IT Governance
What Is It, and Why Do You Need It?

In today's fast-changing technology environment, IT governance committees have emerged as an effective tool to ensure technology investments are supporting organizational objectives and undue cyber risk is not in play. Members of the group often include executive leadership, IT department leadership, and, if applicable, board of directors members or other stakeholders.

The committee's charge includes the regular review of technology planning, project status, cybersecurity program, IT compliance, and IT risk management.

By Caitlin Q. Bailey O'Neill, Assistant Editor

Mark Torello, partner-in-charge of Whittlesey Technology and a member of the CTCPA Board of Directors, was instrumental in helping create an IT governance committee for the CTCPA this year.

Mark recently sat down with *Connecticut CPA* to share more about the process and how it can benefit companies and organizations of all sizes.

What is IT governance?

IT governance is really a process that establishes oversight, accountability, and effective communication so that technology is utilized appropriately, risk is managed, and IT supports business objectives. This comes into play when there's more than one person in the mix for decision-making. Is one person recommending an IT initiative? Is another person approving initiatives at a business level? Is another person, like a CFO, approving it at a financial level? There might be an IT vendor in the mix, too.

So it's really to get everyone on the same page?

Exactly. The main goal really is to establish effective communication so that decisions can be made wisely, more quickly, and with all the appropriate parties' input.

When you have more people in the mix, things easily get lost in translation. The communication gap can be fixed by simply bringing the right people to the table, so they have the chance to ask all their questions together and hear answers to the other people's questions.

Who should be a part of the IT governance committee?

Executive management, the head of finance, the CEO, the head of IT and/or the chief IT vendor if you're outsourcing that service, and sometimes department heads, board of directors members, or other stakeholders. IT needs to support business objectives, not the other way around. If you don't have the right players as part of the governance process, you can easily miss the mark with deploying the right technology.

When the CEO hears the answer to the finance person's question, it gives the CEO a little comfort. When the finance person/CFO hears that the CEO is behind an initiative and got all their questions answered to satisfaction, the CFO is more comfortable allocating the necessary dollars. Then they can look at each and nod and say "Yes, this makes sense." Now, you can have progress that's achieved much faster and much more efficiently for that organization.

Is this a new concept?

We've been doing this for about 10 years now, but recently it's become more important with the level of cybersecurity threat and IT risk that every single business and nonprofit faces. What we found is businesses were getting into significant trouble – getting hacked, getting breached, losing data – because there were silos of responsibility centers. There was the IT person,

there was management, there were people using the technology, and no one was getting together to make sure IT risk was being managed sufficiently and technology was truly supporting business initiatives.

By bringing everyone together, security initiatives can be acted upon much more quickly than before and breaches prevented because, for example, we're not waiting three to six months to communicate the need for two-factor authentication – getting approval from the finance department, the chief executive, and the IT person. It's all decided in one room. Contracts can get signed and action taken much more efficiently.

It sounds like a lot of this really comes down to facilitating communication.

Yes. IT governance is so important and successful because it promotes the right level of communication and it helps achieve the oversight that's required as well. If there's a problem or an opportunity, it's documented. There's an approval process, and the people who are assigned new initiatives know that they're going to be held accountable, that it's important, and that they're going to have to report on it at the next governance meeting. That accountability factor really improves the strength of the organization.

How often should a governance group meet?

Typically committee meetings are monthly, with some level of intramonth activity. Once the program is mature, it can be appropriate to meet every other month or even quarterly, depending on the number of initiatives at play.

> The communication gap can be fixed by simply bringing the right people to the table, so they have the chance to ask all their questions together and hear answers to the other people's questions.

> IT needs to support business objectives, not the other way around. If you don't have the right players as part of the governance process, you can easily miss the mark with deploying the right technology.

What should be the first steps to get things started?

First, establish the agenda and reporting structure – what types of reports should be produced for this meeting to facilitate accountability, and what the responsibilities of all the parties are.

You would most likely have an IT projects agenda item that includes status reports, and an IT and cyber compliance section to talk about different compliance requirements and risk assessments that need to be performed based on your specific compliance and regulatory requirements. You might have an incident report so that everyone in the group can hear what has occurred since the last meeting, what level of risk or damage those incidents might have caused, and what's being done about it.

A lot of times we have a planning agenda item to review technology initiatives for the coming year, and then we have a standard technology reporting section that goes over network health. This is very important because this is where the accountability of whoever is the head of technology comes in. For example, everyone on the governance committee can ask questions about the network health rating, what it is, and how it can be improved.

This is also where you can catch things when you have an IT department or vendor who may not be performing at an appropriate level. One of the big reports that we find important for accountability is security patch management, showing all systems that have security patches that are out of date more than, say, 10 days. That can represent a big risk for the organization.

How does a cybersecurity risk assessment fit into the process?

What the IT governance process makes you realize is that, to really govern IT, we need to do an IT risk assessment every year. When the assessment comes back with recommendations, people realize that there will be associated costs, some changes could cause some disruption to the way the organization operates, and some of these things, we're not sure if we really need them or not. People see the benefit of this larger discussion, and that's how this really adds value.

Some clients decide to have a risk assessment because they lost data, or they had a breach because they trusted one particular vendor, or they trusted the IT person and the IT person didn't tell the right person that the back-ups weren't working, and there wasn't really anyone overseeing things that had an appropriate knowledge level.

Those organizations have a problem, and they bring in an IT auditor who says, "Well, you're not big enough to have a CIO or an organized IT structure, but you're too big not to have sophisticated IT oversight and governance." That's where it may be appropriate to outsource and find a firm that can champion the governance process and act as the committee chair and also as an outsourced CIO. ▶

What if your IT vendor or internal staff are uncomfortable with this level of oversight?

We had one client we did this with and the internal IT administrator was very uncomfortable with the situation. It was a little contentious for the first six months to a year. In the end, though, the executive management bought into the program because the organization had been hacked and it ended up costing the company $160,000.

We know the internal IT staff are really good people and do a really good job, but this does not mean that they do not need oversight, help with specific initiatives, or assistance with translating IT risk to business risk. The executive management really liked that there were more experienced individuals working with him.

Eventually he started realizing the benefits as well because he was getting his projects approved faster. The CEO and the CFO were right there – he didn't have to schedule time with the CEO, who would then send him to deliver the message to the CFO. It could sometimes take him six months to get anything done. Now he's getting projects accomplished in under a month, and he's happy!

> The people who are assigned new initiatives know that they're going to be held accountable, that it's important, and that they're going to have to report on it at the next governance meeting.

At this same organization, they are looking to migrate a particular software to the cloud. The internal IT person was able to pipe up at a governance meeting and say "I'm not really comfortable doing that. Would it be okay if I got some assistance?" Now you've got everyone hearing the request, and the administrator has subject matter experts available to serve as a resource to him. Right there in that meeting, he got tacit approval to call in an expert to ensure the process was successful.

What advice would you give someone thinking about starting an IT governance committee?

Find someone with IT governance or IT risk expertise to lead the charge. You can look for certain certifications in that area – someone who's certified in risk and information controls or a certified information security auditor. In IT governance, part of the goal is to minimize IT risk, but also to make sure technology is supporting the business objectives. That takes someone who can understand both technology and business.

Cyber Security Check-Up: True Tales of a Cyber Audit

By Caitlin Q. Bailey O'Neill, Assistant Editor

We're not just talking the talk by encouraging all members to have a cyber security audit – this fall, we went through one ourselves. Marketing Manager **Melissa Thompson**, who coordinates the office's technology initiatives and serves as a staff liaison to the Technology Committee and the IT Governance Committee, sat down with *Connecticut CPA* to share her cyber audit experience.

Why did CTCPA decide to have a cyber security audit?

The assessment was one of the first steps initiated by our newly formed IT governance committee. We needed to assess the current situation in order to make the best possible business decisions going forward. A cyber audit looks at the entire system. Is data secure? Is the equipment up-to-date and documented? Is there a business continuity plan? Are users up-to-speed on best practices? Are they trained to be suspicious of phishing emails? What are our risks?

Who performed the audit?

If you have an outside IT vendor in addition to or instead of in-house IT staff, that organization should not perform the audit. You need a neutral party who specializes in cyber security audits to really dig in and make sure everything looks secure.

Did your IT company feel threatened by an outside party "checking in" on their work?

A cyber security audit is really good for everybody – it opens up a conversation about risk vs. cost, what we are comfortable with, and other considerations.

If there are any findings (and there always are), it's usually your IT company who will do the work – the company performing the audit is not looking to steal business. It truly is a win-win for everyone. Our IT company was aware of the audit and supportive – I did have to call them a few times the day of the audit to get administrative credentials and things like that.

How long did the audit take? What was it like?

Before site work began, the technology consultant performing the audit asked for a list of things like computer use policies, a network diagram, a software/hardware inventory, applications that store/process customer information, etc. He provided a secure portal to transmit them. If you don't have all of the information, that's okay – it's all part of the process.

Chris [the auditor] was only on-site for one day; I think the only staff person who even noticed anything was going on was me, as the technology liaison. While he was here, he walked around the office to look for things like post-its with passwords (a common no-no!). He took some pictures of things and asked questions to see what policies were in place. He looked at firmware and checked to see if we had documentation of our servers. He tried to hack our guest wireless. In many ways it's similar to a financial audit, really.

Did the audit impact the rest of the staff?

It happened without them even knowing it! It was interesting. Chris emailed me and said he had set up three different phishing emails to test all staff. He told me he was going to send them to me so I would know what they looked like.

I waited and waited, but nothing came through. Score one for us – our spam filter caught them all! I had to call our IT company to whitelist the emails so they would go through. The phishing test went on for three days. All staff received the phishing emails, and in the end, no one fell for them. I'm pretty proud of that.

How were the results presented?

The company wrote up a formal report within a couple weeks and securely sent it through an encrypted site. It was a thorough report, written in essay form and fairly easy to understand as a layperson. The report prioritized potential action items and recommended next steps. There was also a matrix listing minor issues or additional recommendations to make us even safer. For example, following the audit we made our password policy even more stringent.

The assessment was the focus of our first IT governance committee meeting. We spent several hours reviewing the findings, discussing risks and recommendations, and assigning tasks. **Mark Torello**, a member-at-large of our board of directors and partner-in-charge of Whittlesey Technology, will also report the findings to the board of directors. It's important to keep your board of directors or leadership in the loop, because some of the recommendations may very well affect your budget.

What were the biggest benefits of the audit?

You pay for an IT company and assume you're safe; this tests that. If we're breached, the liability is on us, not the IT company. People don't always realize that.

I think it's important to recognize, though, that this is an ongoing process. Experts recommend doing a cyber security audit every year. It's a snapshot – you have to constantly be vigilant and continue training your staff. The bad guys are constantly revising their tactics, so we need to make sure we're staying on top of it.