Q1 Please briefly describe your IT staffing structure - the size and scope of your in-house technology team, IT functions you outsource, and how outsourced resources report within the pool.

Answered: 14 Skipped: 0

#	RESPONSES	DATE
1	TASB Risk Management Services is supported by TASB's IT Service Area. (TASB administers the Risk Management Fund). The IT Service Area is led by a CIO and has 43 FTEs divided into 7 primary teams: • Enterprise Architecture (2 FTE) • Risk Management Systems Support (3 FTE) • Technical Systems Support (7 FTE) • Information Center/Help Desk (8 FTE) • Project Management (8 FTE) • Technology/Software Platform Management (8 FTE) • Software Development (6 FTE) TASB-IT supports all TASB divisions and operations, including risk management. Though there is a dedicated risk management support team, every IT team plays a role in RMS technology support. In addition to TASB-IT, Risk Management Services has a Business Intelligence and Analysis team that works closely with IT that includes 2 DW/ETL developers, 4 reporting/BI analysts, 1 business analyst, and 1 RMS Application Administrator, and a manager – adding an additional 9 FTEs involved in supporting the Fund's technology. TASB does not outsource any major technology functions but uses a variety of service providers and consultants to support its business.	4/2/2018 10:37 AM
2	We have one on staff IT person responsible for internal system diagnosis and who coordinates with software and hardware vendors. We outsource the upkeep of the internal network and management of the hardware.	3/28/2018 11:04 AM
3	Internal IT falls to the finance director (me). We have an outside IT firm for server/network setup and maintenance	3/27/2018 6:46 PM
4	21, mostly in house but outsources parts where require niche skill or separation of duties. For e.g. Security Vulnerability Scans.	3/26/2018 5:52 PM
5	IT manager, IT Services Coordinator, Contract Programmer, Contract IT Services company as IT coordinator back up.	3/26/2018 4:51 PM
6	One in-house full time IT staff. Ongoing contract with IT specialist firm for work outside the expertise of in-house IT, and for IT backup for vacation, sick, etc.	3/26/2018 3:36 PM
7	3 permanent staff, IT manages all IT vendors and outsourcers. Software support for line of business (Claims and Policy Administration) is outsourced.	3/26/2018 2:28 PM
8	Outsourced to MSP for help desk and technical issues, project management, sys admin. There is a resource on site part-time.	3/26/2018 2:26 PM
9	The Benefit & P/L Pools contract with League for administrative services, including IT. There are 7 IT staff (IT Manager, Business Analyst, DB Developer, Project Mgmt Supr, Network Supr, Support Specialist, Data Specialist) who report to the Communications Director. Outside consultant is FPOV.	3/26/2018 12:55 PM
10	As part of our association, the association's IT team handles much of our IT needs. We have a separate IT person on the Insurance Staff who mainly handles our claims software.	3/26/2018 12:55 PM
11	Our Assistant Executive Officer oversees our IT operations with our Business Projects Manager looking after day-to-day issues. We contract with a small IT services company to manage and maintain our IT infrastructure and phone system. As part of that contract, an IT engineer is onsite 12 hours per week to provide support to staff and new IT initiatives. We use a different contractor to maintain our website and a third contractor to build our member management and content delivery platform. The AEO and BPM have monthly meetings with our Electronic Marketing Partners to ensure all parties are aware of each others projects and to coordinate any overlapping impact between those projects.	3/26/2018 11:48 AM
12	All IT is outsourced. Vendor is onsite one day a week, available by phone 24x7. Meetings scheduled as necessary.	3/26/2018 11:09 AM

13	7 members of IT team including manager, developer(s), help desk & network support; QA/Project manager.	3/26/2018 11:09 AM
14	outsource -everything	3/26/2018 10:49 AM

Q2 How do you set IT goals overall, and for specific projects? How is accountability toward goals measured?

Answered: 14 Skipped: 0

#	RESPONSES	DATE
1	IT priorities and goals are determined by individual TASB division business needs and strategic plans, including Risk Management Services. IT resources and objectives are governed by an Association-wide IT Steering Committee. Project results and outcomes are evaluated within the framework of progress toward business plans, financial results, and other organizational performance measures.	4/2/2018 10:37 AM
2	IT goals are based on project deadlines and budget.	3/28/2018 11:04 AM
3	We work with outside IT firm to generate a long term (3-5 years) plan and budget accordingly. We review the goals every September when planning the next year's budget	3/27/2018 6:46 PM
4	IT goals are divided into three high level categories- 1. Project success criteria for individual projects that agreed by business and IT before we start development phase of the project that we have to meet. 2. Operational checklist of items that have to be met every year, which provides the basis for creating IT operational goals, and 3. Continual training/education.	3/26/2018 5:52 PM
5	Goals are set at department level with Exec Director and Board approval. Accountability is measured quarterly towards completion.	3/26/2018 4:51 PM
6	No hard accountability goals. More general performance, did project get done timely, correctly. Some projects have timeline in contract; measurement is did project get done according to contract?	3/26/2018 3:36 PM
7	IT goals are project based against a set of long-term strategic IT initiatives. These projects are discussed, and priorities set during monthly Steering Committee meetings made up of executive leadership.	3/26/2018 2:28 PM
8	There has been changes in IT over the past year and we are compiling a project list in conjunction with the IT vendor. Corporate goals drive IT goals - accountability is "proof is in the pudding".	3/26/2018 2:26 PM
9	All project/goals, but those particularly involving IT, are accountability to the cross-function management team of People, Projects & Priorities (P3). Monthly meetings report on progress and accountability to timeline/project mgmt. All proposed business cases for the following year meet pre-established criteria and are approved/prioritized by P3 during budget prep (Sept).	3/26/2018 12:55 PM
10	We have a Service Level Agreement with the IT department. It is being updated to contain project specific goals and timelines.	3/26/2018 12:55 PM
11	Our staff and vendors are always looking for ways to improve our IT footprint as well as electronic service delivery to our members. Once a year, our executive management team will discuss current and future initiatives. Ideas for change are then shared with relevant staff for their input. Conversations are then had with our IT vendors to determine scope, breadth, and cost of these changes. Ideas that are ultimately approved by the CEO are then added to our two-year budget. The AEO then manages the BPM to work to complete the various initiatives by agreed upon deadlines. Deadlines are project specific. Vendors and staff are consulted throughout each project's life to determine achievable deliverables and deadlines. Relevant staff are kept apprised of changes to project scope and breadth that result in changes to deliverables and deadlines.	3/26/2018 11:48 AM
12	Sr. Staff determines IT goals & priorities. Progress is the standard.	3/26/2018 11:09 AM
13	Deadlines and functionality for projects and set by department managers. Manager tests and sign's off on project once completed and tested.	3/26/2018 11:09 AM
14	We need to set up some IT policies	3/26/2018 10:49 AM

Q3 What business continuity and/or disaster recovery planning have you done specifically for your own pool's operations?

Answered: 14 Skipped: 0

#	RESPONSES	DATE
1	TASB has a business continuity and disaster recovery plan for all of its operations. It is reviewed annually and tested on a periodic basis. It includes system redundancy, data recovery, and alternative working procedures should our primary location become inaccessible.	4/2/2018 10:37 AM
2	Data recovery tests are performed internally annually with procedures in place for response to disaster recover.	3/28/2018 11:04 AM
3	We back up to the cloud several times a day	3/27/2018 6:46 PM
4	We have basic business continuity and DR plan in place and currently going through RFP to further strengthen ourselves in this area.	3/26/2018 5:52 PM
5	Extensive policy and procedures created. Also contract with outside IT vendor services to provide full backup/onsite if necessary with trailers/generators, etc.	3/26/2018 4:51 PM
6	We contracted with a third party for years. Recently set up own process internally and cancelled contract. Part of continuity is agreements with other pools in state but located in different geographic location.	3/26/2018 3:36 PM
7	We are currently in the process of migrating primarily to cloud-based servers for all of our primary systems. This should give us more cost-effective DR options. After this effort is largely complete we anticipate beginning a BCP initiative to prepare updated Business Continutiy Plans.	3/26/2018 2:28 PM
8	Funny you should ask, we are undergoing this corporate-wide initiate currently to address business continuity and DR. IT is main player is the overall project plan. We are still in the beginning stages - utilizing best practice template provided by Agility.	3/26/2018 2:26 PM
9	Not enough. This is a high priority for the League this year, at the Member Pools request.	3/26/2018 12:55 PM
10	We have a business continuity plan for the entire association, include the insurance dept.	3/26/2018 12:55 PM
11	We have an automated mechanism that backs up data from all designated servers (six days a week) and network-connected computers (four days a week) to offsite disk-based storage. All data is encrypted while stored in the data storage center. Tests have been performed and we can restore service within 1-2 hours anywhere in the United States.	3/26/2018 11:48 AM
12	New claims system will be cloud based, eliminating hardware and software upgrades, and security concerns. Also addresses DRP.	3/26/2018 11:09 AM
13	Some, but it's outdated. On our radar to update in 2018.	3/26/2018 11:09 AM
14	none	3/26/2018 10:49 AM

Q4 Has your pool had a cybersecurity audit? If yes, briefly describe how it was conducted and when the audit was most recently completed?

Answered: 14 Skipped: 0

#	RESPONSES	DATE
1	TASB has conducted various cyber security assessments and audits in the past. This includes reviews of internal controls around technology access. TASB is currently working with a third-party vendor to conduct a new preventative security assessment to identify and remediate any identified security issues and establish a new framework for TASB data security.	4/2/2018 10:37 AM
2	We resource with an outside vendor that monitors our network at the firewall and switch level for intrusion detection. We are provided monthly with an activity report.	3/28/2018 11:04 AM
3	No	3/27/2018 6:46 PM
4	Yes, in parts for all new IT systems. Currently in process of issuing RFP to conduct holistic cyber security audit.	3/26/2018 5:52 PM
5	Yes. We are examined every 3- 5 years by the Idaho Dept of Insurance and this is one of the myriad of items addressed during their audit. Last one completed 2 years ago.	3/26/2018 4:51 PM
6	Yes. Contracted with firm to do audit 2 years ago. They came into the office and met with IT and reviewed systems and reviewed policies.	3/26/2018 3:36 PM
7	Yes, external party included both internal and external vulnerability scans. This was completed in late 2016. A follow-up audit including an external penetration test is planned for the next 90 days.	3/26/2018 2:28 PM
8	GreyCastle did an Internal and External Vulnerability Assessment in May 2017 - we have not had a cybersecurity audit.	3/26/2018 2:26 PM
9	No	3/26/2018 12:55 PM
10	No.	3/26/2018 12:55 PM
11	We are about to embark on an audit.	3/26/2018 11:48 AM
12	No.	3/26/2018 11:09 AM
13	A network audit was conducted 2 years ago, and misc internal cyber audits are ongoing.	3/26/2018 11:09 AM
14	nope	3/26/2018 10:49 AM

Q5 Has your pool specifically engaged penetration testing for its own operations? If so, briefly describe how this was done and when testing was last conducted.

Answered: 14 Skipped: 0

#	RESPONSES	DATE
1	The preventive security assessment currently underway includes both internal and external penetration testing and review of several major applications, including Risk Management applications. TASB has conducted penetration testing in the past on its networks and applications.	4/2/2018 10:37 AM
2	No	3/28/2018 11:04 AM
3	No, but I think this is a good idea. We are having 2 new servers installed in a couple of weeks and this would be a good follow up step	3/27/2018 6:46 PM
4	Quarterly penetration test conducted by external vendor.	3/26/2018 5:52 PM
5	Yes. We have conducted tests internally with personnel and discussed hiring an outside firm to do the same.	3/26/2018 4:51 PM
6	No.	3/26/2018 3:36 PM
7	Vulnerability testing has been conducted in external audits performed in late 2016. A penetration test is also scheduled for the next 90 days.	3/26/2018 2:28 PM
8	No - we did consider doing this, but have not done so yet. May be mute if we go to cloud-based platform.	3/26/2018 2:26 PM
9	No	3/26/2018 12:55 PM
10	Yes - our IT dept does phishing tests and other types of training.	3/26/2018 12:55 PM
11	We have not done this but will be doing our first as part of the upcoming cybersecurity audit.	3/26/2018 11:48 AM
12	No.	3/26/2018 11:09 AM
13	Yes, 3 years ago. It was white had testing where the pen testers were giving the layout of our system for the intent of identifying any vulnerabilities.	3/26/2018 11:09 AM
14	none	3/26/2018 10:49 AM

Q6 How do you manage for compliance with HIPAA, PCI-DSS, Medicare Secondary Payor, or other regulations that have an online or technology-based reporting component? How do IT and other departments share responsibility for compliance?

Answered: 13 Skipped: 1

#	RESPONSES	DATE
1	TASB Risk Management Services has a compliance unit dedicated to managing and reviewing compliance with the various applicable regulations and statutes, including some of those noted above. Risk Management Legal and Regulatory Affairs, along with TASB's General Counsel's office review and identify new or changed requirements. Risk Management services works with IT and third-party software vendors to ensure systems, data, and reporting practices meet all legal and statutory requirements.	4/2/2018 10:37 AM
2	All information which has personally identification is encrypted and the policies in place are that if any information that contains personally identifiable information is to be emailed, it must be done securely, either through a secure email server or through encryption with a minimum of password encryption.	3/28/2018 11:04 AM
3	We don't do PCI-DSS. Our staff logs into a firm's website that reports our MSP claims info.	3/27/2018 6:46 PM
4	We do not formally comply with any of these standards but if needed, we will be able to clear most of these standards for IT systems and will need to work on human part of compliance. For e.g. need to designate privacy officer.	3/26/2018 5:52 PM
5	Internal staffing compliance is conducted offline with thorough document retention system with limited access by personnel. Online claims system handles all other compliance.	3/26/2018 4:51 PM
6	Reporting component built into Claims System. We have very few claims involving Medicare, no WC.	3/26/2018 3:36 PM
7	No compliance with HIPAA or PCI-DSS yet. Other compliance, such as financials or claims audits involve 3rd party assessments. IT is involved in providing access to systems to the third party auditors, as well as verifying data and system integrity.	3/26/2018 2:28 PM
8	HIPAA - we have engaged a law firm to compile relevant policies, however they need to be reviewed and updated; PCI-DSS - N/A; MSP - handled by Claims through Origami; we have a number of in-house policies that are reviewed by legal.	3/26/2018 2:26 PM
9	The Pools work with their respective legal counsel and assign staff for compliance. The Pools draw from TPA's and external billing administrator for IT support, when applicable. The Pools do not currently rely on internal IT for support	3/26/2018 12:55 PM
10	IT dept and our IT person handle this.	3/26/2018 12:55 PM
11	For HIPAA, our exposure is limited to our own 25 employees. Security access to their personally identifiable information is limited to the employee that administers our Human Resources tasks. Where we accept credit/debit card transactions, we use PayPal Merchant services. I believe that Medicare Secondary Payor risk is the responsibility of our TPA. Annual review of each of these areas includes questions related to meeting best practices for cyber protection.	3/26/2018 11:48 AM
12	Vendor contracts. The security model is audited by the IT vendor and Sr. Staff to determine compliance.	3/26/2018 11:09 AM
13	We undergo regular HIPAA and PIC reviews, audits and training.	3/26/2018 11:09 AM

Q7 What is the IT risk in your pool that keeps you awake at night?

Answered: 12 Skipped: 2

#	RESPONSES	DATE
1	Data security, particularly personal data for members and claimants. Lax, improperly managed security and user access controls. Failure to innovate and deploy technology solutions that meet member needs timely and ahead of competition. The continuing escalating cost and complexity. Maintaining staff with the appropriate, modern skill sets and ability to learn new technology.	4/2/2018 10:37 AM
2	Users clicking on links in phishing emails. One very obvious phishing email had 2 of our 21 users click on it, thank goodness it seems to be benign. We were able to get the word circulated before anyone clicked on the one from last week, which was nasty. Our customers are getting hacked and their email addresses are being used for these phishing emails.	3/27/2018 6:46 PM
3	Cyber security. This is a never ending game, where you need to stay one step ahead of hacker all the time and sometimes feels like an impossible task.	3/26/2018 5:52 PM
4	Internal staff falling for trap.	3/26/2018 4:51 PM
5	1. Hacker getting access to protected information and 2. Cloud based information system crashing.	3/26/2018 3:36 PM
6	Cybersecurity of our members. We feel reasonably confident that our organization's security has been shored up, though we continue to address IT risks moving forward; however, our members' cybersecurity is all across the board and we continue to look for ways to address this.	3/26/2018 2:28 PM
7	The unknown. Actions that employees may take, even with the best policies and protocols in place, you can't police everything.	3/26/2018 2:26 PM
8	Cyber vulnerability and business continuity	3/26/2018 12:55 PM
9	I'm a very sound sleeper due to what we already have in place. However, on a day-to-day basis, I am waiting for the day when our of our employees clicks on something they shouldn't have and we jump into crisis remediation mode. But I don't lose any sleep over it.	3/26/2018 11:48 AM
10	At the moment, a hardware failure in the rack.	3/26/2018 11:09 AM
11	That a bad actor will find a way into the system.	3/26/2018 11:09 AM
12	access to our cloud based claims system	3/26/2018 10:49 AM