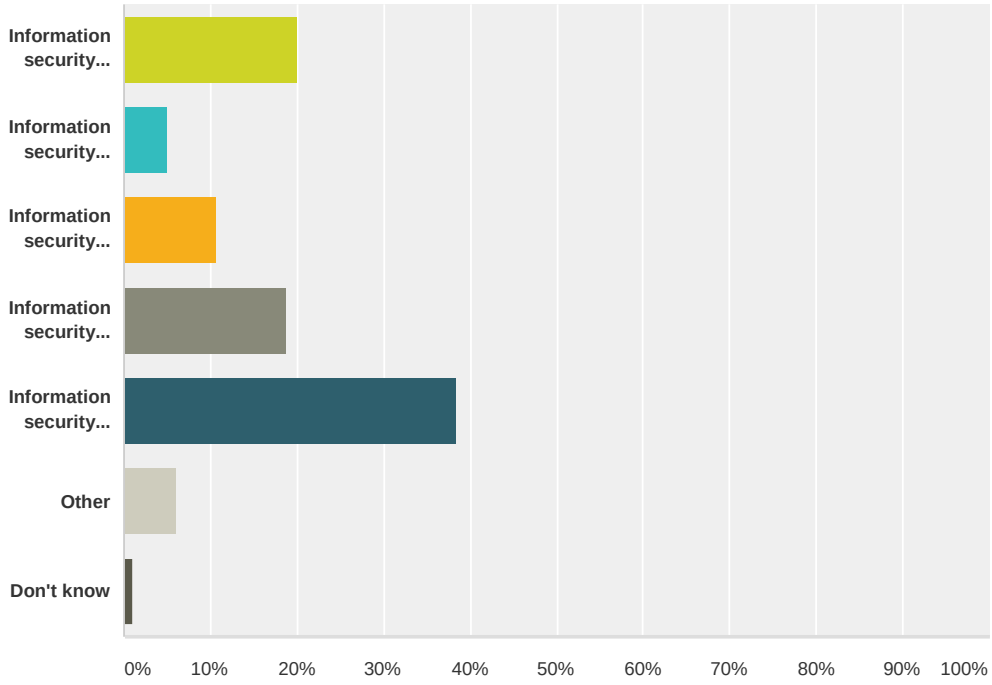
Q5 Which of the following comes closest to your opinion?

Answered: 180 Skipped: 2



Answer Choices	Responses	
Information security management should be led by the IT department / business unit	**20.00%**	36
Information security management should be led by the business continuity team	**5.00%**	9
Information security management should be led by the Board	**10.56%**	19
Information security management should be led by the risk management team	**18.89%**	34
Information security management should be led by a team consisting of representatives from different areas of the organization	**38.33%**	69
Other	**6.11%**	11
Don't know	**1.11%**	2
Total		**180**

#	Optional: Please explain your response to this question
1	Information is held across the organisation in many forms. One size fits all is unlikely to work.
2	Security, and especially IT security, is a behavioural issue and involves everyone.
3	The risk management team has good understanding - hence they can easily classify the various risks and assign it to the appropriate team for investigation.
4	It should not be seen as an IT or BC issue rather an organizational issue where many stake holders need to play their role
5	Different kinds of interruptions need different skill sets but the incident management process should be the same ... just different teams and different sill sets.
6	Operational Implementation should come from a Protective Services / Organisational Resilience Unit.
7	This is not how it is currently in my organization. Info Security is lead by independent CISO and team, includes Continuity and works closely with IT division.
8	IT needs direct management responsibilities for the technical matters but overall planning and strategic oversight needs to come from other management perspectives.

9	Led by IT but with strong partnership / collaboration with other key areas ie business continuity, risk management, internal controls,
10	I believe this is somewhat dependent on the size and scope of the organization.
11	IT dept. is responsible for the security measures in place. IT knows how to best resolve an incident. Other areas (i.e. Legal, Business) would have roles in the Incident Response but it is IT that owns it.
12	Business continuity should focus all protective activities
13	Should be left to the professionals and those closest to the management processes
14	Information security is a business-wide matter and, as such, must not be a delegated responsibility.
15	The board will need to delegate to appropriate teams. Different solution required depending on the structure of the business and demands of each industry/local-global environments.
16	Information security management should be led by a Organisational Resilience Team which includes other disciplines (e.g. risk management, business continuity, IT disaster recovery, insurance, etc.) to give a co-ordinated approach for the organisation.
17	IT knows its business, and therefore is the better group to look after this. There should be communication links or protocols with risk management, business continuity and others so that they can provide input of situational reports when required.
18	We have a dedicated Security department that deals both with physical security and information security. The IT Security person works in Security but works closely with our IT personnel.
19	Information security is a cross-business issue - specialist practitioners may sit within IT but should work in close collaboration with business and governance stakeholders. Information security should also be regularly on the Board agenda
20	IT department has the education, knowledge, and skill to handle Information Security .
21	the board association gives the right level of power to make needed changes. The other options lack the juice to make it happen in a timely manner and adds to many levels of management to the decision process.
22	Need serious technical background and support from various technical experts in security management, so best by IT department. THsi though creates the risk is that it wil nail down to only IT, which is clearly not the case. Focus point for both security info officer and BCM to manage that risk.
23	Having risk management take responsibility for cybersecurity makes the most sense, but as many organizations can't afford a risk department, cybersecurity falls to IT, which is in the best position to deal with the technical issues. Regrettably, IT does not deal with the business implications of a security breach, which suggests a team ought to be formed that represents risk, IT, business continuity and the key business interests of the company, reporting to the board.
24	IndoSec reports to IT but is very closely aligned to Risk Management.
25	Information Assurance/Governance should take the lead with representatives from the groups mentioned above.
26	Both teams should be in the same functional unit.
27	Because of the technical understanding for good process, mitigating controls and response to information security related incidents. Business Continuity and the wider organisation will be involved but more from the comms and reputation protection element when responding to a major incident/crisis.
28	Leading questions - where is the "should business continuity be led by the Cybersecurity Team?"
29	to fully respond and manage information security a team of IT experts, legal, compliance, privacy, and business unit management must work together. We have an internal council to set policy and discuss procedures; a formal security incident response team, and an ad-hoc response team.
30	It should be led within the Assurance/Compliance department
31	Information security is in my opinion part off the "bermuda" triangle : Information Security , Continuity services, resilience. They all hook together.
32	It depends on the company structure. Ideally, the BCT should have an Information Security component, but whether it is lead by the IT unit, the BCT, or some other option depends on how well versed the units are in InfoSec/Cyber issues and solutions.
33	key word is "manage" all have a responsibility for info security within their realm of operations
34	Information Security and Business Continuity are both part of the Risk Mitigation Process of a company and should report "up through the Chief Risk Officer". InfoSec is an "oversight" function of IT and should have a different reporting structure.

35	InfoSec decisions can't be done without keep the rest of the organization informed at some level as to how to respond to employee, client and regulatory questions.
36	Information security management should be led by the IT Security specialized team
37	The InfoSec Incident Response Plan is lead by the InfoSec manager. Should the scope of the incident require the activation of the corporate level BC Plan \ EOC then responsibility \ leadership would shift to the EOC manager.
38	I think that there should be a dedicated information security / assurance lead specifically to deal with Info Sec (ISO27001)
39	In an ideal world the CISO reports to the board, though we see it report to different areas throughout the organization.
40	Info sec in my organisation comes under enterprise risk
41	OUr IT security team is within IT and has their voice muffled at times because they are within the machine, they advocate to be in our Risk Management Team with the General Counsel; we support this.
42	I feel by having other representatives included on the team from the various critical functions can best determine the impact of a security threat on their operation.
43	Ideally, the organisation should have an Information Security or Corporate Security team; however if not, then a forum of interested parties within the organisation should be created to coordinate the Information Security strategy and leverage the necessary expertise from within the organisation or from a third party supplier. Any such forum should also provide regular assurance reports to the organisations senior management team, supported/sponsored by a Director or Board member.
44	IS management should be handled by certified and experienced security professionals. We have a department dedicated to information security. Incidents are led by our Information Security department with the help of the IT department and the affected business areas. BC Team is a part of the Information Security department.
45	Infromation security is a discipline in its own right (as is BCM) and should have a business unit 1st line of defence to ensure such threats do not result in an incident.
46	We have a combined BCM and Information Security team
47	Info Sec shuold be managed by the Risk team but not in a silo; it should reach out to the wider business to create a form or possibly Champions culture
48	Information security management should be led by the Business Security division which must contain Business Continuity and Physical Security, too.
49	This is very technical and requires special knowledge, and response capability.
50	cant leave InfoSec to IT as there are competing interests during business as usual. Do not overload Business Continuity by adding another technical, policy and compliance matter. Board will be too myopic .
51	Information Security Management 'threats/impacts' do not come solely from IT but from a multitude of avenues including direct IT external; internal IT; employye carelessness/deliberate action; poor office security; social engineering; careless talk etc.
52	All business units have to participate.
53	IS should be lead by Information Security Team. It is a mix of IT and business and BC should be kept informed.and may be consulted depending on the impact of the issue (RACI Matrix)
54	RM is the closest entity to manage IS. For IT there might be a conflict of Interest. Within BCM there might not be sufficient skills. The board may not be the right place as Information security involves day to day operations. A team is not suitable is it is not a real entity
55	The ramifications associated with information security impact all segments of the organization. A Team of representatives from all areas can manage the ongoing information security activities and incident response most efficiently.
56	As with Business Continuity Management, Information Security Management needs board level support, at least with 'C' level executives assigned these responsibilities. Delegation of day to day operational decisions may be via a steering committee.(this committee may be authorised to address both BCM and ISM issues). The direct management of an ISMS would be better assigned to a manager with business and ITC knowledge.
57	Top down direction from the Board, and with operational responsibility to coordinate managed by one specific lead, which may be the security & resilience team.
58	Information security consists of more than the traditional digital networks maintained by IT. It also includes hard copy data, manufacturing information, other data that can be critical to business operations and reputation management.

59	Information security isn't just about one section of the organization and information only within your 4 walls. I believe a team touching on all areas of information risk needs to be in place. I'm not concerned about who ultimately holds the organization accountable whether that's the risk team or IT team - the risk team would be a key player on the security team and also have information consolidated for reporting purposes.
60	while IT implements it, info sec is a multi-departmental issue....as such it should be addressed by a multi- departmental 'team' consisting of the key departments within the org as appropriate (e.g. it, hr, marketing/public relations, ecommerce, member/customer services, audit, legal, etc.).
61	Anything security is a cultural thing. Anything cultural trickles down from the top. If the Board is not concerned with security, then no one else in the organization will be.
62	Clearly IS should be led by top management but they will in practice delegate this to specialists who need to engage all areas of the business. It is not an IT matter.
63	The Board, as with all things, has ultimate responsibility and oversight - and adopting internet security policy. Same for executive management. The IT department, continuity team, business units, and all employees have a part to play in protecting the organization from information security threats.
64	In reality organisations should have an ISO that reports to the board with lines to BC
65	Depending where the threat is manifested will determine which departments may need to be involved
66	It depends on what one considers within the bounds of information security.