standards were written. Though it still depends on the auditor or regulator’s interpretation.	4/4/2019 1:36 PM
63	Both activities are essential to compliance with those standards; but I continue to believe the requirements of the standards are out of date and in need of revision.	4/4/2019 1:14 PM